EDITING TEAM

EDITOR-IN-CHIEF
Summer Danzeisen

EDITOR-IN-CHIEF
Laura Ashley Harris

MANAGING EDITORS
Stephanie Goldberg
Trevor Schmitt

SENIOR ARTICLES EDITOR
Molly Hayssen

SENIOR CASE COMMENTS EDITOR
Flora Lee

SENIOR LEGAL NEWS EDITOR
Nur Lalji

SENIOR NOTES EDITOR
Sara Wolovick

SENIOR SOLICITATIONS EDITOR
Lara Rosenberg

SENIOR TECHNOLOGY EDITOR
David Frey

DIRECTOR OF DEVELOPMENT
Kamila Benzina

DIRECTOR OF OUTREACH
Daniel Carlen

DIRECTORS OF TECHNOLOGY
Eric Pait
Kelly Truesdale

EDITORS
Joshua Banker  Avi Ginsberg  Xincheng Ma  Benn Waters
Harsimar Dhanoa  Briana Hauser  John Park  Rachel Wehr
Flora Feng  Laura Hillsman  Alex Rhim  Eric Westerhold
Adam Gerchick  Rachel Johns  Michael Rose  Temesgen Woldezion
## Staff Members

<table>
<thead>
<tr>
<th>Member</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sherlyn Abdullah</td>
<td>Tracey Klees</td>
</tr>
<tr>
<td>Jae Ahn</td>
<td>Sarah Koslov</td>
</tr>
<tr>
<td>Niki Arakelian</td>
<td>Anne Lee</td>
</tr>
<tr>
<td>Devin Benavidez</td>
<td>Ladan Mohaddes</td>
</tr>
<tr>
<td>Raymond Coscia</td>
<td>Sofia Panero</td>
</tr>
<tr>
<td>Alexandra Coyle</td>
<td>Daniel Passon</td>
</tr>
<tr>
<td>Andrew Do</td>
<td>Peter Pyatigorsky</td>
</tr>
<tr>
<td>Joseph Ehrenkrantz</td>
<td>Thomas Sandstrom</td>
</tr>
<tr>
<td>Nolan Fargo</td>
<td>Aaron Scheinman</td>
</tr>
<tr>
<td>Corey Fitzpatrick</td>
<td>David Seidman</td>
</tr>
<tr>
<td>Séké Godo</td>
<td>Shelby Smith</td>
</tr>
<tr>
<td>Andres Gonzalez</td>
<td>Joseph Suh</td>
</tr>
<tr>
<td>Clinton Greub</td>
<td>Lyle Stewart</td>
</tr>
<tr>
<td>Grace Harter</td>
<td>Mary Weaver</td>
</tr>
<tr>
<td>Isabella Havas</td>
<td>Leetal Weiss</td>
</tr>
<tr>
<td>John Heflin</td>
<td>Ruiqiao Wen</td>
</tr>
<tr>
<td>Rebecca Iafrati</td>
<td>Ryan Whittington</td>
</tr>
<tr>
<td>Guiying Ji</td>
<td>Jeff Liji Zhou</td>
</tr>
<tr>
<td>Eric Kashdan</td>
<td>Yifan Zhu</td>
</tr>
<tr>
<td>Aileen Kim</td>
<td>Alan Zorofchian</td>
</tr>
</tbody>
</table>
# Table of Contents

## Articles

Should the Common Law System Welcome Artificial Intelligence? A Case Study of China’s Same-Type Case Reference System ........ 223  
*Jinting Deng*

Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox ................................................................. 281  
*Dr. Thibault Schrepel*

“Deepfakes”: The Newest Way to Commit One of the Oldest Crimes ................................................................. 339  
*Russell Spivak*

## Notes

The Bona Fide Acquisition Rule Applied to Cryptocurrency ............ 402  
*Andrew Balthazor*

A Normative Approach to Broadband Regulation: Curbing the Anti-Competitive Behavior of Internet Service Providers ................. 426  
*Laura Ashley Harris*

## Case Comment

*Berninger v. Federal Communications Commission*: The Outer Limits of Judicial Deference ........................................... 461  
*Daniel Carlen*
Technology Explainers

“Study Drugs”: The Mechanisms of ADHD Medications and Their Abuse on College Campuses ......................................................... 476
Peter Pyatigorsky

Automated Defense Technology .................................................. 492
Shelby Smith

Drones: How They Work, Applications, and Legal Issues ............... 502
Joseph Suh
SHOULD THE COMMON LAW SYSTEM WELCOME ARTIFICIAL INTELLIGENCE: A CASE STUDY OF CHINA’S SAME-TYPE CASE REFERENCE SYSTEM

Jinting Deng*

CITE AS: 3 GEO. L. TECH. REV. 223 (2019)

I. INTRODUCTION

China has recently embraced a national use of “big data” through the implementation of judicial reforms that utilize new technology. These technological reforms have turned China’s judicial system into one closely resembling a common law system. Because of this, China’s use of artificial intelligence (AI) in the judicial setting provides a case study for general implementation of AI in common law systems.

A. Is China Establishing a Common Law System?

Modern China’s case law begins in the 1980s. In 1985, China’s highest court, the Supreme People’s Court of China (SPCC) began to publish “typical cases” (dianxin anli, 典型案例) in its official publication, 

* Dr. Jinting Deng (jintingdeng@126.com) is an Associate Professor in the School of Law, Renmin University of China, a Researcher at the Research Center for Criminal Justice at Renmin University of China, and a Researcher at the Law and Technology Institute at Renmin Law School. Her research areas include anti-corruption, the judicial system, evidence, and comparative law. The article is funded by “National Key R&D Program of China”, 2018YFC0830905. The author would like to thank Professor Pinxin Liu for his help in carrying out the interviews and field observations and thank Professor Pinxin Liu, Professor Zhicheng Dou, Professor Xuejun Li, Mr. Jianyue Zhang, and all interviewed prosecutors, judges, and software designers for their valuable insights and comments during the drafting of the article. The author is grateful for all the comments and edits offered by the reviewers and the editors. All views and errors are the author’s alone.
the Gazette of SPCC. Since then, there have been debates about whether or not to adopt “precedent” into China’s legal system. Against some resistance, SPCC has made consistent efforts to increase the role of prior cases in China’s legal system, leading to the establishment of the guiding case system in 2010. That year, the SPCC issued the Provisions on Case Guidance, which established the guiding case law system for mainland China. Guiding cases (zhì dào xíng àn lì, 指导性案例) are cases that were originally decided by courts at different levels and then selected, edited, and reissued to all courts by SPCC as quasi-binding. These cases are only quasi-binding because they are not recognized as law, cannot be cited as the main basis for a judgment, and judges can decline to follow these cases without specifying reasons. Guiding cases have generated significant discussion among scholars and officials, mostly surrounding their similarity to precedent cases in common law regimes. Prior studies note that, although guiding cases have some similarity to common law precedent cases, significant differences remain, such as their non-binding nature, their origin with SPCC rather than the deciding court, and their relatively short legal reasoning section. Yet, these cases still promote judicial uniformity even through the lens of the civil law regime.

This article examines a series of systems and tools called the Same-Type Case Reference system (STCR). STCR was started in 2015, and is layered on top of the guiding case system. Unlike guiding cases, STCR aims to make prior cases binding, rather than quasi-binding, and thus, is a further step towards creating a type of common law in China. STCR is composed of a series of systems that work together to ensure judges adhere to prior decisions made by their own courts (or superior courts) on cases that are similar to the case before them. These interconnected systems include: a national database of published judicial opinions; software programs that make it possible and convenient to search, analyze, and compare millions of Chinese judgments; and new

---

1 These “typical cases” are issued by the SPCC as a teaching tool for lower courts.
3 Id.
4 A deciding court is the court that issued the original opinion.
5 Id. at 2231–33.
6 In Chinese this is called “类案参考系统” (lei an kao xi tong).
7 SPCC’s Regulations on the Publication of Judicial Opinions on Internet by People’s Courts, revised in 2016 and effective on Oct. 1, 2016.
8 Such software systems include FaXin law trust (法信) (http://www.faxin.cn), developed by SPCC, which was launched April 2016. Liang Xiaohui, China’s Supreme Law “Legal
judicial accountability rules that require judges to follow previously decided cases of the same type.

In 2015, SPCC’s *Several Opinions on Improving the Judicial Accountability System of People’s Courts (Opinions on Accountability)* first formalized a judicial accountability system. The details of the system were further articulated in 2017 by SPCC’s *Preliminary Opinions on the Implementation of the Judicial Accountability System* (Implementation Opinions on Accountability). Because of these two opinions, judges are now legally required to follow same-type cases decided by their courts and superior courts when deciding any new case unless the judges explain and obtain a superior judge’s approval before deviating from previously decided same-type cases. If the judges do not follow these rules, they can be disciplined for failing to comply. With these new judicial accountability rules in place, China is also slowly adding software components to STCR in each province in order to further control judicial conformance with same-type cases.

Compared with the previous guiding case system, STCR is a much more significant step towards a common law regime and deserves examination. Interestingly, China’s motivation in implementing this new common law-type system is not to increase judicial authority. Rather, China hopes to increase judicial independence while also retaining

---

9 *Several Opinions of SPCC on Improving the Judicial Accountability System of People’s Courts*, effective on September 21, 2015. In China, an opinion of the SPCC includes rules for the judicial system.


11 Opinions of the Supreme People's Court on the Judicial Accountability System, art. 8; Opinions of the Supreme People's Court on the Implementation of the Judicial Accountability System, art. 39 & 40(1).

12 Opinions of the Supreme People's Court on the Judicial Accountability System, art. 24(3); Opinions of the Supreme People's Court on the Implementation of the Judicial Accountability System, art. 16(4), 40(2), (3), (4), 43, 48, & 64(3).

13 For the punishment, see Point Two, the Opinions of SPCC and the Supreme People’s Procuratorate of China (SPPC) on Establishing the Disciplinary System for Judges and Prosecutors (Opinions on Punishment), effective Oct. 12, 2016.
supervision over judges. Understanding the structure and function of STCR in China provides a perspective on common law systems that may provide insight into possible transformations in common law regimes through the use of technology.

B. The Growth of Technology in the Judicial System

The establishment and function of STCR is realized, in part, through the intelligentization of China’s judicial systems, i.e. equipping China’s judicial systems with intelligent technologies. This process includes building software programs that digitalize, manage, and establish applications of judgments through legal research services as well as statistical analyses and comparisons. AI allows these software programs to suggest decisions, calculate possible sentences for specific crimes or scenarios, and summarize typical compensation. For example, a judge can upload an electronic complaint or hearing record, and the program will study the complaint or record and compare the record with previously decided judgments to find the same-type case reference files. The machines are “trained” through nearly forty million stored judgments and are able to compare newly loaded complaints with older ones. Then, the system selects same-type cases. Once the correct same-type cases are found, the program will generate preliminary judgments with facts extracted from uploaded complaints or records and reasoning and conclusions learned from same-type case decisions.

In China, STCR is not the only AI system used in the legal context. Prosecutors have tried to use AI programs to help make prosecutorial decisions, and policemen have tried to use some AI programs to predict and investigate crimes. Additionally, the city of Hangzhou has established cybercourts, through which litigants submit their documents

---

14 Such a motive is not explicitly expressed but can be read from the facilitating requirements and the connection to the disciplinary system as well as reforms enhancing judicial authority. This is elaborated upon in Part II of this article.

15 The software system called “artificial intelligent reference of same-type-cases” system (类案智慧推送系统) went online January 2018. The Supreme Court of Wisdom Court Navigation System and the Class Intelligent Push System are Online Today, SOHU (Jan. 5, 2018), http://www.sohu.com/a/215006410_362042 [https://perma.cc/5NRS-WBU8].

16 The SPPC has issued the 2017-2020 Big Data Action in Procuratorates Guidance in June 2017. See Promote Big Data Applications to Create “Smart Policing,” LEGAL DAILY (June 6, 2017), http://www.legaldaily.com.cn/index/content/2017-06/12/content_7201213.htm [https://perma.cc/AKE6-X9RY].
and participate in trials over the Internet without once appearing in court. In other cities, robot guides are positioned in courts and prosecutors’ offices. The robot guides are capable of having simple conversations with litigants to help them file complaints and to provide procedural assistance. Other AI machines answer phone calls or online queries.

The development of these systems was made possible by China’s national strategy to embrace “big data.”

Similarly, the U.S. has seen the introduction of AI machines in both the private and public sector. The ability of these machines to make certain decisions independently with little human intervention, such as relying upon AI to select who shall be investigated by the Internal Revenue Service (IRS) is alarming. Despite these alarms, intelligent financial advisors, algorithmic consumers, robot regulators, robot armies, intelligent policemen, machine witnesses, and robot lawyers

---


19 *Id.*


26 Coglianese & Lehr, *supra* note 21, at 1167–75.
already exist, causing much debate in the legal community. But little serious academic discussion is ongoing about the application of AI in judicial decision-making, and the discussions in the news media consider such application absurd.

Many people in the U.S. find the prospect of a robot judge unfathomable. It seems technically impossible to have machines “find out” the patterns of “recurring situational problems” and make sound judgments after considering numerous normative values without specification of these values and patterns at the front-end design phase of the machines. Additionally, even if these values could be specified beforehand, many still feel it is legally and morally unsound to have a robot decide how to proceed in a case. However, in the private sector, algorithmic dispute moderators are already being used on online trading platforms such as eBay and Amazon, and “blockchain adjudicators” are used on platforms such as OpenBazaar and Buterin. Given the prevalence of AI in private business, its incorporation in courts and the legal system should be explored.

Unlike the U.S., China has no strong resistance to equipping its courtrooms with algorithmic machines and has, in fact, welcomed them. China, with its large population and strong economy, has the potential to provide an important case study on the macro effects of implementing a judiciary which partly relies on computer automated decisions. Moreover,

---

28 For example, LawGeex claims its artificial intelligence is nine percent more accurate at finding risks in non-disclosure agreements compared to experienced lawyers. See AI vs. Lawyers: The Ultimate Showdown, LAWGEEX (Feb. 26, 2018), https://blog.lawgeex.com/ai-more-accurate-than-lawyers/#more-4058 [https://perma.cc/7274-2ZEE].
29 Robots in this article refer to computerized agents that can accomplish certain tasks intelligently.
30 Although there has been speculation that there may be a chief justice robot in the future, such speculations are intended as absurdities. See Sean Braswell, All Rise for Chief Justice Robot!, OZY (June 7, 2015), http://www.ozy.com/immodest-proposal/all-rise-for-chief-justice-robot/41131 [https://perma.cc/94EQ-4HDR].
31 Coglianese & Lehr, supra note 21, at 1152.
33 Kroll, et al., supra note 24, at 695–96. It is difficult to specify or calculate normative values in algorithms for machines to “understand” them.
34 Coglianese & Lehr, supra note 21, at 1152.
with the implementation of STCR, China’s case system is becoming more like the common law system, making the Chinese and American judicial systems more comparable than ever before. The STCR could be seen as a stricter form of the common law system by making precedents binding, since this leaves judges with less decision-making freedom. If the algorithms work satisfactorily in China, STCR may help shed light on how a classic common law system could be transformed through the use of technology like AI.

Accordingly, Part II of this article discusses the characteristics of China’s STCR and the system’s underlying rationale. This establishes the basis to compare STCR with common law systems in Part III. After concluding that STCR has the same central characteristics as a common law system, Part IV analyzes STCR as an experiment to integrate AI into the common law and how STCR’s AI differs from previous in-court machines and scientific instruments. Finally, Part V provides a taxonomy of AI applications in judicial tasks and analyzes how the possible substitution of human judges in certain categories of tasks may impact the systematic function of common law. Part VI of this article concludes by advocating for the application of AI in judicial decision making and calls on the judiciary worldwide to actively participate in the development of AI.

II. CHINA’S STCR SYSTEM: CHARACTERISTICS AND UNDERLYING RATIONALE

STCR represents a technological effort to massively overhaul certain aspects of the Chinese judicial system. This section begins by explaining some of the problems in the existing system that STCR seeks to alleviate. These problems include a combination of the lack of a case database, large amounts of case data, and individual judges’ resistance to change. This section then explains how STCR as a technology, and the procedures for its implementation, have sought to deal with these issues, taking account of both its advantages and disadvantages.

A. Establishing a Database of Judgments and Research Systems

The establishment of STCR is a holistic project involving the formation and coordination of multiple systems—the most important is the database system of Chinese judgments. Case reporter systems are fundamental because they record court case decisions, making later
reference possible and convenient. The new systems in China are similar to Westlaw and LexisNexis, which digitize American court decisions and provide powerful online research engines. Until recently, China, as a traditional statutory system, did not have a case reporter system, and Chinese courts did not publish their decisions for the general public. Now, under pressure from SPCC, Chinese courts have begun to publish their case decisions. SPCC established a uniform case decision website for individual courts nationwide to upload their judgments in a timely manner. While not all cases are publicly available, the national strategy on improving national governance has made large strides to improve the availability of published cases in the Internet era. The site already has more than sixty-six million publicly available judgments, most of which were decided between 2014 and 2019.

The utility of judgments uploaded by courts is sub-optimal if they are not organized and indexed into a powerful research toolkit. According to the annual work reports, China’s courts decide more than twenty million cases each year. Even if a frontline judge in a district court only looks at prior decisions within his or her own court system, there are, on average, more than 30,000 cases made by his or her own court, 40,000 cases by his or her appellate court, 100,000 cases by the high court in his or her province, and 110,000 cases from SPCC during the last five years. In order to utilize the new database of judgments, public-private partnerships were established in which SPCC and Supreme People’s Procuratorate of China provide data to authorized private companies—

---

39 Id.
40 For the annual work reports of the courts, please see SPCC’s website: www.court.gov.cn (last visited Apr. 17, 2019).
41 A judge who decides cases, as compared to judges with more administrative roles.
42 These are simple calculations based on the annual work reports of the courts. Because China’s society and law are still changing quickly and courts primarily began publishing judgments in 2013, frontline judges normally refer to cases made within the last five years.
43 Although more than forty million case decisions are publicly available on SPCC’s case website, many decisions are still not online. (China’s courts decide more than twenty million cases each year.) However, SPCC and SPPC have internal case systems that have all of the case decisions as well as the relevant case materials, including complaints, legal proceeding records, and internally-submitted case closure reports where judges summarize their thoughts and concerns. The SPCC and SPPC provide technology companies with conditional access to these internal databases, so they can train machines
such as ZhiShen and FaXin—entrusting them with the development of software systems specifically for courts to make the intelligent analysis of the judgments possible.\textsuperscript{44} These new technology companies paved the way for full implementation of STCR by conducting the research necessary to make this plethora of judgments available.\textsuperscript{45} In just a few years, China has used these technological advances to establish and index its database of millions of judgments. Following the national “Internet plus action” initiative, keyword research was upgraded to natural language processing.\textsuperscript{46} Establishing these search programs, however, is just a small part of the overall goals of STCR.

B. Establishing a Legal System to Require the Use of the Judgments Database

Despite the availability of the case database and search programs, Chinese judges, at first, did not readily refer to STCR’s collection of prior decisions when making their own judgments. China’s judges hesitated to welcome STCR for several reasons. First, they are traditionally statutory judges and are used to applying only statutes, not cases.\textsuperscript{47} Therefore, significant effort is required for over 110,000 judges to change their decision-making habits.\textsuperscript{48} Second, judges may lack the skills and training to compare cases, find similar fact patterns, and summarize case rules since these tasks are quite different from applying predetermined statutory
to learn from the cases. See Interview with Gridsum Company Officials Miao Rui, Ren Jiao, and Li Bin, in Beijing, China (Mar. 2018); Interviews with Judges from No. 3 Intermediate Court of Beijing, China (Mar. 2018); Interviews with Prosecutors at Zhejiang Provincial Procuratorate (Apr. 2018); Interviews with Software Designers and Programmers for Zhejiang Procuratorates (Apr. 2018); Interviews with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).

\textsuperscript{44} Xiaohui, supra note 8.
\textsuperscript{45} Key word legal research has been provided by private companies like Beida Fabao. See PKULAW.CN, www.pkulaw.cn [https://perma.cc/A2HK-A5TD].
\textsuperscript{47} Jia, supra note 2, at 2230–31.
rules.\(^{49}\) Third, according to the annual work reports of China’s courts, an average frontline judge has to decide more than two hundred cases each year. With such a heavy workload, requiring judges to find prior analogous cases and compare them to the case at hand adds an additional step in their already over-burdened decision-making process.\(^{50}\) Fourth, judges’ discretion shrinks under the STCR system, since it requires them to follow prior analogous decisions while disallowing the judges to make law like common law judges.

Facing these obstacles, the introduction of the database system required additional procedural and substantive measures to support its success. Procedurally, according to SPCC’s *Implementation Opinions on Accountability*, after a trial ends and before a decision is issued, the judge in charge of a case—called the undertaking judge (cheng ban fa guan, 承办法官), similar to the role of the chief judge in U.S. court—needs to research and examine prior analogous decisions, prepare a report of the research and analysis results, and post it on the internal case work system where other judges in the collegial panel, superior judges, and court leadership can review it.\(^{51}\) The undertaking judge also must prepare a draft opinion and recommend whether to follow, distinguish, or revise a prior analogous case decision.\(^{52}\) Before issuing the opinion, the undertaking judge must confer with other judges on the panel about the draft opinion.\(^{53}\) The clerk of the panel records this discussion and posts it to the case system for superior judges and court leadership to review.\(^{54}\) Substantively, with the report and the draft opinion at hand, if a judge wants to issue a decision that deviates from prior analogous decisions, he or she must apply for a conference of judges to be held.\(^{55}\) The judge then needs to explain his or her reasoning to the conference of judges, and the group


\(^{50}\) In the comment area in WeChat under the news about SPCC’s issuance of the *Implementation Opinions on Accountability*, many judges left complaints about the increased workload caused by the new requirements of having to follow same-type cases. They also expressed that they were fortunate that such opinions are currently only about SPCC judges, but they also were worried that in the near future, such requirements may be implemented nationwide.

\(^{51}\) Opinions of the Supreme People’s Court on the Implementation of the Judicial Accountability System, art. 39.

\(^{52}\) *Id.* art. 42–43.

\(^{53}\) *Id.* art. 44.

\(^{54}\) *Id.* art. 45.

\(^{55}\) *Id.* art. 15–16.
decides whether the deviation is establishing a new standard in a new type of case or is revising an old standard already established by prior cases.\textsuperscript{56} If it is the former, the outcome is subject to the approval of the conference of professional judges. If it is the latter, the revision to the old standard must be approved by the adjudication committee of the court.\textsuperscript{57} Court and departmental leadership also can initiate the aforementioned procedures if they find that the draft opinion deviates from the research report, which operates as a supervisory tool.\textsuperscript{58}

C. Underlying Motivations that Shape the Design of STCR

Although the legal system described above appears to have sufficient mechanisms in place to require judges to follow precedents, these procedural steps still must be actually implemented. China has been known to have a significant gap between its law on the books and law as it is actually implemented—"law in action."\textsuperscript{59} The STCR was developed under the background of China’s leaders pushing the development of AI technologies, but whether STCR will only be symbolic or whether it will be fully implemented is another question. If STCR is a symbol to cater to political leadership, and important parties affected by STCR do not sincerely embrace it, STCR may become only a decoration. Underlying reasons and incentives for creating STCR will significantly shape the operations of STCR. Facing resistance from frontline judges who are end users, STCR relies heavily upon the supervision of superior judges and court leadership. But why would traditionally statutory superior judges and court leadership welcome STCR when these key players have similar capacities and decision-making habits as frontline judges and thus similar resistance to STCR implementation?

This leads to one of STCR’s essential functions: supervising frontline judges and their judicial decision-making. Previous literature disclosed that China’s courts have a “black hole” of responsibility—meaning that the judge who wrote and issued an opinion may not have been the true decision maker in the case. This is because, until recently, opinions had to be approved by superior judges who frequently revised the

\textsuperscript{56} Id. art. 40(2)-(3).
\textsuperscript{57} Id. art. 17–19.
\textsuperscript{58} Id. art. 64(3).
opinion during this review process. Further, the head of the court\(^\text{60}\) could be sheltered by the adjudication committee, since the head substantially influences the committee.\(^\text{61}\) In targeting this problem, recent judicial reforms aim to make the judges who actually try the case the true decision maker so that only judges on the panel can influence the decision.\(^\text{62}\) However, judicial independence alone does not guarantee good, reasonable, and fair case decisions—or enhance judicial integrity. In a typical Chinese district court, fewer than fifty percent of the judges have a bachelor’s degree or higher degree in law, and fewer than thirty percent have passed the national bar exam.\(^\text{63}\) Without supervision from superior judges or adjudication committees, frontline judges lacking adequate legal training may be persuaded or captured by powerful agencies, irrational popular pressures, or wealthy litigants.

Thus, along with increasing judicial independence, a judicial accountability system that supervises judges and makes them more accountable in accordance with SPCC’s two opinions on accountability is necessary. The two-sided reform to increase judicial independence while also creating more indirect control by superior judges is carried out according to the principles set by the Central Committee of the Communist Party of China in 2013, which states: “Let the trying judge decide, and let the decider take responsibility.”\(^\text{64}\) Superior judges and court leaders are now motivated to promote STCR as the guiding system to restrict judicial discretion without direct intervention after losing the ability to directly influence case decisions.

---

\(^{60}\) This is a judge with an administrative role in addition to an adjudicatory one.


\(^{62}\) Such reforms include decreasing the intervention by court leaders and adjudication committees in specific cases, improving the collegial panel trial system and building a more professional judge system through selecting “post judges” (员额法官) who should be more capable and prepared to independently make judicial decisions. See generally CHINA CHANGAN NETWORK, http://www.chinapeace.gov.cn/node_25595.htm [https://perma.cc/2SFM-7LNL].

\(^{63}\) Linlong Sang (桑林龙), Research Upon the Education and Training of Local Judiciary (基层法官队伍建设与培养的研究), 11 LEGAL SYS. & SOC’Y (法制与社会) 155 (2017).

\(^{64}\) Point 33, The Decision of the Party Center on Some Important Issues of the Comprehensive Deepening of Reform, passed by the third plenum of the 18th session of central committee of CPC. See Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform, PEOPLE’S NETWORK (Nov. 16, 2013, 2:40 AM), http://politics.people.com.cn/n/2013/1116/c1001-23560979.html [https://perma.cc/DW7X-V7X7].
Successful implementation of STCR also requires the support of frontline judges who face high caseloads and increasing judicial accountability from the public. The focus on precedent in STCR will likely appeal to these judges because it will limit the occurrence of unconstrained judicial decision-making and produce more consistent outcomes. However, STCR’s implementation will require additional steps from judges when making decisions, which may slow down the judicial process. Both frontline judges and court leaders are familiar with the decision-making process in a statutory system. Judges will need training to employ common law-like principles within the framework of China’s statutory system. Given this difficult transition, the implementation of a highly intelligent software system that generates efficient and meaningful guidance is critical to alleviating resistance from frontline judges.

Article 8 of the *Opinions on Accountability* explicitly indicate that STCR shall be utilized to unify “judicial measurement.”

The Chinese legal concept of “judicial measurement” (cai pan chi du, 裁判尺度) does not have an exact analog in American legal theory. The concept of judicial measurement most closely resembles that of judicial interpretation and is frequently used to describe the discretion judges use in calculating specific penalties, imprisonment length, and compensation amounts when applying statutes. Recently, SPCC has frequently used judicial measurement in its opinions that recognize new types of rights and liabilities in intellectual property, environmental, and financial laws.

The scope of STCR could be narrowed to include the types of decision-making generally recognized by SPCC as falling within the meaning of judicial measurement, but this category is largely undefined. Under this implementation of STCR, judges would look to prior decisions only in areas of the law where statutes are unclear and judicial discretion is broad. Among the thousands of opinions issued by SPCC, only forty-five have included judicial measurement, and they have covered specific legal issues such as compensation for (and recognition of) work-related injuries, maritime disputes, and sentences for certain crimes. Where the statutory laws are not comprehensive, STCR would fill in the gaps and make judicial interpretation more consistent and standardized. Where the

---

65 Jia, *supra* note 2, at 2230.
66 More than one-third of the forty-five judicial instructions by SPCC have used the term “judicial measurement” in referencing new types of intellectual property, environmental, and financial law issues after 2011. *Id.*
67 The research was done on Mar. 9, 2018, through Beida Fabao’s database, available at PKULAW.CN, www.pkulaw.cn [https://perma.cc/A2HK-A5TD].
statutory laws are out-of-date, it is possible that STCR may help recognize new rights to satisfy the changing technology. Under STCR, the rationales for certain statutorily-recognized legal concepts that influence decision-making, and the weight of such factors, would be recognized by disparate lower courts in a more consistent manner. Limiting the scope of STCR in this way would likely make it easier for statutory judges to implement decisions based on precedent.

D. Same-Type Cases

A remaining essential component of STCR is the concept of same-type cases. SPCC’s *Opinions on Accountability* do not provide a clear definition of “same-type cases”—nor is there any other judicial interpretation or law with this information. However, several bases for classification exist, including whether the case involves the application of the same statutory article or the same cause of action.

“Guiding cases” and “typical cases” are cases SPCC has deemed to have guiding effects on same-type cases and can help illustrate what are deemed to be same-type cases by SPCC.68 China’s original statutory system provides a basis for identifying same-type cases.69 Generally, cases that involve the same cause of action are considered of the same-type in contract, tort, and administrative law (e.g., there is a category of cases that interprets what constitutes “potential deficiency undiscoverable by reasonable cautiousness” to exempt carriers from responsibility under Article 51 of the Maritime Commercial Law).70 Two cases do not constitute same-type cases when they merely analyze the same statute, policy, or general legal principle. For example, all contractual issues involve the good faith principle in some form, but all contractual cases are not same-type cases. Another example is the category of cases that resolve procedural issues for prosecutors litigating public interest actions in

---

environmental pollution cases. In criminal law, cases prosecuted under the same crimes are considered to be the same-type.

E. Progress in the Implementations of STCR

STCR includes an enormous case database that instantly updates as judgments are handed down. It has highly intelligent research systems that can make recommendations for same-type cases and generate reports and statistical analyses of these cases. The system also permits senior judges and supervisory leaders to ensure that judges follow similar prior cases. STCR’s implementation plan accounts for supervision and efficiency demands, concerns regarding the difficulty of mastering common law-style legal thinking, and the possibility of an increased case workload. This detailed implementation plan suggests the STCR will be more than political decoration.

STCR relies heavily on these intelligent software systems—such as those that efficiently generate meaningful research reports that identify same-type cases—to alleviate the concerns given by frontline judges. The success of the intelligent software systems is essential for the effective application of STCR. China’s national strategy calls for huge investment in big data and artificial intelligence. This investment includes several projects to incorporate AI technologies in courtrooms and in the work of prosecutors and police, which collectively have financial budgets in the billions of yuan and have the support of the Ministry of Science and Technology. As a result, several technology companies have been incentivized to develop customized systems for these needs. For example, FaXin, developed by Gridsum, claims that it can recommend same-type

__Case No. 9 in SPCC’s Ten Model Cases in Environmental Public Interest Litigations in 2017.__

__Although there is no rule expressly stating that same crime cases are considered to be same-type cases, all databases of judgments in China have categorized criminal cases according to the types of crime a case concerns. See the national website for courts to upload judgments at: http://wenshu.court.gov.cn/ [https://perma.cc/7KLM-TJYZ].__

cases, produce statistical analyses, and generate some parts of the judgments for twenty-six crimes within China’s criminal law codes and twenty-one causes of action in civil cases, covering over eighty percent of all cases. Additional models are also being constructed. Approximately sixty-six percent of all courts in China have established systems that can automatically extract the causes of action from complaints in civil and administrative cases; fifty-two percent can automate the production of facts and reasons in civil and administrative cases; sixty-seven percent can automate the information for defendants in criminal cases; thirty-six percent can support automatic extraction of statutory and discretionary sentencing factors in criminal cases; thirty-eight percent can support intelligent recommendations of laws and judicial interpretations regarding sentencing regulations; and thirty-two percent can provide the range of sentences for reference, all based on data analysis of prior analogous decisions.

III. A COMPARATIVE ANALYSIS OF STCR AND THE COMMON LAW

In evaluating whether STCR will make China’s system more like a common law system, one crucial inquiry is whether STCR establishes the key characteristics of a common law system. As such, this section explains the central characteristics of a common law system and compares STCR to the common law.

A. Stare Decisis as the Central Characteristic of Common Law

“Civil law” and “common law” are frequently used as taxonomies to analyze legal systems in different countries and enable communication between disparate legal societies. Although the systems have some convergence, civil law and common law each possess distinct features, which are valuable tools in comparing the virtues of the two legal systems. The Chinese legal system is a variant of the European civil law

74 Interview with Gridsum Department Director Miao Rui, in Beijing, China (Feb. 2018).
75 Id.
76 LI LIN & TIAN HE, ANNUAL REPORT ON INFORMATIZATION OF CHINESE COURTS 46–47 (2nd ed. 2018).
system, with a similar focus on statutory law. Yet, China’s establishment of STCR brings the country closer to a common law system and may be part of a broader trend of global legal convergence.

Common law evolved differently in different countries; for example, while the U.S. legal system is grounded in common law, it is also heavily reliant on statutes. Though transnational, common law has “distinct local expressions” and can “shift over time, context and place.” The concept of common law may refer not only to the substance of the common law doctrines in anchoring statutory rules and constitutional principles but also refers to the methods of deciding cases with “an inherent commitment to rationality and equality through adherence to precedents.” Thus, when arguing that STCR is a common law model in China, this article approaches common law from an institutional perspective (i.e., the functional form of the common law system generally) rather than discussing the substantive content of common law doctrines.

Although common law systems may vary in some respects, all have a central characteristic: the principle of *stare decisis*. *Stare decisis* has three inherent parts. First, all published prior decisions are precedential unless specified otherwise in the judgment. Second, judges must follow precedents if their cases are deemed similar. Third, judges have authority to decide their cases and may decide whether their cases are like—or unlike—precedent. Several theories regarding the superiority of common law over civil law are based on this basic theoretical functional difference, i.e. common law has *stare decisis* while civil law does not. Other distinct features of common law—such as judicial independence and judicial power—are not as intrinsic to common law as *stare decisis*, although the strength of the association is explored further below. Therefore, the next section begins by comparing STCR and the common

---

83 *Id.* at 736.
85 Cross, *supra* note 78.
86 *Id.*
law in light of the *stare decisis* principle. It then discusses several other derivative features and whether they are absent or present in STCR.

B. Comparing STCR and *Stare Decisis*

STCR’s goals demonstrate that it incorporates the principle of *stare decisis*. While there are differences between common law *stare decisis* and STCR’s incorporation of the principle, ultimately STCR has three features that are similar to those of *stare decisis*.

1. **Past Cases Are Precedential Under STCR**

All prior case decisions are in the internal database of judgments available for research (although a significant number of judgments are missing from SPCC’s publicly available case website). While the data judges can directly access depends on their authority, the intelligent research systems are researching and “learning” from all judgments. Unlike guiding cases that are heavily edited with holdings, facts, and reasoning rewritten by SPCC through centralized judicial policymaking, the judgments in the database are the originals as issued by the judges without further editing. This also distinguishes STCR from case law systems in other civil law jurisdictions, which restrict which cases constitute precedent based on the doctrine of *jurisprudence constante* or top-down approaches.

2. **Cases Are Binding on Similar Cases Under STCR**

Judges must follow prior analogous decisions. STCR’s design provides procedural and substantive safeguards and incentives to ensure judges refer to prior analogous decisions made by their own courts, the

---

87 Although the website has more than forty million judgments, considering that Chinese courts have concluded more than eighty-eight million cases during the last five years, a significant part of the judgments are still missing from the website. *See Highlights of Supreme People’s Court Work Report*, SUP. PEOPLE’S CT. PEOPLE’S REPUBLIC CHINA (Mar. 12, 2019), http://english.court.gov.cn/2019-03/12/content_37449108.htm (last visited Apr. 17, 2019); LIn & He, *supra* note 76, at 35–37.


superior courts, or SPCC. If judges do not follow prior analogous
decisions, they must distinguish their cases from previous ones. To
overturn a previous decision, the judge needs to persuade a majority of
judges in the conference of professional judges or pass the adjudicatory
committee of the court.\textsuperscript{90} Although neither China’s legislature nor SPCC
recognize prior case decisions as a source of law in a formal sense, they do
not dismiss the authority of such sources of law. Instead of calling prior
decisions “law” or “precedent”—which has a more ideological meaning—
SPCC uses the words “law of cases” (cai pan gui lv, 裁判规律) to describe
same-type prior decisions.\textsuperscript{91} This phrasing implies that SPCC holds that
same-type prior decisions represent general prior court wisdom and should
be respected by lower courts in similar proceedings. Moreover, with
STCR’s design, prior analogous decisions, in reality, have legal binding
force on similar facts. This differs from guiding cases that have only
influential or referential effects because they do not have the same
restrictive design features of STCR. Since courts cannot cite guiding cases
as a legal basis for judgments, and appellate courts cannot overrule a trial
court decision for not following them, guiding cases cannot achieve
binding force. Empirical research shows that in reality, some courts have
explicitly declined the authority of guiding cases or simply ignored them.\textsuperscript{92}

SPCC refuses to formally pronounce prior decisions as precedents
for two reasons. First, since China has a statutory system, judges do not
recognize cases as a source of law in a formal sense. This reason is why
SPCC has failed to formally confirm the legal status of guiding cases after
decades of effort.\textsuperscript{93} SPCC’s position that guiding cases are influential or
referential is already controversial. Many opponents argue that cases
traditionally are not recognized as law: SPCC has no authority to make
law—even if guiding cases are heavily edited and abstracted through a
centralized process. Making case law contradicts China’s political
structure.\textsuperscript{94} Of note, the word “precedent” has an ideological meaning and
is generally deemed congruent with judicial lawmaking, separation of

\textsuperscript{90} Opinions of the Supreme People's Court on the Implementation of the Judicial
Accountability System, art. 40(3).
\textsuperscript{91} Id. art. 1; Opinions of the Supreme People's Court on the Judicial Accountability
System, art. 12.
\textsuperscript{92} Deng, supra note 68.
\textsuperscript{93} Jia, supra note 2, at 2231.
\textsuperscript{94} An Xuemei (安雪梅), The Limits in Framing Law of Guiding Cases (指导性案例的法律
powers, and democratic Western-style countries. Claiming that prior decisions are not precedents helps circumvent these sensitive, difficult disputes. Using the wording “same-type cases” ornaments prior analogous decisions with good technological packaging—consistent with the national strategy by building a legal system with Chinese characteristics, thereby making the system more acceptable in China’s legal society.

The second reason that prior decisions are not referred to as precedent is that, although they are binding, prior decisions are different from statutory laws in that statutes provide more generalized legal concepts and the elements of legal relationships. In contrast, case decisions are factually based and, using a series of similar cases, filters more concrete factors that could be leveraged to have legal effect or constitute a legal doctrine. For example, China’s criminal statute states that the intent to kill is required to find murder. SPCC further issued a judicial interpretation clarifying that an intent to kill could be found even if the murder is a result of a long-time, serious domestic violence. Using this interpretation, cases can provide more detail surrounding the concepts of “intent” or “domestic violence” with the facts of the cases. The facts and their values and influences shift over cases, time, and place. Because China’s legal society has historically recognized only statutes as sources of law, China has considered sources of law to necessarily be general and abstract; cases—even if they become binding in STCR—are fact-based and concrete, and so China’s legal society struggles to accept cases as a source of law.

3. Judges Determine Similarities Between Current and Past Cases Under STCR

Prior to STCR, China’s judges were known to lack judicial independence and held limited judicial power. This view needs to be reevaluated because the ongoing judicial reforms have sought to enhance judicial independence through the establishment of STCR, the elimination of superior judges directly approving opinions, and other judicial

95 Crimes of Infringing Upon the Rights of the Person and the Democratic Rights of Citizens, P.R.C. Laws (China), art. 232.
97 Elen, supra note 79.
reforms.\textsuperscript{98} However, several studies have noted strong resistance to advancing these reforms—especially due to the contradiction between judicial independence and upholding party dictatorship. Under the current design, even if reforms are successfully implemented, the judiciary may gain enhanced independence only from local party/government interference, but they can never be independent of party leadership. STCR may provide judicial independence similar to common law with respect to local affairs but not in regard to the party or politically sensitive cases. However, judicial independence may not be a necessary component of common law, and so a common law system may be able to function without it\textsuperscript{99} because precedents do not rely on judicial independence to be binding and functional. Thus, it remains unclear whether precedent and judicial independence are intrinsically associated.\textsuperscript{100} Other political or legal structural factors also influence judicial independence, such as democracy and the non-bureaucratization of court systems.\textsuperscript{101} Yet, China may be able to establish a common law system using STCR with only a semi-independent judiciary. Recognition by society that these decisions are binding on its behavior may be enough for STCR to have common law legitimacy. It remains to be seen whether and how STCR will function if judicial independence does not increase, and such results will surely contribute to the understanding of the relationship between judicial independence and common law.

Separate from the idea of judicial independence, the concept of a relatively strong judicial power is deemed more intrinsically related to common law. "By deciding cases and establishing precedents that are discretionary with the courts," judges in common law may "exercise greater judicial policymaking power."\textsuperscript{102} Similarly, with the implementation of STCR, judicial power in China will expand, which makes China’s case system more like common law. Cases decided by ordinary judges would have binding force, and ordinary judges would have stronger power in deciding cases with ongoing reforms. Judges


\textsuperscript{100} Cross, \textit{supra} note 78, at 56.


\textsuperscript{102} Cross, \textit{supra} note 78, at 54.
would be bound by other judges’ decisions, i.e. their interpretations of law. Although STCR courts should interpret and apply statutory rules and establish judicial standards, which is unlike common law judges overturning laws for “moral reasoning” or equity, China’s judges may overrule some statutory rules that contradict higher-level statutory rules or principles (such as good faith in some limited situations), and they may fill in statutory gaps or establish judicial standards in new types of cases where the legislature acts too slowly. This potential rise in the judicial power of judges in China may further STCR’s ability to function like a typical common law system.

Chinese judges are entrusted by the constitution to apply law to concrete cases and are authorized to decide cases. Judges also may decide which prior decisions are similar to the pending cases. This function is similar to the concept of judicial power in common law. Although STCR search programs may automatically recommend same-type cases, judges can choose to accept or decline these recommendations. Additionally, besides these automatic results, judges themselves may search using keyword search or other methods to find their own similar cases. Thus, STCR’s programs still need the guidance of human judges.

C. STCR and Other Distinct Features of Common Law

Stare decisis can’t explain all the differences between common law and civil law. Other distinct features include judge-made law, retroactive lawmaking, and the ability of judges to overrule existing law. Although these features have been historically more incidental and less intrinsic than precedents, they are considered essential to judicial lawmaking in common law. Considering these features, it would seem that STCR is potentially in opposition to the common law system. In China, only the legislature is authorized to make new laws, or change existing laws. With statutes in

103 Id.
104 Deng, supra note 68.
105 Interview with Gridsum Company Officials Miao Rui, Ren Jiao, and Li Bin, in Beijing, China (Mar. 2018). Judges could manually add or delete the recommended cases by changing the elements of the pending case found by the machine from the legal documents of the pending case. The machine considers cases analogous if they contain same case elements. Moreover, the machine is trained by supervised learning of which human intervention is necessary. Unsupervised machine-learning will be difficult to achieve in the near future.
107 Id.
hand, judges proactively—rather than retroactively—apply the laws to cases. The cases in STCR’s database were decided according to a cited statute and help to clarify the meaning of these statutes. Although common law jurisdictions have statutes, and many common law doctrines have been codified, those statutes are taken as amendments to common law and are interpreted “in light of the stage reached at that moment in the judicial development of common law.” For example, even if a statute makes no explicit requirement of criminal intent, common law judges can add such a requirement based on common law doctrines. Chinese judges cannot add any requirement that is not already in the statute.

On further inspection, however, the difference between common law and STCR may not be so significant. First, judges in China are prohibited from making law, while judges in common law systems face similar challenges in justifying their perceived lawmaking power. One relatively sound justification is that common law judges do not make law, but instead, find law that grows naturally from fact patterns, situational sense, or “social propositions” spoken by judges. Judges have restraints from their professional training and law school education, as well as from adversarial trials, procedural requirements, bar associations, reasoned open judgments, and other systems, and these institutional factors require judges to make law in a predictable, consistent way. Similarly, in STCR, the binding force of prior analogous case decisions is justified by “the law of cases” reflected therein. The common fact patterns in these cases require any following cases to be decided similarly so that the same justice realized in earlier decisions can be similarly upheld in following cases. This is the same major justification commonly advanced for a judicial lawmaking power. Noting these similar justifications, it appears the power to make precedents in common law and the judicial power to decide cases that bind subsequent cases in STCR may in fact not be so different after all.

Second, the scope of judicial power in common law and in STCR may also be comparable. Although common law jurisdictions have a body

110 Llewellyn, supra note 32, at 73.
111 Eisenberg, supra note 49, at 14–42.
112 Llewellyn, supra note 32, at 15–16.
113 Opinions of the Supreme People's Court on the Implementation of the Judicial Accountability System, art. 1; Opinions of the Supreme People's Court on the Judicial Accountability System, art. 12.
of common law doctrines for judges to use to either decide cases directly, or to modify or overrule statutory rules, such common law doctrines have been heavily codified.114 Lacking a body of common law doctrine, China has published additional statutes of doctrines similar to common law so that judges have statutory laws to instruct their decision-making.115 This is not to say that China has similar rules to American common law, as the content of specific rules are subject to many factors (e.g., cultural, situational, historical, and geographical). But these additional statutes are functionally equivalent to common law doctrines. When required by justice, these additional statutes allow judges in China to modify or restrain other statutes. Because there are not enough statutes restraining judicial decision-making, some people have criticized China’s judges for having overly broad discretion.116 Unchecked judicial discretion is a common problem in civil law countries that provides motivation for the establishment of case law systems, like the guiding case system in China and the adjudications compiled by Taiwan’s Highest Court to bind lower courts.117

Common law statutes are also unlike civil law statutes because they do not have immutable authority.118 Some literature already notes that common law judges have the power to decide whether to extend, revise, or reject written law to maintain congruence with the social propositions read in precedent.119 In other words, judges can revise both written law and uncodified common law doctrines in deciding cases. This incompleteness—or retroactive lawmaking and moral reasoning—has distinguished common law from civil law and enabled judges to expand their powers.120

However, statutory judges in China are also influenced by social propositions, which are frequently referred to as “sense” (ren qing, 人情).

115 These include the good-faith principle, the general provisions regarding criminal intent, and criminal responsibility in China’s criminal law, along with the general provisions in China’s private law and numerous judicial interpretations.
117 Jia, supra note 2, at 2231.
119 EISENBERG, supra note 49, at 140–60.
120 Schauer, supra note 49, at 464.
They also have the duty to promote justice in specific cases. A major theme for establishing STCR and implementing judicial reform is to enhance a public feeling of justice in every case. An essential source of the public’s perception of justice comes from consistent case decisions—such as following prior analogous decisions—and these decisions drive STCR. And, although common law judges may revise the law, it does not mean that the laws—or “doctrinal propositions”122—have no normative value and are only a servant to social propositions. A positivist theory insists that law consists of a set of discrete rules that are divergent from open-ended social norms, which constitutes legal autonomy.123 And so, in common law jurisdictions the law can only be revised under certain conditions, without which the law is immutable. Thus, the statutes in civil law may not be so immutable or complete, and the precedents in common law may not be so revisable or incomplete. In summary, while STCR and the common law system are somewhat different, their differences may not be so great.

D. Evaluating Common Law’s Normative Values and STCR

As the previous discussion highlights, STCR is more similar to common law than other case law systems in civil law countries. A central distinction is the authority to make cases binding. In other civil law countries cases must be selected—or edited—by either the highest court or a specially authorized court to become binding.124 This is similar to how China’s guiding-case system worked. But under STCR, all original judgments are generally binding without filtering by the highest court. Similar to common law, this principal distinction entrusts the power to make binding decisions to judges and not a centralized bureaucracy. The underlying forces of precedent—logical reasoning, the requirement of consistency in legal systems, customs in the community, or a sense of the situation found (or created) by judges125—begins at the bottom, as

121 See Xi Jinping, Strive to Let the People Feel Fair and Justice in Every Judicial Case, PEOPLE’S NETWORK (Feb. 24, 2013), http://politics.people.com.cn/n/2013/0224/c70731-20581921.html [https://perma.cc/6ZXL-RNBV].
122 EISENBERG, supra note 49, at 1.
124 Jia, supra note 2, at 2230-31.
125 The difference between law being “found” and “created” by judges depends on whether we believe that there is immanent law in every case that can be found by every judge or that the law in some cases is created by judges either because there is no such immanent law in every case or because judges are limited as humans and may miss such
opposed to authorization from the top. Similarly, prior decisions in STCR achieve binding force because they represent “the law of cases,” which also comes from the bottom. Consequently, this leads to a more empowered judiciary and a bottom-up channel for the formation of rules.

Despite these similarities with common law jurisdictions, some differences remain. In China, prior decisions are not a source of law in a formal sense. Judges are subject to bureaucratic control and cannot overrule statutes. But from a quantitative perspective, there may only be trivial differences between Chinese and common law judges’ lawmaking power. Statutes are not wholly immutable, and in certain instances, Chinese judges can let social values prevail and use judicial creativity with some “leeway” in applying statutes.\(^{126}\) At the same time, there have only been a few cases where common law judges have truly acted as legislators.\(^{127}\) Even if they want to make law and consider social values in every case, because of the belief in legal autonomy from social values, only a few situations can actually create new laws: the social value under consideration must be so important that it supersedes laws.\(^{128}\)

From a qualitative perspective, the differences between STCR and common law can be significant. In those few cases where common law judges behave as legislators, they make groundbreaking decisions that are cited repeatedly to shape the law,\(^{129}\) and the judge is lauded, even to the point of becoming a cultural hero.\(^{130}\) Under STCR it is reasonably foreseeable that lower-level courts’ decisions will attract more attention, and they will use this opportunity to play a more important role in shaping the law.

However, the expansion of judicial power is still conditioned on upholding the strength of party leadership.\(^{131}\) STCR must fit into China’s political structure to survive. An essential normative commitment of common law is democracy, where common law works to empower judges, enhance judicial independence, and strengthen the separation of powers.\(^{132}\) As discussed infra Section II, there are two essential missions of STCR: restraining judicial discretion and enabling court leaders to supervise

\(^{126}\) Deng, supra note 68.


\(^{129}\) Clark & Trubek, supra note 125, at 256.

\(^{130}\) Cross, supra note 78, at 53.

\(^{131}\) Elen, supra note 79.

\(^{132}\) Id.
judicial decision-making. Although the ability to make binding case decisions can empower judges, prior decisions can also work as judicial restraints. This constitutes part of the legitimate control in judicial lawmaking and serves as a reason to establish case law in civil law jurisdictions.\footnote{Jia, supra note 2, at 2231–33.} STCR further expands the restraining function of precedents as a supervisory tool. Similar to other civil law jurisdictions, judges are essentially part of the civil service under the control of party committees in China.\footnote{Cross, supra note 78, at 4.} Moreover, judges are subject to internal bureaucratic control through evaluation and promotion.\footnote{XIN HE, JUDICIAL INDEPENDENCE IN CHINA: LESSONS FOR GLOBAL RULE OF LAW PROMOTION 180 (Randall Peerenboom ed., 2010).} Some of China’s other ongoing judicial reforms—such as improving the juror system and making trials more adversarial—have incorporated systems frequently seen in common law countries. These reforms protect judicial independence from intervention by local authorities but not from the party center.

When evaluating STCR’s shift towards a common law system, the fact that STCR is subject to the party leadership’s supervision should be considered. STCR generally has a central institutional shape similar to that of common law (i.e., reliance on precedent), but, unlike common law, STCR does not have a normative commitment to democracy and independence. The evaluation depends upon how the common law system is defined. If \textit{stare decisis} is deemed to have value independent of democracy in the function of the common law and is a determinative factor in deciding whether a case system is a type of common law system, then STCR can be seen as a type of common law with different political commitments. But, if democratic commitments are intrinsic to the function of common law, without which a \textit{stare decisis} system has no essence of common law, STCR may not be considered a kind of common law. Under the latter definition, the normative value of the common law is viewed as more foundational than its mere external form in upholding \textit{stare decisis}.

This article argues that it is better to identify common law through its adherence to \textit{stare decisis}, rather than any political commitments. \textit{Stare decisis} has an essential and independent value to common law and cannot be replaced by analogous judicial functions. It is thus necessary to preserve the \textit{stare decisis} component of common law; otherwise, a common law system cannot be distinguished from the case law in a civil
law system. Since *stare decisis* stands as the most significant characteristic of common law, we may take *stare decisis* as intrinsic and integral to the formation of common law. If this is acceptable, then China’s STCR is an example of common law, not functioning to advance democracy, but to strengthen centralized control over judges.

However, STCR does not necessarily lead to the negation of the common law’s virtues in advancing democracy and liberty. Whether an institution is morally neutral or has some normative commitments is another question.

IV. STCR: “INTELLIGENTIZING” THE COMMON LAW SYSTEM

Having established the structural organizations of STCR, this section discusses the implementation of STCR technologically. Additionally, this section explores some of the positive effects of intelligentizing common law, such as efficiency, and the negative consequences of the technology, such as the inability to detect factual errors and account for discretion.

A. The Intelligent Court System in China

As introduced in Part II, STCR is being implemented as part of a national strategy to intelligentize courts in order to relieve the burden of judges’ heavy case-loads, as well as to enhance the quality of judicial decision-making in every case. The significant number of prior judgments provides a sufficient data set to train a machine learning case system, and, for this reason, STCR was launched quickly and smoothly in a number of provinces. SPCC intentionally uses “类案” (lei an), referring to “similar cases,” and avoids the Chinese characters “案例”(lei an) and “判例,” (pan li), which have similar meaning to precedent, in order to distinguish STCR from common law. SPCC maintains that STCR is part of a broader program, in response to President Xi’s call to build systems, to erect judicial systems with Chinese characteristics. SPCC

---

136 See discussion supra Part II.
137 Conversely, the establishment of China’s guiding case system has taken decades, which makes only a few judgments binding. Even for these few guiding cases, their binding force is still in dispute. See Jia, supra note 2, at 2216–20.
138 President Xi has emphasized the confidence in China’s own systems and paths. Zhao Mingren, To Achieve the Chinese Dream, We Must Affirm "Three Self-Confidences," GUIZHOU DAILY (Nov. 28, 2013, 8:46 AM),
may sincerely believe that STCR is different from common law, since STCR is used to uphold party leadership rather than the separation of powers. But, as discussed above, both STCR and common law rely on precedents, even if STCR does not use that word. Thus, STCR, in some ways, may be seen as an experiment in intelligentizing common law.

The intelligent court system is part of the informatization of the Chinese courts, and it contains three key areas: intelligent case resolution, intelligent office administration, and intelligent personal evaluation.\footnote{139} Intelligent case resolution aims to move offline court-related activities to the online space, using AI to do judicial work to the greatest extent possible. These functions include opening a proceeding, serving electronic documents, submitting evidence, trying a case, and enforcing a judgment online, with AI assisting—or substituting for—humans.\footnote{140} STCR’s AI involves trying and deciding a case—the heart of a court’s work.

B. Intelligent Case-Deciding Programs

Currently, the AI programs meant to search and decide cases are unique to each province. To learn more about different STCR AI programs, the author interviewed officials in the sales, operations, and design departments of the companies that provide intelligent case-deciding programs to courts, such as Faxin and Zhishen.\footnote{141} The actual programs were observed in-person, and the author also interviewed judges and prosecutors who have used the programs during their daily work.\footnote{142}

Based on observations made in the field, several commonalities between each province’s programs can be deduced. Generally, the AI

\footnote{140} \textit{Id.} at 63.
\footnote{141} Interview with Gridsum Company Officials Miao Rui, Ren Jiao, and Li Bin, in Beijing, China (Mar. 2018).
\footnote{142} Interviews with Judges from No. 3 Intermediate Court of Beijing, China (Mar. 2018); Interviews and Observations with Prosecutors at Zhejiang Provincial Procuratorate (Apr. 2018); Interviews with Software Designers and Programmers for Zhejiang Procuratorates (Apr. 2018); Interviews and Observations with Prosecutors at Hangzhou City Procuratorate, in Hangzhou, China (Apr. 2018); Interviews and Field Observation with Judges at the Internet Court of Hangzhou, in Hangzhou, China (Apr. 2018); Interviews and Field Observation with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).}
programs include three components: the program recommending cases of the same type (same-type program), the program providing statistical analysis of prior analogous cases (prior-case analysis program), and the program generating judgments (judgment-generating program).\textsuperscript{143} All three subprograms are currently used in differing degrees based on the subject matter of the case. These subprograms are built using a similar series of algorithms to read the complaints, pleadings, and judgments from approximately forty million cases.

To build these programs, three steps must take place. First, a knowledge graph of factors is created for a computer to “understand” an uploaded document. These factors in the graph are sometimes more concrete than just legal elements, for example, a fact pattern that demonstrates a third degree disability or serious bodily harm to the victim. To create these graphs, experienced prosecutors and judges helped program manufacturers factorize each basic cause-of-action in civil law and each crime and built up the knowledge graph based on statutes, judicial interpretations, guiding cases, and their experience. Now, when a complaint is uploaded, it will be “factorized” with regard to this graph.\textsuperscript{144}

For each document that is uploaded, the graph tells the computer which factors were in the document and influenced the decision.

Second, algorithms inform the computers which linguistic expressions in the documents represent the existence of a factor. For example, if the document states “Defendant Jane Doe is nine-years old,” the computer will classify this as “Defendant under the age of criminal responsibility.” This second step is realized by a combination of technologies, one of which is natural language programming. Natural language programming is already capable of resolving certain linguistic statements, such as extracting the names of litigants, but some statements

\textsuperscript{143} Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).

Also note that the programs are not finalized, and even the finished components are continually being upgraded. Thus, programs may differ in detail and shift over time.

\textsuperscript{144} “Factorize” is a term of art—not by SPCC or governmental entities—and refers to a process that builds a legal knowledge graph for computers, using a decision tree, neural networks, or probabilistic graphical models. Interview with Gridsum Company Officials Miao Rui, Ren Jiao, and Li Bin, in Beijing, China (Mar. 2018); Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).
are not suitable for natural language programming to understand. This requires new algorithms—such as those involving certain Chinese characters or defining their properties and sequence to instruct the computer to find the related factor. If a factor has diversified linguistic expressions that are difficult to represent with several characters, or if such characters make the algorithms too complicated, supervised machine learning technology may be utilized. This enables the computer to self-study the rules of hundreds or thousands of documents that have been manually labeled as containing a certain factor. After self-learning, the computer can automatically factorize the factors from unlabeled documents. Unsupervised machine learning, which does not require humans to manually label documents in advance, is still unrealistic in analyzing the Chinese language. These technologies, thus, may be used together if it helps the computer return more accurate results and reduces the need for human work. The goal, ultimately, is increasing the accuracy and intelligentization of the process.

Third, after the machine has factorized the judgments, including the pending case documents, it examines the overlap between the factors and displays the most relevant prior cases. Generally, the more factors in common between a prior and pending case, the more analogous the two cases are. The same-type programs end their process here. Prior-case analysis programs, which are still in development, aim to provide statistical analyses based on recommended cases. Such analyses include calculating an average compensation amount, sentence range, or factor frequency of cases with selected factors. An increasing number of analyses, such as regression analysis used to evaluate the weight of certain factors on the final sentence, will be added as more statistical models are uploaded. Currently, because the final judgment and complaint contain much of the same information, judgment-generating programs assist by simply copying and pasting information from the complaint to the judgment. Such programs also incorporate the evidence list for judges to modify. Certain factors cause the program to rerun the first two steps to provide a list of possible issues in the case. Additionally, the program may insert relevant legal articles, penalties, or compensation suggestions based on the analyses of the most relevant prior cases. In the near future,

---

145 The development of natural language programming is still limited in analyzing relatively complicated language. Such limitations are more pronounced in understanding the Chinese language.

146 Unsupervised learning may be used to divide cases into broad categories by clustering, but it cannot realize sophisticated or subtle analyses.
judgment-generating programs aim to complete the reasoning and conclusion sections of the judgment using multiple machine learning algorithms, including the ones mentioned above, as well as unsupervised learning (e.g., clustering and representation learning), to analyze prior cases.\textsuperscript{147}

C. The Virtues of Intelligent Case-Deciding Programs

1. An Advanced Legal Researcher?

Computers have long played a role in courts by helping establish facts in legal disputes through machine identification of evidence\textsuperscript{148} and by assisting in the operation of the court, by recording trials and hearings, maintaining documents, and providing legal research and analyses. All of these things influence judicial decision-making to some extent—trial judges rely on machine evidence to decide the facts of cases, appellate judges review trial documents to determine issues, and judges generally refer to summaries of prior analogous cases prepared by clerks and litigants through computerized research. Thus, the intelligent court program may be nothing more than an advanced version of previous technology. Same-type programs can be viewed simply as advanced legal research engines similar to those used in other countries. For example, Westlaw has traditionally enabled diversified legal research methods, including the ability to search for cases by key words and natural language. It also has its own “key” system, which categorizes cases into issues summarized by its experts. Judges and clerks can find and review similar cases through these searches and select the cases they deem most relevant. Rather than require the user to search for analogous cases, same-type programs return results after the user uploads the complaint. Judges can then review and search the provided cases. These new programs may be more advanced than previous legal research programs like Westlaw in their accuracy, comprehensiveness, and simplicity.

But identifying relevant cases within a large database is never an easy task. This is why law schools require courses that teach legal research skills and why Westlaw and LexisNexis offer frequent training and online research assistance. To avoid missing relevant cases, research starts out

\textsuperscript{147} Interview with Gridsum Company Officials Miao Rui, Ren Jiao, and Li Bin, in Beijing, China (Mar. 2018).

\textsuperscript{148} Roth, supra note 27, at 2000–16.
broadly and gradually narrows. This requires researchers to use diversified expressions for a concept or to go through all possible key numbers in the key system (or similar systems). Legal research takes a lot of time and effort to complete—even for an experienced research assistant. Moreover, it may be unclear whether the research was done well because there might be a specific term the researcher missed. Missed research can be detrimental and embarrassing to the researching party when the judge or opposing party has a relevant prior case. Such a problem will not happen using same-type programs because all users will have the same results after uploading the complaint. The results are based on the strength of the program rather than the strength of the researcher. Although modifying a complaint may alter the research results, the research is still much more accurate and stable than key word research. This is because same-type programs can associate almost all commonly used expressions for a concept through its legal knowledge graph that is designed and constantly updated by groups of experienced law professionals. Moreover, after analyzing the facts, the program carries significantly more information than an individual researcher carries when researching, thereby reducing the selectivity and randomness of the research.

The use of same-type case programs may also have positive societal effects through the program’s ability to identify the most relevant prior cases with relative ease. With the program, a lay person could complete the research simply by uploading the document without having prior legal knowledge or mastering complicated research techniques. This accessibility lowers the entrance bar to the legal system for the general public. Additionally, individuals may reasonably predict the results of their own pending cases simply by comparing their facts with the facts of the recommended cases. This will allow individuals to make informed decisions without any understanding of legal reasoning or doctrines. Consequently, same-type programs decrease the necessity and importance of hiring lawyers, thereby reducing litigation costs. Same-type programs also decrease the importance of legal research techniques and lower the opportunity cost of litigation. Both parties to a case will have nearly the same research results without the possibility of missing important cases. Same-type programs, therefore, improve legal accountability by eliminating one factor of legal vagueness, i.e. disparities in identifying prior analogous cases without knowing their representativeness of the whole database. That said, difficulties may arise from cases with certain facts that have not been factorized in the legal knowledge graph but are
considered important to the pending case. Such facts may be new or old facts that need new evaluation. Moreover, the system can only find what was written in the judgments or proceeding documents; if something is merely implied it would need to be specified in the system’s algorithms. The results are also subject to the limits of NLP development in enabling machines to understand language.\(^\text{149}\)

2. An Advanced Legal Analyst?

Prior-case analysis programs’ ability to automatically analyze prior analogous cases may be viewed as a supplement to or replacement for judicial clerks. Currently, these analyses are statistical models coded in algorithms that computers automatically process. For example, the program may recommend a compensation amount for a pending portraiture right\(^\text{150}\) infringement case, given certain factors.\(^\text{151}\) The factors in the complaints may be factorized automatically by the machine or entered manually by the judge. Building the algorithm to calculate the compensation amount is similar to the process of factorizing cases. First, factors that may influence the calculation of the compensation amount are summarized using legal statutes, judicial interpretations, and the experience of judges who specialize in relevant issues. Second, multiple deep learning methods are used to enable computers to factorize previous portraiture right infringement cases, during which new factors that have influenced judges’ measurement of compensation may be recognized. Third, the impact of the factors on the compensation amount is studied and tested by regression models based on theories offered by legal professionals and practitioners in similar legal studies. Fourth, the acceptance or declination by judges of the recommended compensation amount after consulting the model will be tracked and collected to test and

\(^{149}\) NLP development is limited by the vagueness of language and the variation of words’ meanings over time, place, and context. See Philipp Broniecki et al., *Data Innovation for International Development: An Overview of Natural Language Processing for Qualitative Data Analysis*, INT’L CONF. ON FRONTIERS & ADVANCES DATA SCI. (2017), at 92–97.

\(^{150}\) The portraiture right is a unique right in China that is part of a bundle of personal rights, including a right of honor. *Photos Taken During a Concert: Legal Regime in China*, HFG L. & INTELL. PROP. (Nov. 29, 2016), www.hfgip.com/news/photos-taken-during-concert-legal-regime-china [https://perma.cc/3PHC-XL9P].

\(^{151}\) Such a program has been developed by a project completed collaboratively by computer scientists, an electronic business company, and a district-level court in Beijing. Interview with the Project’s Chief Computer Scientist, Professor Dou Zhicheng, in Beijing, China (Apr. 2018).
adjust the model, allowing a twenty to fifty percent variation. The analytical model could be quite simple or very complicated depending on the context in which the program is used.

Judges find such analyses useful when the law fails to provide clear guidelines in areas such as calculating sentences and deciding the seriousness of the criminal activity. Like in the portraiture right infringement case, the law only states that the compensation shall be decided according to the loss caused by the infringement, but it does not specify how to decide the loss. Without a model, judges have to perform the calculation ad hoc, and the results may vary widely. Judges, thus, may seek advanced machine assistance in more difficult contexts. Situational difficulty is reduced as facts not previously factorized in the law are incorporated.

In some respects, prior-case analysis programs provide more advanced assistance than legal researchers—the programs can offer some previously-thought-impossible analyses, and suggestions are more straightforward, scientific, and case-based. However, limitations still exist. In some cases, reliance on past judicial decisions or experiences may not be appropriate given the context, and associations found by programs may be incidental rather than causal. Further, its findings may be biased due to design deficiency or a discriminatory training pool. All of these factors need to be quantified in the model, which may inappropriately import normative values. Additionally, the system is limited in that it can advise legal applications but cannot adjust fact-finding. It must presuppose that the facts recognized in the judgments are facts that judges believed to be true when deciding the cases, which may not be accurate in many cases. Each specific question of law, therefore, needs a specially designed and trained model, which takes time and effort. Deciding whether to resolve a question manually, by machine, or by judicial discretion is a balancing act.

Although judges need only refer to the advice offered by these machines, judges may be unreasonably reliant on them without other references available or a thorough understanding of potential sources of bias or errors, such as design deficiency or inadequate training.

---

152 Id.
3. A Robot Judge?

Intelligent case-deciding programs are capable of generating judgments, essentially making them like robotic judges. However, the concept of automatically generating judgments may not be entirely new—it can be viewed as an advanced type of a judgment template. Judgments are routinely written in a similar style, containing the information of the litigants, their evidence, their claims and arguments, the findings of fact and opinions of the trying court (or the lower court’s fact-finding and opinions in an appellate case), and the conclusion. This template provides a framework for judges to copy and paste information and write their own findings and opinions. Meanwhile, judgment-generating programs automatically fill in information that can be found in the uploaded complaints. With the help of same-type and prior-case analysis programs, and additional models, judgment-generating programs may complete the findings and opinions sections as well. Unlike in the United States, judgments at the district and intermediate levels in China are as short as one or two paragraphs. Such judgments start with canonical statements from relevant statutes and continue with the facts as found by the court. The reasoning section consists of a summary sufficient to satisfy the elements required by the relevant statutes and ends with responses to each party’s arguments. Finally, the opinion cites relevant statutes and makes a decision.

With proper training, a machine can competently complete many of these steps. Relevant legal statutes may be filled in with commonly used language based on prior analogous cases. Similarly, frequently used expressions from convictions, sentences, breach of contract, compensation, etc., can be collected and recommended by the program. It can further present the language used in the reasoning section of prior analogous cases that had similar decisions. For the fact-finding section, the program can copy and paste the facts claimed by each party. Judges only need to decide what facts they believe to be true without having to organize the language. Judges also need only decide whether to convict or compensate and do not need to organize the language and write out the whole decision, thus transforming their behavior into high-level managers. Nonetheless, judges would still have the ability to modify the suggested language if the machine’s response was inadequate. Thus, judgment-generating programs provide an advanced template, similar to a preliminary judgment prepared by a judicial clerk. The program can be useful for simple and clear cases but may not be as helpful for unique or
complicated cases that are distinguishable from prior cases. After all, the program presents choices only from past decisions. If the program’s suggestions do not contain the one the judge wants, she will need to write a new opinion.

In sum, STCR aims to relieve the burden of judges’ heavy caseloads and improve the quality of judicial decision-making with AI assistance. AI programs act as legal researchers, analysts, and decision makers. They do this by conducting legal research more efficiently than human researchers, providing statistical analysis of prior analogous cases, generating judgments, and writing decisions. All of this is subject to judicial oversight, with judges retaining the ability to reject any part of the STCR AI process and manually complete such tasks.

V. IS ROBOTIC COMMON LAW STILL COMMON LAW?

This section addresses whether machine-made law should be considered part of the common law. While machines are capable of completing most tasks, a portion of which they can resolve more efficiently than human judges, there remains a portion of cases, which machines cannot resolve. This disparity requires an analysis of machines’ impact on the common law, namely stare decisis, the function of incrementally updating laws, and judicial lawmaking.

Although STCR is highly automated, it serves only to assist judges in its current state and is not yet able to replace them. STCR’s intelligent programs, i.e. machines, analyze judicial documents according to algorithms. The rules carried out by the machines are designed by groups of law professionals and programmers, based on their expertise. The algorithms serve two functions: first, they tell the machines which statements correspond to which factors; second, they tell the machines how to make certain routine judicial decisions with specified factors, using models such as decision trees. Although machines may independently learn to equate certain statements to certain factors, this initial exercise is completed by humans. Unless the accuracy of an association found by machines surpasses a high threshold, as verified by humans, such a model will not be used in practice.

154 See discussion infra Part IV.
155 See discussion supra Part III.
156 There is not a standard accuracy rate requirement, but normally, such a rate has to be at least ninety to ninety-five percent. Otherwise, the products based on these models
At each node of its decision model, STCR’s programs allow judges and users to intervene and make modifications so that they control the final output. After a document is uploaded, same-type programs will factorize it and make recommendations. Judges can correct the factors and instruct the program to find analogous cases based on those modified factors. Additionally, judges can instruct prior-case analysis program models to analyze the determinations made by judges. Prior-case analysis programs can return suggestions based on the factors entered by judges. Judgment-generating program models rely on judges and their selections to proceed. In the end, judges retain the discretion to reject any of the suggestions and answers provided by the machines. Even if the Implementation Opinions on Accountability requires judges to follow prior cases produced by machines, judges can still distinguish cases through selective interpretation of prior cases. Thus, STCR’s intelligent programs simply provide the same level of aid that judges receive in interpreting prior cases. However, STCR’s existence and potential capacity to complete advanced, abstract thinking and analysis can go further. Ultimately, these programs can help replace judges in simple, non-controversial cases. This possibility makes the following discussion of STCR more meaningful. There is an open question as to whether machines should be allowed to provide such assistance to judges—or even replace judges in some cases. If so, it remains to be decided whether machine made law is common law.

The United States judicial system makes wide use of computer programs. Employing such use affects both fact-finding and lawmaking. Evidence created by or collected with the help of computer programs dominates modern trials, especially in criminal matters. Judges rely on these models to evaluate damages, expected profits, risk, danger, and value. Previously, these elements were determined according to judges’ subjective determinations. In contrast, there is now software in use that helps decide the risk of recidivism and assists judges in deciding bail, remission, and sentencing. Literature in the legal field about AI use cannot satisfy judges’ demands and will not be able to compete in the market. Interview with Gridsum Company Officials, in Beijing, China (Mar. 2018).


159 Benjamin Liebman, Artificial Intelligence in the U.S. Legal System: Challenges and Concerns (美国司法实践中的人工智能:问题与挑战), 2 CHINA L. REV.
centers on two notions. First, such an application may contradict existing relevant constitutional or common law doctrines, including substantive and procedural due process, the confrontation clause, and anti-discrimination requirements. The other notion considers public policy, societal problems, and new errors that may be caused by machines, such as the loss of jobs, hidden discrimination, algorithmic bias, machine error, and accountability. Both of these ideas lack a discussion about the overall impact of algorithms on the common law system from a jurisprudential perspective. Additionally, these discussions omit the analysis of the influence over central characteristics and functions of common law, such as stare decisis and upholding democracy and liberty. The following section aims to fill this gap. Using STCR as an example, it first discusses the kinds of tasks in the judiciary that may be completed by machines and which factors are influential. Then, it focuses on the impact that replacing judges with machines will have on the common law system.

A. Machine Capabilities at Completing Tasks

Literature on robot regulators divides the use of machines in law into two categories: routine decision-making and agency lawmaking. Machines used for rather simple legal processes are categorized in the routine decision-making category. Machines in the judicial realm fall into the agency lawmaking category and are considered more problematic and subject to various legal doctrines and policy concerns, such as nondelegation, transparency, and reason-giving. However, this categorization may not be suitable. In simple cases where judges are interpreting law and making decisions, they in fact repeat the application of clear law and seem to partake in routine decision-making. Thus, the current same-type technology employed in China does not fit neatly into these categories. Moreover, the previous taxonomy is too human-centric and fails to incorporate the rules of machine “behavior.”

---

(中国法律评论) 54, 54 (2018); see also State vs. Loomis, 881 N.W.2d 749, 754–55 (Wis. 2016) (evaluating the use of an algorithm that purports to predict whether a criminal defendant will reoffend).

160 See Chessman, supra note 158; Liebman, supra note 159; Roth, supra note 27, at 2030–516.

161 Chessman, supra note 158. See generally Kroll et al., supra note 24.

162 Coglianese & Lehr, supra note 21, at 1214–15.

163 Id. at 1147–49.

164 RONALD M. DWORKIN, LAW’S EMPIRE 338 (1986).
some circumstances, models can be more complex and difficult to maintain, as well as subject to higher error rates in routine decision-making than in lawmaking.

This article instead divides the tasks of the judiciary into three categories: (1) readily machine-resolvable tasks (RMR); (2) possibly machine-resolvable tasks (PMR); and (3) impossibly machine-resolvable tasks (IMR). Additionally, the success of AI in completing these tasks can be evaluated by how well the machines function as either humanly or rationally. Humanly refers to measuring success in terms of fidelity to human performance, while rationally refers to measuring against an ideal performance. Following this taxonomy, RMR tasks in the judiciary are defined as tasks, which, with existing available data, machines can perform better than experienced judges at an acceptably low error rate. A simple “human” test of the soundness of machine performance is to look at whether suggestions provided by machines are always accepted by experienced judges who are free to reject these suggestions. Conversely, a “rational” test could look at whether machine performance is statistically significantly closer to an ideal performance than judges on average. Under conditions that should be realized in the foreseeable future, PMR tasks are those that a machine can perform better than experienced judges at an acceptably low error rate. In contrast, IMR tasks are those in which machine performance cannot surpass the soundness test or the conditions cannot be satisfied.

This taxonomy should not be used to suggest that readily and possibly machine-resolvable tasks should be completed by machines. Instead, it provides the basis for further discussion on the impact of machines replacing judges in common law. When machines are introduced to complete these tasks, they may initially require strong human supervision. But after being in use for a period of time, the machines can advance to where they will only require partial human supervision. With sufficient training, machines may be able to complete relatively difficult tasks without any human supervision at all. This sort of training and

---

165 This idea is inspired by interviews with computer scientists, STCR intelligent software developers, and online canonic AI-related course materials. See Interviews and Field Observations with One Mathematician, Two Computer Scientists, Four Software Developers, and Many Program Operators and Users, Beijing, China, Zhe Jiang, China, and Shanghai, China (Feb.–May, 2018); Wang Wenmin (王文敏), Artificial Intelligence Principles (人工智能原理), PEKING UNIV., https://www.icourse163.org/learn/PKU-1002188003/#/learn/content [https://perma.cc/Y8CU-ZW4E].

166 Wenmin, supra note 166, at pt. I, sec. 1.4, p. 3.
supervision process is currently the standard way to “teach” machines to be intelligent.\textsuperscript{167} Thus, even if STCR’s programs currently look like pre-AI judicial assistants, a gradual substitution of machines for judges may eventually occur as the machines are further trained.

The difficulties in enabling machines to complete complicated tasks multiply along the above categories. The data, time, and effort needed for developing RMR-targeting programs are substantially less than the other categories. Inspired by STCR’s programs, two aspects may influence the categorization of a judiciary task in the taxonomy—the data and the factors. Data refers to both the amount and the availability of data needed to train the model for a specific task. The amount of data need not be vast, so long as it can cover nearly all of the circumstances of the task. The availability of data refers to the degree of digitalization of human behaviors and experiences in completing the task and the sensitivity, accessibility, and usability of the data. “Factors” refers to the complexity of the task, including the number and range of variables that may affect the solution. These variables include (1) the capacity of the human expert in specifying these variables, (2) the coverage of all variables by existing human expert experience and knowledge, and (3) the decision rules about how these variables work together in the minds of human experts to achieve the outcome of the task. Capacity of human experts depends directly on the ability of the human experts to connect the factors with the real world, namely distinct words, photos, and other records. The coverage of the variables pertains to whether the summary of factors embody all the considerations and specifications of each factor. Further, it is crucial that the coverage includes all possible representations of the factors in the real world. The decision rules for different legal issues will likely be different but will rely generally on the connections between the variables and the problem to be addressed. For example, these variables in STCR are the factors summarized by experienced judges or prosecutors in their decision-making, such as the elements of the crimes and their sub-elements.

For a judicial task to be RMR or PMR, it needs to be computable, algorithmizable, sustainable, applicable, and have data available. First, the calculation of the algorithm for a judicial task needs to be within the calculation capacity of computers. If the algorithm includes an exponential

\textsuperscript{167} Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).
increase, it may be outside the calculation capacity. If the factors or their representations in the real world may increase exponentially over time, the judicial task may not be computable.

Second, the judicial task needs to be resolvable in algorithms so that machines can calculate them. As some literature has already noted, specification is one factor used to decide whether a judicial task can be translated into an algorithm, i.e. being algorithmizable. The number of factors and the decision rules also affect whether judicial tasks are algorithmizable. The more factors there are—and the more they vary—the more difficult it will be for a judicial task to be coded in algorithms. For example, the decision rules such as “forming a moral certainty” or “conforming to a sense of justice” are still deemed incapable of being presented in the form of an algorithm, although there are some discussions about whether computers may form their own wills capable of deciding justice in the future, through machine learning.

Third, for machines to “understand” the designed algorithm, and then act or think accordingly, the resolution of the judicial task needs to be sustainable. This means that the factors, their representations in the real world, and the decision rules must remain relatively the same for a substantial period of time. Such sustainability guarantees the effectiveness of the algorithm, the established knowledge graph, and the labels marked manually in the documents. A significant break from, or overruling of past decisions, may necessitate a fundamental change to the algorithm. Further, it requires a revision of the labels manually marked on thousands of documents.

Fourth, the factors, their representations in the real world, and the decision rules need to be uniform nationwide for the machines to be applicable in different places. Otherwise, as in the case of sustainability, algorithms will need modification and the original manual labeling may all be wrong. But the granularity of the algorithm can be enlarged to some degree to increase the applicability and flexibility of the algorithm so that lower-level rules can be different while upper-level rules are uniform.

Finally, machines need sufficient data for training. The amount of data needed increases substantially with the growth of the number of factors and their representations in the real world, as well as the degree to which they could be specified. At this time, no legal standard for a desired or acceptable accuracy rate exists. It has been suggested that clearly

168 Coglianese & Lehr, supra note 21, at 1156–60.
169 Ingles, supra note 25, at 519–522.
specified and defined factors in the law may require hundreds of samples to train computers so that the accuracy rate can approach ninety-five percent.\textsuperscript{170} Factors that are well-known and could be specified by legal experts according to their expertise may need thousands of training documents. But there is still a risk that their accuracy rate may only approach eighty percent.\textsuperscript{171} Examples include finding information about time, place, identity of defendants, and their mental situations. Factors that are intuitively understood by legal experts and cannot be specified in general ways may need tens of thousands of samples. And under those conditions, the accuracy rate only approaches seventy percent.\textsuperscript{172} Some mandatory data may become available once the judges’ behavior in resolving the judicial task can be digitalized, while some tasks may need judges to teach computers how they think when they behave in a certain way, which increases judges’ steps in resolving the task. An example would be labeling certain statements in a criminal’s confession as “motivations” in order to produce training materials for computer programs.\textsuperscript{173} Some data, however, may involve trade secrets, patent protections, agency interests, state secrets, or security concerns, making it difficult to use these materials for training computers.

These factors together help categorize a judicial task and represent the characteristics of the task. RMR or PMR tasks are those where computers may actually replace judges in the foreseeable future and are thus the starting point for a discussion of the impact of robotic substitution within a common law system.

B. Impact of AI Machines on the Common Law

As discussed in Part III, despite the disparate evolution of common law across different countries and the growing convergence of civil and common law systems, it is generally believed that common law needs certain features to be distinguished from case law in civil systems. For similar reasons to the comparison of China’s STCR with common law, this section will examine the central characteristics, distinct features, and

\textsuperscript{170} Interviews and Field Observations with Software Designers and Programmers of Shanghai Procuratorate, Shanghai, China (Apr. 2018).

\textsuperscript{171} Id.

\textsuperscript{172} Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).

\textsuperscript{173} Id.
functions of common law when analyzing the impact of machines. These include *stare decisis*, judicial lawmaking, the function of incrementally updating laws and providing reason, and commitments to upholding democracy and liberty.

1. *Stare Decisis*

Do machines treat like cases alike when they replace judges in RMR or PMR tasks? The answer is yes. Machines’ capacity to complete these tasks is built by having machines study past analogous judgments. Data from prior cases is the lifeblood of AI in the judiciary, without which machines cannot be created. When machines decide RMR or PMR cases, they factorize the pending case, associate it with past cases that have similar factors, and then decide it according to the rules of past analogous cases. This is the same process judges normally follow with regards to precedent. When machines factorize the pending case, they associate statements with similar meanings based on past judgments and mark them with the same factors. They learn association through either a knowledge graph or self-learning. The rules of past analogous cases are normally provided in algorithms designed by legal experts and programmers according to the most plausible readings of relevant laws and generally accepted effects of these factors in deciding cases. Machines may provide statistical analyses and proof for such readings or effects. However, they may not be permitted to draw the rules through self-learning from the results and the factors of past analogous cases directly because it may cause the “black box” problem.\(^\text{174}\) Consequently, facts that were considered factors will continue to govern in new cases, and those facts which were not considered factors will not affect new cases. Cases that have similar factors will be decided similarly as past decisions.

Using intelligence to follow precedent seems to be a rigid version of *stare decisis* but can be distinguished in several respects. First, in algorithms, the elements and the interpretations of doctrines and statutes of past cases are predetermined, specified, and fixed. In contrast, with *stare decisis*, there are disputes over whether to uphold formalist (or non-formalist) interpretations of doctrines and enacted texts,\(^\text{175}\) and even the

\(^{174}\) See generally FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015). The black box problem generally refers to when a machine self-learns to find ways to complete tasks, but a human cannot determine how the machine completed the task.

\(^{175}\) Pojanowski, *supra* note 157.
“reasonably clear, public semantic meanings” of the texts upheld by the textualists are not unified. The text according to judges may have several meanings or interpretations with slight differences, and these differences can be nontrivial in extreme circumstances. Second, the factors of precedents are pre-extracted when using artificial intelligence. What factors each precedent has and what facts in the precedent constitute each factor are determined and fixed, whereas when judges follow precedents, they may reinterpret them or even go back to the whole set of facts and endow originally trivial facts with new values. Through this process, judges also reinterpret relevant doctrines and legal texts. Third, when deciding whether two cases are similar, machines simply calculate the similarity of the factors they have been given according to algorithmized rules, while judges may apply selective rules in finding similar cases. In some instances, judges may consider past cases for all the factors shared with the pending case as controlling precedent; while in other instances, they may use a qualitative test, ignoring some factors. Fourth, all these factors, rules of decision, and their representations in documents are programmed into algorithms to represent the interpretations of the legal experts who participated in developing and training the machines. Labeling documents represents the understandings of people who do the labeling. However, when judges follow precedents, they have their own understandings of the doctrines and legal texts, and they apply their own rules of comparison to follow them. Such understandings are individualized within certain parameters and may differ from those of the experts who completed the initial labeling. Although judges theoretically all start with the same body of precedent in crafting a judgment, each judge makes individualized decisions and takes responsibility for those decisions. Hence, the intelligent system of precedents nearly eliminates ad hoc discretion of individual judges.

However, it is inaccurate for several reasons to conclude that within these tasks, judicial discretion would be entirely eliminated. Discretion and specification are not inherently contradictory because discretion does not equal vagueness, and specification does not mean the algorithms are fixed or unchangeable. First, judicial discretion exists in algorithms. When legal experts summarize the factors and mark their

177 Clark & Trubek, supra note 125, at 255–76.
178 These skills have been summarized as the leeway of common law. See LLEWELLYN, supra note 32, at 62–120.
facts, they build into computers judicial discretion in applying relevant laws. The difference is that such discretion is specified and represents the judicial discretion generally accepted by these legal experts. The algorithms could be modified to reflect an update of the laws and the legal experts’ generally accepted judicial discretion. Further, the granularity of the algorithms to filter targeted factors and facts could be adjusted to accommodate different degrees of acceptance of specified judicial discretion.¹⁷⁹

Second, machines are designed to mimic humans in completing these tasks. A fundamental difference between AI and previous scientific instruments and programs is that AI seeks to replicate human thought and actions. This lack of differentiation is the goal of the Turing test, one measure of AI’s success. The Turing test holds that a computer may be deemed to have intelligence if a human interrogator, after posing some written questions, cannot tell whether the written responses came from a person or a computer.¹⁸⁰ There are updated versions of the Turing test, such as a visual Turing test,¹⁸¹ but all seek to argue that at some point, the difference between humans and machines may reach the point of undetectability. The Chinese Room Argument presents an alternative hypothesis to AI completeness. It theorizes a person locked in an enclosed room who does not know Chinese, but with translation software, can translate English words into Chinese. The Chinese Room Argument posits that, although people outside the room will receive Chinese words correctly translated from the English words by the person inside, it is incorrect for people outside to conclude that the person inside understands Chinese.¹⁸² This argument disputes the soundness of the Turing test and its variants and argues that a program cannot give a “mind,” “understanding,” or “consciousness” to a computer.¹⁸³ Applied to judicial tasks, this article argues that the Turing test can similarly ask, after posing some legal questions, whether a human interrogator can distinguish between the written responses of an experienced judge and a computer. When there is little difference, machines may replace judges in answering legal

¹⁷⁹ Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).
¹⁸⁰ Alan M. Turing, Computing Machinery and Intelligence, 49 MIND 433 (1950).
¹⁸³ Id. at 418.
questions, consistent with the practical development path of judicial AI. Initially, machines should complete these tasks under the full supervision of judges (as in China’s use of STCR). As the performance of machines becomes more accurate and reliable, the supervision can become more limited. Finally, when machines regularly return decisions substantially the same as decisions of experienced judges, the supervision can be wholly removed.\textsuperscript{184}

Judges can improve machine decision-making performance by creating labels that enable self-learning. Self-learning criteria are based on the acceptance or rejection of machine-created statements and suggestions.\textsuperscript{185} Since a machine acts like a human in these tasks, its decisions represent judicial discretion and may be given the same deference as a judge’s decisions. In an ideal world, every judge would use AI that can track his or her considerations and decisions. Then, if judges generally agree on the same resolution for certain issues or evaluate certain facts and factors similarly (i.e., with minimal variation), machines will record these judicial behaviors, form rules, and incorporate the rules into algorithms. Such cases where judges hold generally unified discretion, and where the situations are relatively simple, can be viewed as RMR or PMR tasks where machines can continue the exercise of judicial discretion after they have learned gradually from judges. On the other hand, if judges reach disparate resolutions or evaluations (as is the case with IMR tasks), machines may not be able to form rules and may return error messages or provide no suggestions. This includes situations where non-formalistic and formalistic interpretations of doctrines or enacted texts lead to opposite outcomes or where reasoning contradicts the sense or equity of the situation. However, in situations where even human judges cannot agree on a resolution, machines cannot be relied upon to complete IMR tasks in a predictable manner.

2. \textit{Incrementally Updating Laws}

Understanding the continuity of judicial discretion in AI judges is essential to evaluate the impact of machine substitution on the function of the common law system over time. A common law system has well-

\textsuperscript{184} Interview with the Project’s Chief Computer Scientist, Professor Dou Zhicheng, in Beijing, China (Apr. 2018).
\textsuperscript{185} \textit{Id.}
recognized advantages over a civil law system.\textsuperscript{186} For example, a common law judge has the mission, authority, motivation, and competence to pursue consistency among enacted or precedential legal rules and social values by incrementally modifying laws, case-by-case, with the effect of weaving past and future laws into a seamless web.\textsuperscript{187} However, continuous change is not the same as the smoothly continuous flow of real numbers (such as in calculus). Statements in logic are viewed as discrete objects and have distinct, separate values. However, they still vary continuously in a legal sense. Although current computer science is built on discrete mathematics, which excludes continuously varying objects, it considers the variation of discrete objects. Thus, AI judges should have the potential capacity to capture, incorporate, and reflect the variation of laws. Again, specification is not equivalent with remaining fixed and unchanged.

An argument may be raised against AI judges’ competence to incrementally update law. Although machines can incorporate changes, they need modifications to the specifications in their algorithms to do so. Consequently, machines may track the changes of human judges in their decision-making and follow those changes, but machines cannot create changes in the same manner as human judges. Common law judges are believed to be able to identify and forge a shared sense of reasonableness on the social problems presented in pending cases and apply reason rather than pure precedent to resolve cases.\textsuperscript{188} Human judges incrementally change the law when deciding every case through this lawmaking and re-evaluation of legal meanings present in recurring fact patterns. AI judges must wait until their algorithms are changed to reflect the outcomes of newer cases, which is more like the civil law-style of modifying statutes. Moreover, an essential reason to have trials is to provide a public forum for disciplined deliberation by parties so as to converge diverse views, provide collegial wisdom and insight from the local community, and make judicial decisions on public guidance for local people.\textsuperscript{189} If AI judges cannot be influenced by the deliberation and arguments happening in ad hoc trials, it becomes meaningless for the parties to participate in trials—or for trials to even continue to exist.

\textsuperscript{187} Harlan Fiske Stone, \textit{The Common Law in the United States}, 50 Harv. L. Rev. 4, 12 (1936).
\textsuperscript{189} Id.
Although this would be a strong argument against AI judges, AI judges can in fact be influenced by in-trial deliberation and argument. For example, when evaluating damages or the seriousness of results in criminal cases, STCR’s programs are designed to consider the testimony of the victims about their suffering from the crimes and the explanations offered by the defendants in legal documents.\textsuperscript{190} China’s STCR is currently at an elementary level in this aspect. A fact may automatically become a factor if the algorithm has a rule to evaluate the importance of the fact and a standard to evaluate the fact against. Further, a fact may have different legal meanings if the algorithms incorporate the perspectives of the victims.\textsuperscript{191} Specification here does not equal unification. This capacity is rooted in the foundations of AI technology and is necessary for AI judges to act or think humanly or rationally because in many situations, the task environment is dynamic, partially observable, and unknown.\textsuperscript{192} In such situations, AI judges may not find their action in a lookup table, so the system has to learn how to make reasonable decisions.\textsuperscript{193}

There are several routes to strengthening AI’s capacity to interact with its task environment, including symbolic, connectional, logic-based, anti-logic, and statistical approaches.\textsuperscript{194} For example, the anti-logic approach specifically targets difficult problems in vision and natural language processing that require ad hoc solutions.\textsuperscript{195} AI can automatically update its knowledge of factors if it includes in its function a model that simulates real-world trial debates and can determine in what situations a fact becomes a factor.\textsuperscript{196} It is foreseeable that as the sensors of machines improve to capture information from human behaviors, facial expressions, and other physical symptoms, AI’s capacity to consider in-trial deliberation and argument will be substantively improved and may surpass human judges in catching and analyzing those pieces of information.

\textsuperscript{190} Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).
\textsuperscript{191} Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).
\textsuperscript{192} Wenmin, supra note 166, at ch. 2.3.
\textsuperscript{193} \textit{Id.}
\textsuperscript{194} \textit{Id.} at ch. 2.1.
\textsuperscript{195} Professors Marvin Minsky and Roger Schank from MIT uphold such an approach. \textit{Id.}
\textsuperscript{196} Such as the types of AI machines as a model-based agent and a learning agent. \textit{Id.} at ch. 2.5.
addition, neuroscience and cognitive psychology are foundations of AI, which study how brains process information and how humans think and act.\textsuperscript{197} Incorporating these learnings into an AI judge would make AI judges more similar to human judges in this regard.

Moreover, judges’ ability to incrementally update law is disciplined and reason-based, which is possible for machines to learn. The reason to uphold the lawmaking role of common law judges in deciding cases is that judges do not make law according to their arbitrary wills but through their identification and articulation of a disciplined, shared reasonableness.\textsuperscript{198} Judges derive this competence from their legal training, extraordinary reasoning ability, and moral standards. Judges are required to specify the reasoning behind their decisions to better guide the people subject to their decisions and ensure public accountability.\textsuperscript{199} Since judicial decision-making needs to be a disciplined, reasoned, and balanced process, either through a formalistic or dynamic interpretation of doctrines or enacted texts in order to maintain legal autonomy, such a process is not dependent on jurist arbitrariness or unfounded intuitions. Judicial decision-making should be replicable in models to some degree and incorporated in AI programs. Such models can be constantly refined by machine learning based on the critiques and responses of human judges on machine suggestions.\textsuperscript{200}

Furthermore, AI judges provide an advantage over human judges in that the former are more disciplined, objective, and logical than the latter. Both legal realists and legal psychological studies have shown that judges can be biased and make decisions intentionally or subconsciously according to personal preferences and discriminations.\textsuperscript{201} In contrast, AI judges decide according to the algorithms, which are specific without any unclear point or disputes of uncertain meaning. Although machine decision-making can have the “black box” problem, leaving the human unaware of a machine’s process,\textsuperscript{202} literature has already noted that such a problem could be resolved by requiring machines to state the reasoning

\textsuperscript{197} Id. at ch. 1.2.  
\textsuperscript{198} Postema, supra note 189, at 2–11.  
\textsuperscript{199} Id.  
\textsuperscript{200} See generally Wenmin, supra note 166 (the types of AI machines as a model-based agent and a learning agent).  
\textsuperscript{202} PASQUALE, supra note 175.
underlying their decisions (at the cost of efficiency).\(^{203}\) Although machines too may be biased and discriminative, such biases can be disclosed by checking machine suggestions against the indicators of suspected discriminations, such as using regression models to check whether extralegal factors, e.g., sex and social class, have effects at a significant level. Once detected, bias or discrimination can be corrected or prevented by refining the algorithms, adding random factors, and generating unbiased training samples.\(^{204}\) With algorithmic affirmative action, highly specified AI decision-making has been the preferred method for reducing discriminatory or biased decisions of open-ended human judgments, which may happen subconsciously and can be difficult to correct.\(^{205}\)

3. **Human Judge-Made Law and Normative Commitments**

Human judges may be biased and arbitrary, but replacing them with machines still sounds unimaginable to many people. As Oliver Wendell Holmes said, “[t]he life of the law has not been logic; it has been experience.”\(^{206}\) The life experience of human judges has formed the basis for their intuition and sense of justice and custom in the community. This enables human judges to find or create the best solution for the case at hand, to fit within the appropriate legal framework and social values. Although many models in disciplines such as economics and social sciences appear to simulate the world, the real world is believed to be more fluid and complicated than these models suggest. The more factors to be considered, the more difficult it is for AI to model the situation.

Moreover, machines lack the creativity that human judges have. Once the best solution for an issue has been identified, justification is easy. But often, reason alone is insufficient to lead to the solution—reason cannot produce creativity. Reason works to make unknown things known when the relationship between what is known and what is unknown is obvious. Conversely, creation and intuition work when such a relationship is not clearly known. Further, machines reason and decide by performing

\(^{203}\) A goal model or a utility model for AI can be used to reflect the AI’s decision-making process. See generally Wenmin, supra note 166196; see generally Kroll et al., supra note 24.


\(^{206}\) OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (1881).
calculations on large amounts of data while humans usually reason when there is only a small amount of information.

Besides the advantages of human judges in judicial creativity over AI judges, the goal of the rule of law is to realize concepts such as justice and fairness that are rooted in human feelings. Reasoning in past case decisions alone may be insufficient to recognize these considerations. Sometimes, decisions merely confirm or modify preexisting feelings, which come from the intuitive sense of justice of the individuals involved in the case. Such feelings cannot be digitized and thus cannot be “felt” by machines. Even if the feelings could be digitized and read by machines, arguing that machines can embody human feelings is controversial—this mirrors the Chinese Room Argument against the Turing Test. In law, such an argument has another layer of strength: individuals facing AI judges may not believe that their feelings are being fully considered. Only when a human judge is the decision-maker, with human emotions and a limited life span, will litigants believe their feelings are fully considered in making decisions. This makes it easier for diverse views to reach congruence, thus making the decisions more acceptable to litigants, ultimately affecting the legitimacy of AI judges.

Moreover, people tend to trust and respect the decisions of human judges who, generally, are perceived by the community to be reasonable, prudent, disciplined, and impartial. Historically, human judges have played heroic roles and have been relatively powerful, especially when working together, because of their reputations, well-recognized capacity, and high socioeconomic status. Such power works to enhance the force of judicial decisions. More importantly, both the characteristics of human judges and the power they have are essential in upholding the separation of powers, liberty, and the counter-majoritarian role of the courts. Replacing human judges with AI judges removes the advantages that human judges offer, such as generating creative judicial solutions; providing the means for incubating new rights, obligations, and legal doctrines; persuading the general public; balancing against other political powers; and protecting disadvantaged parties.

The advantages of human judges over AI judges are sensible and persuasive, which is why the common law system remains nearly unchanged in the digital era. Nevertheless, the judicial system faces

207 Searle, supra note 183, at 418.
208 Cross, supra note 78, at 53.
209 See id. at 21–59.
exciting advances made possible by big data\textsuperscript{210} and AI. Underlying the arguments supporting human judges’ advantages over AI judges is a strong faith in the subjectivity or mastership of humans over machines. This strong faith in humans is reflected in the normative and technical perspective that lawmaking in certain difficult cases, especially those requiring sophisticated tasks, is best reserved for humans. However, having AI judges to deal with simple, recurring cases that are RMR or PMR does not mean that human judges will be replaced in all cases—particularly those that are more complex.

As discussed, machines may learn from human judges’ experiences by building a knowledge graph, summarizing factors, and having judges manually label the judgments that are used to train machines.\textsuperscript{211} However, some legal tasks are too difficult or differentiated to be resolved by machines. For example, in building China’s STCR system, experts originally tried to train machines to resolve intentional murder cases.\textsuperscript{212} This failed, however, because there have been too few cases to provide sufficient training materials, and the facts of intentional murder vary greatly and cannot be modeled.\textsuperscript{213} As summarized by the chief designer of the essential STCR software, machines need more than 10,000 cases to grasp the life experiences of human experts in order to achieve an accuracy rate of around seventy percent. A life experience includes analyzing whether a statement reflects the motives of the suspects and whether the same statement represents their means to conduct the crimes.\textsuperscript{214} However, given the great costs a machine error may impose, machines should only replace human judges in tasks where the accuracy rate of machine performance is high enough to approximate human accuracy. So, even with RMR tasks, human supervision cannot be removed until accuracy improves and stabilizes. Thus, a more accurate and suitable conclusion is that instead of replacing human judges, AI judges can help relieve human judges from easy cases where the fact

\begin{multicols}{2}
\textsuperscript{210} “‘Big Data’ is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics.” Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C.L. REV. 93, 96 (2014).
\textsuperscript{211} See discussion, \textit{ supra} Part IV,C.
\textsuperscript{212} Interviews and Field Observations with Software Designers and Programmers of Shanghai Procuratorate, Shanghai, China (Apr. 2018).
\textsuperscript{213} \textit{Id.}
\textsuperscript{214} Interviews with Software Designers and Programmers for Zhejiang Prosecutor’s Office (Apr. 2018); Interviews and Field Observations with Prosecutors, Software Designers, and Programmers at Shanghai Procuratorate, in Shanghai, China (Apr. 2018).
\end{multicols}
patterns can be delineated and the decision-making is routine—allowing human judges to focus on complex or new cases. For example, although China’s STCR originally tried to cover many crimes, only models of a few crimes have been considered mature enough to be used, namely dangerous driving and theft.\textsuperscript{215} In the Zhejiang province, there have been around 5,000 cases of dangerous driving or theft decided with machines in which the machines extracted factors and recommended resolutions under human judges’ supervision. This represents more than seventy percent of the cases that fell within the scope of simplified procedures.\textsuperscript{216} Because of their frequent occurrences and limited types of fact patterns, models can easily be built and machines can easily be trained for cases involving these crimes. This approach saves significant human effort in resolving these types of cases.

In RMR or PMR tasks where machines have been trained to make decisions similar to those of experienced human judges, the value of judicial creativity is insignificant, and the loss of judicial creativity could be accounted for by modifying algorithms and inputs periodically. This is possible because fact patterns in these cases do not change within a certain period. Machine-generated virtual cases could provide alternative ways to test the effects and soundness of new judicial solutions, while helping predict litigants’ responses to different kinds of judicial decisions, without having to experiment on real people and cases.\textsuperscript{217} Besides, although it is true that people feel more comfortable communicating with human judges—and people respect human judicial decisions—society is fundamentally changing. Communicating with AI robots, machines, and software is becoming normal for people who grew up with technology as a tool in their daily lives. Moreover, since these cases do not vary much

\textsuperscript{215} Shanghai’s High Procuratorate has developed models for eight crimes. See Secret “206”: The Future Artificial Intelligence of the Court (揭秘“206”：法院未来的人工智能图景), \textsuperscript{\textit{JUST. ONLINE} (正义在线)} (June 10, 2017), http://www.sohu.com/a/155948492_434781 [https://perma.cc/NPJ7-HD52]. Zhejiang provincial procuratorate has developed models mainly for the crimes of dangerous driving and theft, according to the interviews. Interviews and Observations with Prosecutors at Zhejiang Provincial Procuratorate (Apr. 2018); Interviews with Software Designers and Programmers for Zhejiang Procuratorates (Apr. 2018).

\textsuperscript{216} Such models are developed by Zhejiang procuratorates and are currently in use throughout Zhejiang procuratorates. Interviews and Observations with Prosecutors at Zhejiang Provincial Procuratorate (Apr. 2018); Interviews with Software Designers and Programmers for Zhejiang Procuratorates (Apr. 2018).

\textsuperscript{217} Coglianese & Lehr, \textit{supra} note 21, at 1204–05.
from cases with similar arguments that were previously decided by human judges, repeating these trials may become redundant and inefficient.

The concern that judicial power would decrease and be insufficient to balance against other political powers if machines replaced human judges in a significant number of cases is unsupported. First, no matter how intelligent a machine is, it is acting according to its algorithms, which are designed by human judges and programmers. If used well, machines can help human judges handle a greater number of cases with more efficiency than currently possible. This will lead to reductions in judicial costs and decrease the burdens and costs of litigation. This may help make justice more accessible to ordinary people and should be viewed as an enhancement to judicial power. Second, as mentioned in the Introduction, AI machines are already being used in government agencies. As AI continues to develop, the increased use of AI in other political realms is foreseeable, making operations more efficient and effective. If the judicial branch lacks AI's benefits it will become comparatively disadvantaged. Third, as society is filled with machines and operates at a faster pace, the judiciary faces many new demands that are difficult to satisfy without AI machines. For example, the judiciary needs to evaluate evidence materials produced by society’s non-judiciary AI machines and deal with large amounts of information that cannot be handled manually. If judges are not equipped with AI designed according to their needs, courts will become more reliant on experts hired by litigants. As disputes from online transactions and worldwide customers increase, the demand for courts to resolve these cases online will increase as well. Remote trials may be crucial in some instances because of difficulties in physically holding court, e.g., if litigants reside in different countries.

These arguments do not suggest that human judges need to be replaced by machines. What is argued here is that the judicial system should be open-minded and creative regarding AI’s use in judicial decisions. Two factors further strengthen this opinion and explain China’s motivation in developing STCR. First, at the outset, machines need human supervision and a significant amount of training to become suitable to complete RMR tasks—the use of machines in real case work produces the data necessary to train machines for PMR tasks. In other words, AI machines need to be used to be successful. The more they are used—and corrected—by human judges, the better and more reasonable their suggestions and solutions will be. This process not only trains machines to

\[218\] Id.
be more advanced but also teaches the human judiciary how to communicate with machines and utilize machines in their case work. Human supervision works as a safeguard for the use of AI judges. Second, just like with a human judge, if a litigant feels the AI judge made a mistake in the case decision, the litigant should have the capacity to appeal to higher level courts to correct the judgment. Additionally, the government may create new procedural rights and institutional measures to protect litigants from machine errors and provide litigants with remedies. For example, AI developers can implement more error discovering algorithms and tests to find machine errors.\textsuperscript{219} In these aspects, the AI legal community needs to research machine errors, create new institutions, and maintain environments that are friendly and suitable to machines.\textsuperscript{220} As discussed, AI judges have numerous advantages over human judges, such as the ability to process large amounts of information, quickly perform complicated calculations, provide transparent decision-making logic, and avoid personal preferences and biases.

\section{VI. Conclusion}

This article discusses the STCR system that is being developed in China and compares it with the common law. STCR, discussed throughout, refers to a series of systems that helps find past cases of the same type and make prior similar cases binding on the case at issue. Having analyzed common law characteristics, like \textit{stare decisis} and incrementally updating the law, this article argues that STCR is an exceptional version of common law in China, which upholds the leadership of the party center. STCR’s \textit{stare decisis} characteristic and nondemocratic, normative commitments provide an extreme case to study the intrinsic relationship between the common law and its well-recognized normative functions and advantages. This article further explains that STCR is part of China’s national strategy to increase the court system’s intelligence and upgrade its governance capacity. Because precedents produce the big data necessary for AI to be applied in the judiciary, \textit{stare decisis} has become acceptable and welcome in China. This is part of the reason that STCR has been built relatively quickly with few roadblocks.

\textsuperscript{219} There have been many algorithms to discover or self-check machine errors and verify whether machines return results that are truly desired by programmers.

\textsuperscript{220} Machines can bring about new types of errors. See Chessman, \textit{supra} note 158.
STCR serves as a case study for improving the intelligence of the common law system. Part IV analogized STCR’s intelligent programs into three types of workers: advanced legal research assistants, advanced legal analysts, and judges. The virtues of STCR include providing more accurate and comprehensive research, reducing litigation costs, answering more advanced and difficult legal questions, assisting new judges, increasing judicial efficiency, and decreasing judicial workload. But STCR does not replace the human judiciary, and it is incorrect to conclude that STCR tries to create a robot judiciary. Although machines may complete more complicated and abstract tasks than before, they are under human supervision, and their suggestions can be corrected or ignored by a human judiciary. Moreover, it is still humans who make judicial decisions because humans can ignore or alter an AI judge’s decision.

However, these machines can likely be trained and improved to provide suggestions that are always deemed reasonable and, thus, accepted by human judges. The notion that machines may replace humans in judicial decision-making may cause concern surrounding the development and application of AI. Such concerns are reasonable because, although STCR’s intelligent programs can be viewed as advanced versions of previously used machines, AI machines are programmed to act or think humanly or rationally, a notion that makes the new system inherently different from the non-intelligent machines of the past. Facing these concerns, difficult decisions may need to be made as to whether to allow AI’s application in the judiciary or to develop AI machines that can complete judicial decision-making tasks.

This article provides a machine-centered taxonomy dividing judicial tasks into those, which are readily machine-resolvable (RMR), possibly machine-resolvable (PMR), and impossibly machine-resolvable (IMR). It then argues that AI’s application in the judiciary can relieve human judges from RMR and PMR tasks so they can spend more time on IMR tasks. Further, this article examines the impact of AI’s possible systematic substitution for human judges in RMR and PMR tasks within the common law. This includes a discussion of stare decisis, incrementally updating law, judicial lawmaking, and other normative commitments.

In these tasks, AI judges have advantages over human judges because AI judges strictly follow precedents, restrict improper judicial discretion, prevent personal biases and preferences of individual judges, handle large amounts of information, complete complicated calculative balances, and discover statistical representations of variations of fact
patterns and legal factors. These advantages come from AI machines’ algorithmic functions, which combine both human judges’ experience and legal reasoning logic. On the other side, the advantages of human judges in terms of judicial creativity, sensitivity, and communication with litigants are less valued in RMR and PMR tasks than in IMR tasks. As for transparency and reason, AI judges may or may not be disadvantaged compared to human judges given that algorithms may be designed to delineate machines’ decision-making processes while human judges are subject to personal biases. Although AI machines need to have specified instructions, this does not mean AI can only make invariable, mechanical, and unified case decisions. It is possible for AI to allow some degree of judicial discretion, legal vagueness, and individual specialty. Moreover, in light of AI’s increasing number of applications in private and public fields, AI judges can help to empower human judges, including relieving human judges from large amount of simple cases, increasing the efficiency and the availability of judicial system to be compatible with modern society, decreasing the cost of litigants, and helping more ordinary people achieve justice.

Ultimately, the competitors of humans are still humans—not robots. Humans compete with humans for resources, social status, and profits. Machines are intelligent and are meant to assist humans who exercise dominion over machines, at least for the foreseeable future. Society is currently in a transitional period where human judges must learn to train and utilize AI to facilitate their work. The judiciary should participate in the process to influence the development of AI machines’ thought processes. Thus, this article argues that AI will not fundamentally change the intrinsic character of the common law system and that AI’s application in the judiciary should be encouraged. Machine intelligence provides another route to resolve legal issues. Judges’ participation in the development of AI programs is crucial to design reasonable algorithms to complete judicial tasks and correct machine errors. In addition, there is a fundamental question of how these new measures should be pushed forward and carried out. China provides a central, governmental-leading model of implementing the STCR system, which has been deemed the Chinese mode of development. In this model, the central power selects certain places to experiment with new systems and then generalizes the experiences nationwide. In other societies, however, other modes of development may be more appropriate. The leading power can be either the central or local government, or a public or private entity, with each model having its own localized and time-sensitive values and costs.
IS BLOCKCHAIN THE DEATH OF ANTITRUST LAW? THE BLOCKCHAIN ANTITRUST PARADOX

Dr. Thibault Schrepel*

CITE AS: 3 GEO. L. TECH. REV. 281 (2019)

INTRODUCTION

Blockchain fever is hotter than ever. The World Economic Forum predicts that ten percent of global gross domestic product will be stored on blockchain by 2027,¹ which has caused an unparalleled craze regarding blockchain’s possibilities.² Some see it as a new way of organizing modern-day society,³ while others fear the chaos that it could create.⁴

¹ WORLD ECON. FORUM, TECHNOLOGY TIPPING POINTS AND SOCIETAL IMPACT, SURVEY REPORT 24 (Sept. 2015).
² WORLD ECON. FORUM, BLOCKCHAIN BEYOND THE HYPE: A PRACTICAL FRAMEWORK FOR BUSINESS LEADERS 3 (Apr. 2018) (“One of the most unique aspects of blockchain is its high number of evangelists — people who believe blockchain can solve everything from global financial inequality to access to financing for start-ups, the provision of ID for refugees, to solving supply chain problems and enabling people to sell their houses without needing an estate agent.”).
³ MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY vii (O’Reilly Media 2015) (“[T]he blockchain concept is even more; it is a new organizing paradigm for the discovery, valuation, and transfer of all quanta (discrete units) of anything, and potentially for the coordination of all human activity at a much larger scale than has been possible before.”).
There are skeptics that deride blockchain as the new Netscape, while others see it as the most important innovation since the Internet. If the latter proves to be true, societies will radically change and so too must legal systems.

Western legal systems have historically helped establish trust between parties and reduce transactional uncertainty by providing recourse to legal procedures. Nonetheless, establishing trust still imposes significant transactional costs. Blockchain may reduce these costs to “a much, much smaller level” because it might make contracting easier and, on a broader scale, because it may alleviate widespread contractual inadequacy by creating a world in which “computers . . . fill in the gaps of contracts.” Blockchain could then efficiently facilitate trade, but it also presents numerous legal challenges with substantial implications for antitrust law.

Several institutions, including the Organization for Economic Cooperation and Development (OECD), have identified the need to

---

4 On the idea that new technologies may, if not create chaos, generate losses, See Lawrence Lessig, Code: And Other Laws Of Cyberspace, Version 2 339 (Basic Books 2006) (ending his book by the following: “it is not a great time, culturally, to come across revolutionary technologies. We are no more ready for this revolution than the Soviets were ready for theirs. We, like they, have been caught by a revolution. But we, unlike they, have something to lose”). On the same subject, see also Jonathan Zittrain, The Future of the Internet—and How to Stop It 242 (Yale University Press 2008) (“Traditional cyberlaw frameworks tend to see the Net as an intriguing force for chaos that might as well have popped out of nowhere. It is too easy to then shift attention to the ‘issues raised’ by the Net, usually by those threatened by it.”).


6 A technology which disappeared after being seen as very promising.


8 Russ Roberts, Jim Epstein on Bitcoin, the Blockchain, and Freedom in Latin America, Econ Talk (Feb. 13, 2017), www.econtalk.org/archives/2017/02/jim_epstein_on.html [https://perma.cc/WAW6-ZFB7].

9 Lin William Cong & Zhiguo He, Blockchain Disruption and Smart Contracts 4 (Dec. 27, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764 [https://perma.cc/Z9QW-W7MA] (“[B]lockchains, via decentralized consensus, enable agents to contract on delivery outcomes and automate contingent transfers. Hence, the authentic entrant is now able to signal her authenticity fully. This eliminates information asymmetry as a barrier for entry and greater competition, enhancing welfare and consumer surplus in this blockchain world.”).


address the antitrust challenges created by blockchain. The first of these challenges is suggested by the word “antitrust” itself. On the one hand, much of competition law is articulated as anti-trust, employing the American terminology that emerged as a reaction to the misuse of the trust instrument. On the other hand, blockchain technology eliminates the need for a fiduciary—that is, a person who creates trust—because it functions automatically, without any natural or artificial person. What happens, then, when antitrust law contemplates a technology that functions without a trusted counterparty? Is it time to leave behind the blanket term and regime of antitrust? And, from a legal perspective, are the current rules well-suited to analyzing blockchain and its processes? Further, what should be the focus for antitrust authorities, and how can companies limit their legal risks in this respect?

Answering these questions now, when blockchain technology is still evolving, presents a substantial risk of inaccuracy, and yet, it is essential to do so before existing models of antitrust enforcement become outdated.

In fact, antitrust law has avoided the gallows before. When the Internet entered the mainstream, some individuals announced the end of antitrust law, which they predicted would be rendered useless by the rule of code. Several other authors sought the implementation of a new set of

[http://perma.cc/R723-8N9B].

See The Legislative History of the Federal Antitrust Laws and Related Statutes 10–13 (1978); see also Daniel R. Ernst, The New Antitrust History, 35 N.Y.L. Sch. L. Rev. 879 (1990). Robert L. Bradley, Jr. underlines John Sherman’s “intense opposition to trusts.” See Robert L. Bradley Jr. & Lawrence H. Summers, On The Origins of the Sherman Act, 9 CATO 737, 740 (1990); see also, ERIC POSNER & GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY 363 (Princeton University Press 2018) (“During the Gilded Age, monopolies interfered with politics in many ways; indeed, the Sherman Antitrust Act, and the reforms undertaken by the Progressives, were motivated as much by the political dangers posed by monopolies as their economic costs.”). In the UK at the beginning of the nineteenth century, “the common law negative view of monopolies was the default rule which could be modified or abrogated by statute.” Barry E. Hawk, English Competition Law Before 1900, 63 ANTITRUST BULLETIN 1, 19 (2018); see ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF 19, 412 (Basic Books 1978) (“[R]unning through the arguments and decisions of this early period was a recognition of the need to eliminate the evils of monopoly without hampering business efficiency,” and later adding that “there is always in Congress, moreover, a strong element of anticorporate populist sentiment, a desire to punish business precisely because it is successful.”).

PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 209 (Harv. Univ. Press 2018) (“Given that blockchain technology is still largely immature, there is a danger that regulating the technology too early could preclude the emergence of new and unexpected applications that have not yet been fully explored or discovered.”).

Id. at 206 (“[L]egal scholars thought that the rule of code would ultimately prevail on
dedicated rules specific to Internet regulation. The idea that the Internet required the creation of a *sui generis* body of law, however, had its fifteen minutes of glory and attracted more than its fifteen minutes of criticism. In his famous article *Cyberspace and the Law of the Horse*, for instance, Judge Frank H. Easterbrook argued that any effort to create specific rules for the “cyberspace” arena was, like efforts to create from whole cloth a special law of horses, “doomed to be shallow and to miss unifying principles.” Time has shown that the Internet did not kill general bodies of law. In fact, most of the same principles are applied today as twenty years ago, and antitrust law is but one example of this. Easterbrook was correct in his analysis. The regulation of the Internet has certainly developed on the basis of existing general principles, whether through the creation of technology-focused statutory regimes or through the fine-tuning of existing laws.

Blockchain’s technological underpinnings, however, are a radical departure even from those of the Internet. The Internet, which is primarily a communications technology, challenged the legal system by substantially increasing the speed at which the law needed to be applied, as Judge Richard A. Posner argued in his famous article *Antitrust in the New Economy*. With blockchain, it is not just about speed: the very nature of the technology raises fundamental questions about antitrust law and how individuals conduct transactions.
This article intends to contribute to the literature by describing the challenges that blockchain presents for analyses of unilateral anticompetitive practices and proposing some changes to antitrust law and regulations that address those challenges. This article is divided into three parts.

First, this article argues that, because blockchain is decentralized, anonymous, and immutable, questions arise regarding the ability to detect anticompetitive practices and their perpetrators. Answering these questions may be exceedingly difficult.

Next, this article discusses current antitrust laws and how they can properly regulate blockchain. Some legal remedies, for example, cannot be used to prevent the development of anticompetitive practices implemented through the blockchain because of the nature of the technology. It addresses how antitrust authorities should tackle these issues. On the one hand, regulators must avoid using their unfamiliarity with a new technology to justify overregulating a potentially beneficial advancement or employing what this article calls the “blockchain excuse” for regulation. On the other hand, antitrust enforcement must adapt to stay relevant, and this article suggests that regulators adopt a new methodology of “regulatory infiltration.”

But even if this new regulatory scheme is adopted, some ultimate questions demand resolution. This article seeks to address them in part three: is blockchain the death of antitrust law as we know it? Should it be? Answering those questions is not easy because blockchain continues to evolve. Nevertheless, the decentralized nature of blockchain forces us to consider the legitimacy of antitrust law, which rests on centralized legal structures and enforcement that are inconsistent with blockchain’s trustless nature; although, antitrust is still needed. This is the blockchain antitrust paradox.

I. UNILATERAL PRACTICES ON BLOCKCHAIN

Unilateral practices are anticompetitive conducts perpetrated by a single company holding a dominant position. This section evaluates how unilateral practices might be carried out on the blockchain: because the technology changes the way that an organization conducts business, blockchain will likely affect how legal doctrine is applied. To set the stage

---

20 We exclude cartels from this study in order to make this article a reasonable length. Many of the developments of this article can nonetheless be applied to cartels analysis. For a specific study of blockchain challenges created for collusive agreements, see Thibault Schrepel, Collusion by Blockchain and Smart Contracts, 33 HARV. J.L. & TECH. (forthcoming 2019).
for the legal discussion, the article first describes how blockchain functions. The second part examines how blockchains compete among themselves and shows how relative competitive power might be distributed. A third section is dedicated to the analysis of unilateral practices.

A. The Functioning of Blockchain: Setting the Stage

Blockchain is still a new technology, with rapidly evolving functionality. As a consequence, this section only focuses on the fundamental points of blockchain operation, focusing specifically on those relevant for antitrust analysis. Additionally, this article discusses the distinction between public and private blockchains, which is important because of the distinction’s implications with regards to antitrust law. Lastly, this section explores the differences between blockchain 1.0, 2.0, and 3.0 to show how blockchain is used today and the direction it may be headed.

1. General Points

The World Wide Web “enables the frictionless transfer of information”—blockchain “enables the frictionless transfer of value.”[21] In the words of Satoshi Nakamoto, blockchain is based on “cryptographic proof instead of trust.”[22] This feature makes blockchain “not a ‘disruptive’ technology . . . [but] a foundational technology”[23] that “has the potential to create new foundations for our economic and social systems.”[24]

---

[21] Katya Malinova & Andreas Park, Market Design with Blockchain Technology 1 (2016); see also Paul Vigna & Michael J. Casey, The Truth Machine: The Blockchain and the Future of Everything 21 (St. Martin’s Press 2018) (“Blockchains point the entire digital economy toward something people are calling the Internet of Value. Whereas the first version of the Internet allowed people to send information directly to each other, in the Internet of Value people can send anything of value to each other, be it currencies, assets, or valuable data that was previously too sensitive to transmit online.”); Siraj Raval, Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology 21 (O’Reilly Media 2016) (“Bitcoin was the first successful decentralized store of wealth.”).


[23] Marco Iansiti & Karim R. Lakhani, The Truth About Blockchain, HARV. BUS. REV., Jan.–Feb. 2017, at 118, 120, https://hbr.org/2017/01/the-truth-about-blockchain [http://perma.cc/57XH-TIPE] ([A]dding that “with blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries
A blockchain is an open and distributed\textsuperscript{25} ledger that can record—manually or automatically—all sorts of transactions between users.\textsuperscript{26} The transactions follow a set of algorithms and rules, which are called computational logic. In theory, each transaction’s existence is seen by all users, but the “meaning” or purpose of the transaction is kept secret because the transactions are encrypted.\textsuperscript{27} Users on either side of the transaction interact with one another using peer-to-peer transmission, with communication occurring directly between them instead of through a central point. All users are identified by a unique alphanumeric address, and so a blockchain is said to be pseudonymous.\textsuperscript{28}
Once they are recorded on the blockchain, information and transactions are permanent. They are put into blocks and each block contains the identification (called the “hash”) of the data inside the previous block. The hash is generated automatically by the blockchain, making it nearly impossible to modify or hack into a block in the chain insofar as it will automatically change its hash when any information is modified. The copy of the blockchain, with a corrupt block, will be invalidated as such. Because these transactions cannot be changed, it is said that “unlike Pinocchio, the blockchain doesn’t lie.” This theoretical immutability of blockchain presents both a cost and benefit, discussed in Part II. A. infra with regards to antitrust law.

Blockchain transactions can be seen by all users because of the distributed architecture of blockchain system. In principle, each participant has a copy of the entire blockchain on his computer, providing him with access to all information and transactions registered on it. Furthermore, no single participant controls that information; no one is in charge of public blockchains, and no one may decide unilaterally to alter them. This core principle of blockchain is the reason why no central point of failure exists. As a consequence, all damaging effects from one person’s reckless behavior are limited to that person because only his copy of the blockchain will be affected and thus, invalidated.

Lastly, when using a blockchain, every user agrees to a certain set of procedures, called the protocol, which is governing it. Once the
protocol of one blockchain is established, no deviation from it is theoretically possible unless it is decided by the majority of users. This immutability participates in creating trust.  

Establishing trust is central to the technology’s viability and the reason for the technology’s wide adoption. In 1975, Kenneth Arrow stated that “virtually every commercial transaction has within itself an element of trust,” trust being “an imperfect substitute for information.” Blockchain provides information by granting access to the ledger. By ensuring that every user has access to the ledger and establishing trust, blockchain also solves the “Byzantine Generals Problem,” according to which computer systems cannot reach consensus without relying on a central authority. Solving this problem is the defining element of blockchain’s potential. As a consequence of following the *lex cryptographia*, blockchain can do everything that a computer does but in a decentralized manner.
2. Public vs. Private Blockchain

A public blockchain, also called a “permission-less,” or “open,” blockchain, is a blockchain that anyone can read and on which anyone can propose new transactions. In most open blockchains, there is no guarding against bad actors and no access control, thanks in part to the original influence of the open source and cypherpunk movements. Applications may be added to the network without the approval or trust of others, allowing the blockchain to function as a platform layer. In practice, some public blockchains only permit a finite number of actions to be contained in a transaction, perhaps only allowing their users to send tokens among them. But most public blockchains do not impose such limitations. Transactions are generally secured by merely requiring new entries to include a proof of work.

A private blockchain, also called a “permissioned” blockchain, is a blockchain that restricts reading permissions to certain participants. The completion of new transactions is generally limited to a predetermined list of participants, and the creator of the blockchain does not generally hold a full copy of the ledger. Private blockchains are subdivided into two different categories. The first is called “single entity blockchain.” As its name suggests, a single entity will set up the protocol and run the blockchain, while reading permission may be public or restricted to certain participants. The second is called “consortium blockchain.” In such a blockchain, the consensus process is controlled by a pre-selected set of nodes. For example, the consensus mechanism could be made of five companies, each of which operates a node, and to validate a block, three would have to sign. Regardless of the technical particulars, all consortium

42 See VIGNA & CASEY supra note 21, at 99 (“How do tokens work? Just as Bitcoin’s protocol steers users and participants into certain actions that serve the community’s interest—in its case, creating a secure, reliable ledger that all can trust—the programs that run tokens incorporate incentives and constraints that encourage certain pro-social behavior. A new concept—token economics—is emerging. It encapsulates the idea that we can embed into these “programmable” forms of money a way to steer communities toward desired common outcomes. Tokens might help us solve the Tragedy of the Commons. In other words, they could be a big deal.”).
blockchains operate under the leadership of a group instead of a single entity.

In addition to private and public blockchains, there are also semi-private blockchains. Those blockchains are run by a single company that grants access to any qualified user. The following graphic shows a representation of these three different blockchains.

In practice, semi-private and private blockchains have multiple access levels. They may, for example, constitute entirely permissioned blockchains, in which a predefined list of participants with known identities perform transactions. In other circumstances, they may be less strict, such that reading transactions, proposing new transactions, or creating new blocks of transactions may be only partially restricted. This information is summarized in the table below.

---

44 For a discussion of hybrid blockchain, see Marc Pilkington, Blockchain Technology: Principles and Applications, in Research Handbook on Digital Transformations 21 (Edward Elgar ed. 2016) (“The Bank of England is currently reflecting on ways to implement ‘hybrid systems’ involving distributed ledger technology, also bearing in mind the idea of a continuum, and raising the issue of remuneration, incentives, and honest participation, so as to ensure socially efficient outcomes.”).
Blockchain types | Public blockchain | Semi-Private blockchain | Private (single entity) blockchain | Private (consortium) blockchain
---|---|---|---|---
Access | No permission required | Qualified users via online approvals | Members only | Members only, who could be co-founders
Typical implementation | As a public blockchain application | One company launches and acquires users after | Via a private blockchain implementation | Via a private blockchain implementation
Innovation target | New business models | Supporting existing models or launching new services | Supporting existing models or launching new services | Processes within existing relationships
Blockchain governance | Public consensus | Controlled by a single owner | Controlled by a single owner | Equal weight to all participants
Number of users | Millions (billions?) | Hundreds of thousands | Dozens to few thousands | Dozens to few thousands

3. Consensus and Governance

Blockchains can be classified by the way they achieve consensus. The consensus mechanism is the general agreement, unanimous by nature, under which the blockchain operates. Blockchain integrity relies on the chosen consensus to clear transactions. Together with other potential mechanisms that may be introduced on blockchains in order to regulate it, they form the governance of the latter.

Most of today’s major public blockchains (e.g., Bitcoin and Ethereum) currently use the proof of work form of consensus, in which some users—here called miners—are racing to solve a cryptographic puzzle in order to be chosen to verify the integrity of transactions. The first to solve it is rewarded by receiving a transaction fee. Many public blockchains are currently working on developing proof of stake consensus achieved by cryptoeconomics and game theory.

45 See generally Winston Maxwell & John Salmon, A Guide to Blockchain and Data Protection 16 (Hogan Lovells 2017), https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf ([https://perma.cc/M257-7QGL] stating that “off-chain” mechanisms are used to store confidential information separately on another platform while “sidechains” are parallel blockchain working alongside the primary one.).

46 See Vigna & CaseY supra note 21, at 39 (“Consider that Bitcoin is now the most powerful computing network in the world, one whose combined “hashing” rate as of August 2017 enabled all its computers to collectively pore through 7 million trillion different number guesses per second. Well, it would still take that network around 4,500 trillion trillion trillion years to work through all the possible numbers that could be generated by the SHA-256 hashing algorithm that protects Bitcoin’s data.”).

In the words of Ethereum founder Vitalik Buterin, “public blockchains are secured by cryptoeconomics—the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake.” With private blockchain, however, there is generally no mining, no proof of work, and no remuneration. The benefits of private blockchain come from its valuation and applicability. Uses of private blockchain include (1) serving as a transfer value (currency, securities, votes, industrial patents, Internet of Things (IoT), stocks, bonds), (2) serving as a register to verify the exchange of products and assets; and (3) serving as a smart contract by enabling an automatic program to insert terms and conditions.

Whoever controls the consensus—also known as the consensus mechanism—controls the governance of the blockchain. The consensus operates and communicates between network nodes. It creates an economic incentive structure in some blockchains (including Bitcoin) because it creates convergence without coercive action. The proof of work

---

48 For instance, Ethereum is said to intend to migrate to proof of stake. 
49 Some private blockchains use proof of work and are moving to proof of stake. 
50 On the contrary, the main incentive to use public blockchains is that using it brings value, and value brings profitability. 
52 Id. 
54 Guegan, supra note 51, at 5. 
system incentivizes a solution to the “Byzantine Generals Problem.”\textsuperscript{58} In these situations, it is not possible to implement unilateral strategies regarding the blockchain because there is no central source of power. However, some blockchains are already implementing new mechanisms on top of the consensus in order to create more sophisticated governances.\textsuperscript{59} For instance, Dash, a crypto-currency,\textsuperscript{60} uses a governance system that allows its users to vote if they hold tokens.\textsuperscript{61} Decred\textsuperscript{62} and Tezos\textsuperscript{63} are also crypto-currencies with more centralized governance systems. In fact, one of Tezos’ main characteristics is its ability to amend its consensus when necessary.\textsuperscript{64} Further, more traditional systems such as “off-chain” and “sidechain” mechanisms\textsuperscript{65} are in development. The mechanism called BIP 9 already allows Bitcoin developers to probe miners about technical changes. By doing so, blockchains supplement the sole consensus mechanism (and create new opportunities for unilateral conduct).

An empirical study of these different types of blockchain governance should be conducted with antitrust laws in mind once the blockchain governance systems are more developed. A blockchain’s ability to implement anticompetitive strategies will vary depending on the governance system of the blockchain. The day blockchain governance is entrusted to artificial intelligence,\textsuperscript{66} even more opportunities to implement

---

\textsuperscript{58} Lamport et al., supra note 37, at 382 (“Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement.”). For a technical analysis of the byzantine agreement, see ROGER WATTENHOFER, THE SCIENCE OF THE BLOCKCHAIN 33 (CreateSpace 2016).


\textsuperscript{60} See DASH, https://www.dash.org [https://perma.cc/3WVH-X2T3].

\textsuperscript{61} Some of these users, called Masternode, have more power into the community.

\textsuperscript{62} See DECREd, https://www.decred.org/ [https://perma.cc/VWE7-97DT].


\textsuperscript{64} See id. (“protocol can be amended to reflect virtually any blockchain based algorithm”).

\textsuperscript{65} See Zamfir, supra note 47 for a description of developments of “off-chain” and “sidechain” mechanisms. For a description of this need, see Benito Arruñada & Luis Garicano, Blockchain: The Birth of Decentralized Governance 1 (2018) (“For blockchain to fulfill its promise and outcompete centralized firms, it needs to develop new forms of ‘soft’ decentralized governance (anarchic, aristocratic, democratic, and autocratic) that allow networks to avoid bad equilibria.”).

\textsuperscript{66} Melanie Swan describes blockchain as a “path to artificial intelligence.” See SWAN,
such illegal practices will appear, but for now, the technology is not quite ready yet.

4. From Blockchain 1.0 to Blockchain 3.0

Antitrust concerns about the blockchain platforms and the software operating on it address different types of anticompetitive practices: those that are committed via the blockchain itself as a platform and those that are committed via the applications working on the blockchain.

Not all blockchains allow a software layer (“layer 2”) to run on top of the root blockchain (“layer 1”) as described above, but most do. Ethereum, for example, is a root blockchain that allows any type of software layer. In fact, Ethereum was specifically built to allow users to create “smart contracts,” or agreements between accounts to automatically transfer tokens when certain conditions are met. Anyone can upload a program onto this platform and leave it to self-execute securely.

These blockchain applications can be distinguished by three generations of blockchain. The first, blockchain 1.0, is similar to a currency and includes “cash, such as currency transfer, remittance, and digital payment systems.” The second, blockchain 2.0, is a contract, including “stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts.” This category includes all blockchains allowing

---

supra note 3, at 26. She contends that “blockchain technology facilitates the coordination and acknowledgment of all manner of human interaction, facilitating a higher order of collaboration and possibly paving the way for human/machine interaction. Perhaps all modes of human activity could be coordinated with blockchain technology to some degree, or at a minimum reinvented with blockchain concepts.” See id. at 27.

67 Peder Østbye, The Case for a 21 Million Bitcoin Conspiracy 3 (Mar. 7, 2018) (“Most software implements a rule that only valid transactions are propagated further to the network. This is however no hard rule, but dependent on users following the protocol.”).

68 See DANNEN, supra note 33, at 3 (“In Ethereum, the protocol is designed for building decentralized applications, with emphasis on rapid development time, security, and interactivity.”).

69 Id. at 51 (Smart contracts are therefore not necessarily contracts in the legal sense).

70 TAPSCOTT & TAPSCOTT, supra note 28, at 221.

71 SWAN, supra note 3, at 23–24 (explaining that there are different smart contracts on “a potential progression to increasingly complex and automated smart contracts.” The first, Dapp, is an application that runs on the blockchain. DAO, the second, is more complex, with “a constitution, which would outline its governance publicly on the blockchain, and a mechanism for financing its operations. DACs are similar to DAOs but organized under another legal form. The third is called DAS and gathers smart contracts and/or Dapps, DAOs and DACs.”); see also RAVAL, supra note 21, at 1 (anticipating that Dapp will someday “become more widely used than the world’s most popular web apps.”).

72 SWAN, supra note 3, at ix.
applications that enable these financial activities.\footnote{See \textit{id}.} Finally, blockchain 3.0 includes all “applications beyond currency, finance, and markets—particularly in the areas of government, health, science, literacy, culture, and art.”\footnote{\textit{Id.}}

All major blockchain platforms, even private blockchains such as Corda and Hyperledger, are open source or offer an open source version. Therefore, these three types of applications can be developed freely on most blockchains. Today, it seems unlikely that a closed-source blockchain platform, in which the code is not public, would succeed.\footnote{Indeed, only open-source blockchain can rely on token effects, which are key to their growing in a competitive environment, see the discussion of token effects, below.} Note, however, that there is no requirement that software be open source.\footnote{See \textit{WERBACH, supra} note 39, at 106.}

To this day, major closed-source software has yet to be created, and accordingly, this paper mostly focuses on open-source blockchain as a platform.

B. At War: Competition Between Blockchains and Non-Blockchain Platforms or Applications

Today, competition between tech companies such as Google, Facebook, Uber, and Amazon garners significant public attention.\footnote{See Juan Manuel Sánchez-Cartas, & Gonzalo León, \textit{Multisided Platforms and Markets: A Literature Review} (Jan. 2019) https://www.researchgate.net/publication/325225786_Multisided_Platforms_and_Markets_A_Literature_Review [https://perma.cc/M6FQ-DLS6].} Soon, competition between blockchains, but also between blockchains and non-blockchain platforms and applications, may be a topic of great interest as well.

1. The Token Effect

The competitive pressure between blockchain technologies and services is high because different foundations and companies aspire to lead the market. The intensity of that competition means that today’s dominant blockchains are not secure in their market positions. This section focuses on the synergies which may help blockchains maintain dominant market positions. For that purpose, two questions must be asked: can blockchains benefit from network effects? Is the agglomeration effect of users different on the blockchain than it is on other kinds of platforms? This article answers both questions in the affirmative.
Network effects are often examined in the literature on digital sectors. These effects are twofold: direct and indirect. The theory is that the more a technology is used, the more new users are encouraged to join the group. This scaling effect, described as Metcalfe’s Law in the context of information technology, calculates the value of a network to be approximately proportional to the squared number of users (people plus machines) that it connects. At a tipping point, once a certain number of users is reached (called the critical mass point), the value derived from the product or service is greater than its price, hence the eagerness of new users to join. And because of that cyclical mechanism, competition is more difficult. The question is: could blockchain be the way out of existing network effects? In other words, could blockchain be used to compete more easily with non-blockchain applications enjoying a strong network effect? As discussed below, this seems very likely.

With blockchain, data is public and shared by the distributed ledger system. This creates an incentive to spread the information about the existence of the blockchain in order (1) to make it effective against third parties and (2) to encourage other users to share information on it. In the words of Fred Ehrsam:

> [O]pen data has the potential to commoditize the data silos most tech companies like Google, Facebook, Uber, LinkedIn, and Amazon are built on and extract rent from. This is great for society: it incentivizes the creation of a more open and connected world. And it creates an open data layer for AIs to train on.\(^3\)


80 Cf. John M. Newman, Complex Antitrust Harm in Platform Markets, CPI ANTITRUST CHRON. 3 (May 2017) (“reputation has emerged as one of the most vital facets of competition in many modern markets”).

81 See Neil Gandal & Hanna Halaburda, Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market, 7 GAMES, at 3 (2016); see also Abeer El Bahrawy et. al., Evolutionary Dynamics of the Cryptocurrency Market, 4 ROYAL SOC’Y OPEN SCI. 11 (Nov. 2017).

82 See ERIC A. POSNER, LAW AND SOCIAL NORMS 221 (Harv. Univ. Press 2009) (explaining that Marx and Weber have argued that the market—or, capitalism—undermines community. Blockchain, driven by capitalism, proves this analysis to be incorrect).

The incentive system created on public blockchain also creates a strong inducement to join quickly, contrary to what happens on digital platforms outside of the blockchain eco-system.\(^4\) Indeed, network effects are created by a critical mass, meaning that there is a real connection between the number of users and the utility of the product or service. Therefore, when the critical mass is not reached, the interest in joining the network of existing users is low. Blockchains, however, operate differently because they are “adding financial utility when application utility is low,”\(^5\) as summarized in the following figure:\(^6\)

![Network effect](image)

**Network effect**

Willingness for an user to join once the critical mass is reached

Utility of the product or service

Number of users

![Token effect](image)

**Token effect**

High incentive for an user to join before the token value is too high

Utility of the product or service

Number of users

This article refers to network effects on blockchains as “token effects,” and indeed, they operate somewhat differently than network effects. Token effects are created more easily on blockchain than network effects off blockchain because of the financial disconnect created between the incentive to join the service and its utility.\(^7\) Initial Coin Offerings,\(^8\)

---

\(^4\) Werbach, supra note 39, at 89 (describing how the blockchain eco-system could provide incentives for users to engage with what could become the next Facebook).


\(^6\) See id. (illustrating Dixon’s ideas).

\(^7\) For instance, Steemit, a decentralized Reddit-like token network, makes payments to
for instance, incentivize coin holders to make the blockchain well-known and prosperous as soon as possible. Other blockchains give away tokens, which is called an “airdrop.” When doing so, they usually impose several conditions, the most common is the creation of a user account via a social network in order to get access to the new user’s entire contact list. Here, the incentive to join is particularly high when the value of the tokens is low. This phenomenon is not seen outside of blockchain because companies would have to give dollars and euros to attract customers, which would be prohibitively costly.

In short, because of the token effect, blockchain could set up new rules of competition. Token effects might also explain why public-ledger currencies have been extremely volatile thus far. This raises concerns

users who post and upvote articles.


89 See Dirk Zetzsche et al., The ICO Gold Rush 6 (2018) (offering “a taxonomy of initial coin offerings”); cf. Christian Catalini & Catherine Tucker, Seeding the S-Curve? The Role of Early Adopters in Diffusion 1 (2016) (“We then show not only that natural early adopters are more likely to reject the technology if they are delayed, but that this rejection generates spillovers on adoption by their peers who are not natural early adopters.”).

90 For example, Mtoken, Betherum, Sharelectric, Xriba, ConcertVR, Blockport, Wr, Articlenx. See What New ICOs Are Giving Away Free Tokens Right Now?, QUORA, https://www.quora.com/What-new-ICOs-are-giving-away-free-tokens-right-now [https://perma.cc/RM9B-YHWY]. To track them, see Airdrop Alert.com, https://airdropalert.com [https://perma.cc/AF6P-FLJ8]; see also Vigna & Casey, supra note 21, at 103 (“Brave’s model included a token-issuance strategy for dealing with that challenge. It set aside a 300 million–strong ‘user growth pool’ to attract new users. There’s a plan, for example, to deliver a small number of BATs to the integrated Brave wallet whenever there’s a unique new download of the browser. In this way, the token is designed as a tool to bootstrap adoption, to foster network effects.”).

91 This is also called a “coin drop.” See Swan, supra note 3, at 73.


94 See David S. Evans, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms (Coase-Sandor Inst. for L. & Econ. Working Paper No. 685, 2014) (explaining that in 2014 Bitcoin was “more than 18 times more volatile than the Euro”). See generally June Ma, Joshua S. Gans & Rabee Tourky, Market Structure in
about the stability of crypto-currencies and, more generally, about the stability of blockchain. As previously argued, the intrinsic characteristics of blockchain might cause token effects to be created even faster than network effects; however, they may also disappear faster. Will blockchain lead to a new era of “serial monopolies”? It remains to be seen, but the nature of token effects makes this hypothesis likely.

2. Competition for End Users

The competition that blockchains will pose to traditional platforms due to the token effect is reinforced by the fact that this technology does not need middle-market companies to run. In the words of Vitalik Buterin, founder of the Ethereum, “blockchains will drop search costs, causing a kind of decomposition that allows you to have markets of entities that are horizontally segregated and vertically segregated.” It is then expected that competition will shift to end users, endangering big tech firms precisely because they are middleman firms in the transactions they offer. Middleman firms have existed throughout history, but blockchain could lead to a reduction in their usefulness by helping “self-sovereign identity” to become mainstream. Instead of being asked to

---


95 Darcy Allen, Chris Berg & Mikayla Novak, Blockchain: An Entangled Political Economy Approach 13 (2018) (“The potential significance of crypto-entities from an entangled political economy perspective cannot be understated. The blockchain enables virtual start-ups and open-source enterprises to directly compete with entrenched, conventional-economy incumbents with inflated transactions costs and locked-up rents.”).

96 Although some intermediaries will remain. See De Filippi & Wright, supra note 13, at 8 (“Even though blockchains create increasingly autonomous and potentially lawless systems, there are still means to shape and control their use and deployment. Blockchains may reduce the need for intermediaries, but they are unlikely to eliminate them altogether.”); Tapscott & Tapscott, supra note 28, at 54 (quoting an interview with Vitalik Buterin, stating “instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.”).

97 Tapscott & Tapscott, supra note 28, at 183 (quoting a September 2015 interview with Vitalik Buterin).

“Login with Facebook” on a website, you may one day “Connect with Bitcoin.”

As a consequence, there is a potential scenario where “no intermediary brokered the deal; no social-media network captured the data from [a] transaction to better target its advertising; no credit bureau tracked the activity to build a portrait of [an individual’s] financial trustworthiness.” Social media, for instance, could only hold the data generated by use of the service (such as likes and other activities on the platform), and in such case, users would keep total control over their data (including photos, statuses updates, etc.). If this were to happen, blockchain would greatly diminish the power of existing platforms by reducing the completeness of their database. This would create competition on the platform rather than for the platform. It is also technically possible to store all data (including that generated by the use of services such as social media) on the user’s private blockchain or across many hard drives throughout the blockchain network, leaving the product or service developers with no data in hand. The platforms would have to find new ways to incentivize their users to give access to their data. In other words, because of blockchain, the business model of digital products and services may need to be entirely rethought in the coming years.

C. Which Unilateral Practices to Expect: The Crystal Ball

Blockchain poses two problems: it complicates both the characterization of dominant market positions and the attribution of liability for anticompetitive practices. This is particularly concerning because anticompetitive practices are expected on blockchain, as demonstrated below by analyzing how and why monopolization practices could be implemented on it.

99 See SWAN, supra note 3, at 35 (explaining that BitID offers “a decentralized authentication protocol that takes advantage of Bitcoin wallets as a form of identification and QR codes for service or platform access points. It enables users to access an online account by verifying themselves with their wallet address and uses a mobile device as the private-key authenticator”); RAVAL, supra note 21, at 26 (“Due to the recent advancements in cryptography, a lot of the solutions have been ‘assume a public-key infrastructure.’ Basically, assume that people would be willing to store a private key safely and identity will be decentralized. Only those with the keys would have access to it. BitAuth is a good current example of this.”).


101 WERBACH, supra note 39, at 238.
1. The Dominant Position (Relevant Market)

Defining relevant markets—a tool to define the boundaries of competition between firms taking into account material and geographical dimensions—on digital markets can be challenging. This is especially true where services are proposed on “zero-price markets.”\(^{102}\) As a result, the definition of the relevant market seems to be a legal deception. In fact, it is hard to imagine that an antitrust authority would withdraw its investigation against some Internet giants because the dominant position could not be shown. And yet, the relevant market must be properly defined so that only the practices of dominant companies will eventually be sanctioned.

Blockchain raises important questions about what exactly a dominant position is. And because decentralized organizations, like blockchain, are not recognized as legal entities,\(^{103}\) numerous questions arise such as, “can a non-entity hold a dominant position?” Can blockchain create a “monopoly without a monopolist?”\(^{104}\) Lastly, if blockchain is dominant, which users and/or entities hold that dominant position? Depending on how a dominant position is characterized, liability will be assigned in different ways considering the fact that an entity that holds a dominant position is fully liable for the practices implemented within it. The same is true for blockchains: the way in which the dominant position is characterized will determine the scope of liability.

There are a number of characterizations of dominance that could be applied to blockchains. As far as the material dimension of relevant markets is concerned, different theories of liability are conceivable.

The first theory of liability would be to consider that all blockchains hold a dominant position in and of themselves. Excluding all of the issues related to the characterization of dominance, each blockchain—as a ledger on which transactions are registered—would constitute a relevant market. If this were the case, all blockchain users would be considered co-holders of this dominant position. Accordingly, the liability for anticompetitive practices would fall on all of them, creating an inseparable whole. In practice, however, it would be illogical to consider all blockchain platforms to hold a dominant position while attempting to prevent the implementation of anticompetitive practices by a fraction of the users. Retaining such a market definition would considerably reduce the incentive to use blockchains, since unwitting users could be held liable for practices performed by third parties unknown to

---

103 De Filippi & Wright, *supra* note 13, at 143.
104 See generally Huberman et al., *supra* note 55.
them. As such, this first way of defining dominant positions should be rejected.

A second option would be to evaluate the dominance of blockchains based on the number of users. In this scenario, blockchains with the most users would be seen as dominant, regardless of the applications running on each platform. But this poses a problem in terms of blockchain substitutability, which is central to a market definition. It follows that the liability for anticompetitive practices would fall on all of the users. But should the dominant position be characterized by all of the blockchain users even though they are distinct entities? Should they be considered to hold a collective dominant position? This would solve the issue relative to the fact that blockchain is not an entity, and yet, the possibility must be ruled out. Under European competition law, collective dominance implies the finding of economic links between undertakings enabling them to adopt the same line of action on the market.\footnote{Case C-68/94, France v Comm’n, 1998 E.C.R. 1-1375.} Such links do not exist on blockchain; a tiny fraction of users is interacting with another tiny fraction of users when they are co-contractors. Other users simply verify the authenticity of transactions without being involved in them. This characterization of dominance should therefore be rejected.

A third option would be to evaluate the power of blockchains based on the number of recorded transactions, revenue linked to the number of transactions, or the number of blocks. If blockchains are considered dominant under this standard, they would be entirely liable for all of their users’ practices. This raises causation problems.\footnote{Jeff Miles, \textit{Principles of Antitrust Law}, AM. BAR ASS’N (2016), https://www.americanbar.org/content/dam/aba/administrative/healthlaw/01_antitrust_primer_01.authcheckdam.pdf [https://perma.cc/XMF2-W85Y]; see also Hanns A. Abele, Georg E. Kodek & Guido K. Schaefer, \textit{Proving Causation in Private Antitrust Cases}, 7 J. COMPETITION L. & ECON. 847 (2011).} For example, the foundations who introduced blockchains do not control how they are used, nor do they control the information and transactions published on them. Once again, this third option has an inherent flaw because blockchains are not necessarily interchangeable. For these reasons, this third option should be rejected.

A fourth option would be to evaluate the respective market power of blockchain users, and accordingly, some blockchains would be deemed dominant if their users are key players on their respective markets. In short, the market definition would not be linked to the technology of blockchain but to all different sorts of external markets. This approach would preserve most users’ interests in using the blockchain as well as incentivize dominant users to prevent anticompetitive conduct on the blockchain. And yet, it must be ruled out because it would make the
assessment of market power extremely complex and, above all, would greatly reduce the legal certainty of blockchain users who would logically ignore the power of other users on their respect markets.

A fifth option consists of evaluating the dominance of blockchains based on their type of governance. Accordingly, public blockchains would compete in one market while private blockchains would compete on a different market. But this option is unworkable. An open-source platform can compete with a proprietary platform, and for the same reason, a private blockchain can compete with a public blockchain. The same could be said of evaluating the dominance of blockchains based on the type of consensus each blockchain uses. It only has the merit of showing the need to take into account the type of service provided by the blockchain.

A sixth, and final option, is the only viable solution. This approach determines market power based on the type of applications (products and services) that run on the blockchain as a layer 2. The type of blockchain (1.0, 2.0, or 3.0), which are different strata of smart contracts, will then be at the center of the market definition in which the biface nature of the market will be taken into account by analyzing the functioning of applications. Notably, layer 1 blockchains as a platform would be part of a different market because they do not compete with layer 2 applications.

Under this approach, the blockchain market power would be assessed in comparison with other digital products or services, and potentially, non-digital alternatives. As a result, blockchain power would be evaluated the same way online sales can be integrated into the general sales market (including physical sales). This would address the issue of what are reasonably effective substitutes. This option follows a more classical definition of relevant product markets.

Characterizing a dominant position this way would make it possible to retain liability only for users who offer, run, or use a dominant

107 A distinction would be further made on whether the blockchain allows the realization of a service taking place outside of the technology, or whether it provides a service within the blockchain. In the first case, it will have to be determined whether blockchain can be integrated into a wider market—as it is the case, for example, with online sales that can be integrated into the general sales market (including physical sales). In the second case, only competition between blockchains will have to be evaluated.

108 Namely smart contracts, Dapps, DAOs, DACS, DASs and DASs. See discussion, supra note 71; see also Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305 (2017) ([D]istinguishing between strong and weak smart contracts “as defined by the costs of their revocation and modification.”).


110 See for instance case 39740, Google Shopping, 2017 E.C.R. 145, in which the market definition was established by comprising the totality of interchangeable products or services.
application that has implemented an anticompetitive practice. It would
then allow antitrust authorities to make a distinction between three key
players on the blockchain: developers, users, and miners, depending on
who commits the anticompetitive practice.111

Left unanswered, however, is the question of which elements to take
into account in order to evaluate the power between blockchains running the
same type of applications: the number of users, the number of transactions
recorded, the number of blocks, the revenues, etc. In the Google
decision, the court noted that the European Commission has used market shares by
volume as a proxy for several reasons.

First, market shares by value cannot be computed because
general search services are provided free of charge to the
user. Second, despite its best efforts, the Commission has
been unable to obtain precise and verifiable values regarding
the Revenue Per Search (“RPS”) of the main general search
services. Third, advertisers look at usage shares when
deciding where to place their search advertisements.”112

But are these reasons true for all blockchain platforms? The answer
will depend on how blockchains evolve in the future, but for now, the
answer appears to be no. Thus, all signs suggest that different elements will
have to be taken into account on a case-by-case basis. For example, in some
instances, the number of active users in combination with the revenues113
will be assessed, while in other circumstances, the number of active users
will be compared to the number of transactions.

As far as the geographical dimension of relevant markets is
concerned, it should be stressed that although the language used on
blockchain is universal, some applications may be focused on a local market
while others may compete globally. Here, only a case-by-case analysis is
possible.

In short, establishing a methodology for assessing dominance is
needed insofar as it increases legal certainty for all blockchain players.
Whether such a methodology can be rapidly established remains to be seen.
Furthermore, evaluating market power of a blockchain network creates new
challenges, the extent of which will only be measured in the coming years.
One challenge, for instance, is tied to the absence of central power, and the

111 See Schrepel, supra note 57 (providing an analysis of the three categories of players).
112 See id. at 275.
113 Also, let us stress the difficulty to compare blockchain revenues when their tokens are
not convertible into the same currency. In addition, the value of tokens fluctuates widely,
which can cause major difficulties in terms of valuation.
need to ask the majority of blockchain users to adopt changes, which greatly mitigate the idea of “power.”

2. The Abuse of Dominance

This section focuses on unilateral practices that are directly related to “layer 1” blockchain. Practices that originate outside a blockchain, such as the imposition of unfair terms by smart contract or the tracking of products are not addressed because they do not pose the same degree of difficulty and because they are too numerous to be studied in a single article. The same goes for anticompetitive practices taking place on “layer 2” blockchains, meaning, on software using blockchain. Still, two questions remain: (1) does blockchain further enable anticompetitive practices that are already recognized? And (2) does blockchain give rise to new anticompetitive practices that are related to the technology? Both questions may be answered in the affirmative.

This article discusses these different types of unilateral practices: exploitation, exclusion, and discrimination. This article also distinguishes between public and private blockchains. Indeed, the governance design of private blockchains allows the platform to be piloted by one or several

\[^{114}\text{This is seen, for instance, with Ethereum, which has to convince its own users to adopt upgrades to the software. See Christine Kim, \textit{Ethereum Upgrades as Hard Forks Activate on Blockchain}, COINDESK (Feb. 28, 2019) https://www.coindesk.com/ethereum-upgrades-as-hard-forks-constantinople-and-st-petersburg-activate-on-blockchain [https://perma.cc/SPR7-CMR5]. Note that when a blockchain is changing its functioning rule, such as the protocol consensus, all blocks validated according to the new rules are seen by the blockchain software as being invalid. For that reason, all nodes need to upgrade their software to the new rules.}\]

\[^{115}\text{This article does not address cartel issues, for more on that topic, see Cong & He, \textit{supra} note 9, at 1 (“Smart contracts can mitigate informational asymmetry and improve welfare and consumer surplus through enhanced entry and competition, yet the distribution of information during consensus generation may encourage greater collusion.”}).}\]

\[^{116}\text{See Chris Reed, \textit{et al.}, \textit{Beyond BitCoin—Legal Impurities and Off-Chain Assets}, 26 INT’L J. L. & INFO. TECH. 160 (2018) (explaining how to use the blockchain for assets which exist outside the blockchain itself).}\]

\[^{117}\text{See Kevin D. Werbach & Nicolas Cornell, \textit{Contracts Ex Machina}, 67 DUKE L.J. 313 (2017) (smart contracts); Cong & He, \textit{supra} note 9, at 11 (providing a natural functional definition of smart contracts as “digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution.”}).}\]

\[^{118}\text{See VIGNA & CASEY, \textit{supra} note 21, at 148 (tracking could be used to ensure compliance with a fixed price, for example).}\]

\[^{119}\text{Buterin, \textit{supra} note 59 (“[P]eople who think that the purpose of blockchains is to completely expunge soft mushy human intuitions and feelings in favor of completely algorithmic governance (emphasis on “completely”) are absolutely crazy.”}).}\]
users who are not purely relying on the consensus mechanism. The same is not true of public blockchains, and for that reason, there is no real possibility of implementing unilateral strategies on public blockchains unless they have been designed in such a way from the day they are created. As things stand, anticompetitive practices are then more likely to be found on private blockchains. However, because most blockchains are currently working on the introduction of sophisticated governance systems, this article takes a step ahead of the currently deployed technology and describes unilateral strategies that will be implemented on public blockchain once new governance systems are democratized.

Even though it was hacked, TheDAO demonstrates the type of programmable organizational governance that is possible on a blockchain, such as off-chain and “sidechain” mechanisms. Governance systems will exist on a spectrum from those permitting easy modifications of governing rules to those with stricter forms of governance control.

The table below helps to identify which kinds of unilateral practices are the most likely to occur, understanding that damage to the consumer must be proven on a case-by-case basis for all of them, as it cannot be presumed. The table will have to be revised depending on the evolution of the blockchain technology in the years to come but can nonetheless be used as a first canvas. Here is an estimate of how likely the following anticompetitive practices will soon appear:

---


121 See DE FILIPPI & WRIGHT, supra note 13, at 137 (demonstrating that so far, blockchains are “managed primarily by distributed consensus—using smart contracts to aggregate the votes or preferences of token holders”).

122 The DAO is a participatory investment fund operating on the Ethereum. It takes the name of DAO (“decentralized autonomous organization”), but it must be distinguished from it.

123 DE FILIPPI & WRIGHT, supra note 13, at 138 (“TheDAO represented the first significant experiment with programmable organizational governance. Following the example of TheDAO, other blockchain-based organizations have emerged—including Digix.io and MakerDAO—which operate using a consensus-based governance model.”).

124 See id.
Before analyzing these unilateral practices in greater detail, two common patterns deserve emphasis. First, all information and transactions recorded on public blockchains are, to some extent, visible by all,\footnote{Most of the data put in the blockchain is encrypted so that only people with the right keys can decrypt it. However, the “visible effect” remains the rule and the protocol design is visible by all. Therefore, when anticompetitive practices are set up in the blockchain, that information is visible. Only the manifestation of that practice may be encrypted.} which this article calls the “visibility effect.”\footnote{For an example with a random wallet address, showing how easy it is to check up every incoming and outgoing transaction from a known wallet, see Bitcoin Address 1439q4Na8v88kPBqoyg8F4ueL9SYr8ANWj, https://blockchain.info/address/1439q4Na8v88kPBqoyg8F4ueL9SYr8ANWj [https://perma.cc/H7D7-U92J].} As for private blockchains, the transactions are only visible to its users if they are designed that way.\footnote{Privacy blockchain-based cryptocurrencies widely use “zero knowledge proof,” which provides trust. Trust in the system is also ensured by the fact that transactions are visible by all users. The more there are, the more trust there is in the blockchain and the higher its utility. It is therefore uncertain whether private blockchains will, in the future, make transactions non-visible.} Therefore, the number of anti-competitive practices may be lower on public blockchains than in other tech markets, precisely because public blockchains create greater transparency between users.\footnote{SUN Tzu, THE ART OF WAR 25 (Yuan Shijing trans., 1998). As stated by Sun Tzu, “what...}
one should expect that because transactions can be seen by all users on the blockchain, the inherent transparency creates a disincentive to implement anti-competitive practices in the first place, thereby reducing their occurrence. But vigilance is required because unilateral practices won’t entirely disappear due to blockchain second pattern, known as the “opacity effect.” On blockchain, all transactions are encoded, and the identity of blockchain users is protected by pseudonymity. As a consequence, the existence of a transaction may be visible, but the nature and purpose of the transaction are unknown to outsiders, which makes the interaction between users more opaque. This “opacity effect” is even stronger on private blockchains where the content of the blockchain is kept secret to outsiders.

To demonstrate which unilateral practices could be implemented on blockchain, hypothesize company $X$ operating in a digital market. $X$ decides to diversify its activities and creates a private blockchain to do so. $X$ designs the blockchain so that $X$ can choose which users may access the blockchain, which operations the users can perform on it, and which protocol will govern the blockchain. $X$ has the power to change these settings at any time. To generate revenue, $X$ has developed a new professional social network called TrustJobs, that operates as a layer 2 on its blockchain. TrustJobs enables users to either post job offers and/or apply to them. At each stage of the recruitment process—from the first interview to the acceptance or refusal of an offer—a smart contract is recorded on the blockchain. Everything is conveniently automated, but the registration of each of these transactions has a cost that the users looking for candidates pay for with tokens. After a while, this application attains great success, and $X$ realizes that some of its competitors are using TrustJobs to recruit candidates that will enable them to better compete with $X$. In response, $X$ implements an anticompetitive strategy.

i. Exclusionary Abuses

1. Refusal to deal. First, a company like $X$ might simply refuse to do business with a rival. Refusal to deal is a common practice outside

---

129 See WERBACH, supra note 39, at 45.

130 For a general overview on European refusal to deal, see Case C-7/97, Oscar Bronner v. Mediaprint Zeitungs und Zeitschriftenverlag, 1998 E.C.R. I-7796; Cases T-374/94, T-375/94, T-384/94, and T-388/94, European Night Servs. Ltd. (ENS) v. Commission, 1998 E.C.R. II-3141; Case T-301/04, Clearstream Banking AG v. Comm'n, 2009 E.C.R. II-3155. In short, refusing to provide access to a facility is abusive if it is likely to eliminate all competition on the secondary market, if access is indispensable for entering the market in question, and if access is denied without any objective justification. For an
blockchains, but it is expected to be more rare within blockchains, at least when it comes to public blockchains. A refusal to grant access to a blockchain would have to be implemented within its governance design, which is otherwise coded to allow public access. No deliberate or exclusive user selection is necessarily possible. Accordingly, refusal to deal can only be made possible by modifying the access rules themselves. Exclusionary strategies, then, are inconsistent with the inherent nature of public blockchains, and the blockchains implementing them will no longer properly be “public” blockchains.

By way of contrast, the refusal to grant general access is an essential characteristic of private blockchains. Within such permissioned blockchains, users can restrict who can enter and who can create smart contracts. Going back to the TrustJobs example, company $X$ is running a private blockchain and may refuse access to competitors $Y$ and $Z$. Furthermore, even if $X$ granted access to $Y$ and $Z$, $X$ could change its original decision or, alternatively, could engage in a refusal to deal scheme by means of (1) preventing some users from reading the information on the blockchain, (2) forbidding them from proposing new transactions on the blockchain, or (3) keeping them from validating blocks. Per IBM:

[A] private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter . . . The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue

overview of American refusal to deal, see Verizon Comm. Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004), in which the court suggested that a refusal to deal motivated solely by a desire to eliminate competition, with no other purpose, might constitute illegal monopolization. To establish liability under the essential facilities doctrine, a plaintiff must show that the monopolist holds control over the essential facility, the plaintiff’s inability to duplicate the essential facility, the denial of use of the facility, and the feasibility of providing access to the facility.

The refusal to grant access to the blockchain could be an abuse of dominant position if decided by one company, but it could also be a cartel if the blockchain is run by a consortium.

De Filippi & Wright, supra note 13, at 31. (“A number of alternative ‘permissioned’ blockchains have emerged. These blockchains rely on a peer-to-peer network, but they are not open for anyone to join. Rather, a central authority or consortium selects the parties permitted to engage in a blockchain-based network, imposing limits on who can access or record information to the shared database. Consortium members ultimately control membership, thus creating an environment where each party on the network is known or somewhat trusted.”).
licenses for participation; or a consortium could make the decisions instead.\textsuperscript{133}

Such a refusal to grant access bears similarity to the issue of standard essential patents. Obtaining a license to such patents is deemed essential in order to compete on the market, and for that reason, holders of such patents are strongly encouraged to license them on fair, reasonable, and non-discriminatory (FRAND) terms so as to avoid any breach of antitrust law. One can therefore imagine the development of similar case law in which private blockchain holders will have no choice but to grant access to their blockchains on reasonable and non-discriminatory terms if access to the blockchain is deemed essential to compete. For that reason, a firm that runs an essential private blockchain might soon be prohibited from setting certain access terms which create a strong exclusionary effect. In fact, blockchain gatekeepers (the ones in control of private blockchains) should already consider whether refusing access to third parties is compliant with antitrust law.\textsuperscript{134}

In the United States, \textit{Trinko}\textsuperscript{135} made it clear that the profit sacrifice test should be applied to refusal to deal cases in assessing the legality of the practice at issue. Referring to \textit{Novell v. Microsoft}, the court found “willingness to forsake short-term profits to achieve an anticompetitive end” as a key element of finding liability.\textsuperscript{136} However, the sole fact of proving that a company has sacrificed its profits is insufficient to show a violation.\textsuperscript{137} For instance, a company may want to temporarily waive its profits in order to build customer loyalty, which is not necessarily anticompetitive. Moreover, this test assumes that all practices that do not generate any profit in the short, medium, or long term are necessarily anticompetitive, which might lead to numerous types of errors (wrongful conviction of a pro-competitive practice). Finally, it wrongly gives a free pass to all anticompetitive practices in which the losses incurred are immediately recovered.\textsuperscript{138} For all these reasons, this test is ineffective.


\textsuperscript{136} Novell, Inc. v. Microsoft Corp, 731 F.3d 1064, 1076–77 (10th Cir. 2013).


In Europe, the “as-efficient-competitor” test, asking whether an equally efficient rival could compete in the presence of the challenged practice, is often used in cases of refusal to deal.\(^\text{139}\) In addition to intractable difficulties in determining what “efficiency” means and how to evaluate it, another difficulty could appear when blockchain creators are solely engaged in providing a blockchain without operating in any other market. In such a situation, comparing the efficiency of the company asking to access the blockchain with the company refusing to grant access is made impossible. Plus, when the blockchain gatekeeper is more efficient than all of its competitors within a given market, the application of this test would give it a free pass to refuse to grant access to any of its competitors.

Instead, the “no economic sense” test is best suited to the blockchain context. Under this test, a practice may only be sanctioned if it tends to reduce or eliminate competition and provides a benefit to the dominant firm solely because of its tendency to reduce or eliminate competition. This test can also be adapted to study issues that can occur on blockchain.\(^\text{140}\) If a trier of fact suspects that some of the effects created by a practice are pro- or anticompetitive, he must determine whether it is possible to distinguish between all the modifications made to the product, here the blockchain or the smart contract,\(^\text{141}\) and identify the economic justification for each. The application of this test thus makes it possible to evaluate accurately the pro- or anticompetitive nature of exclusion from the blockchain. Therefore, this test is best suited for evaluating refusals to grant blockchain access for anticompetitive motives. Yet, it remains to be seen if courts will apply this test in such cases.

2. **Tying/bundling.** Tying is the practice of subjecting the sale of one product (or service) to additional sales or obligations.\(^\text{142}\) Tying may also entail subjecting a contract to the acceptance of supplementary obligations that have no connection with the original subject of the contract. Blockchain

\(^{139}\) See 2009 O.J. (C45) 2, 85.


\(^{141}\) On how to modify smart contracts, see Raskin, *supra* note 108, at 326–27.

may be used to implement such strategies by subjecting its use to the creation of an account on another platform or to the showing of tokens. This could be seen as anti-competitive.

Tying/bundling is unlikely to be seen on public blockchains. Indeed, this type of blockchain can be freely accessed or used; accordingly, submitting it to the use of another product or blockchain is unlikely. To this extent, and given the difficulty of modifying public blockchains, it is unlikely that such practices would be seen on public blockchains because tying or bundling practices would have to be incorporated into the governance design from the day of the blockchain’s creation. Also, such strategies can lead to a reduction in the potential number of users. Precisely because tied sales and the creation of token effects do not mix well, the modification of the blockchain in order to implement such practices is even more unlikely.

On the other hand, private blockchains may, if created by for-profit companies, have an interest in imposing tying or similar practices. This may be the case, for example, for a company that requires an account on another platform to connect to its blockchain or to get tokens. Returning to the TrustJobs example, X may require an account created on the service it offers outside the blockchain to connect to its application. This may be counterbalanced by the desire to create a network effect, but such balancing is necessarily more limited than it would be on a public blockchain. Tied sales are therefore expected on private blockchains.

3. Predatory innovation. Innovation is “the implementation of a new or significantly improved product (good or service).” Accordingly, when the blockchain governance is modified, it could be seen as an innovative practice. In fact, where there is innovation, there is a risk of predatory innovation: “the alteration of one or more technical elements of a product to limit or eliminate competition.” Predatory innovation appears at first to mirror authentic innovation—it is, after all, a new version of a product or technology—but it is not innovative because it does not bring any real improvements to consumers. In short, predatory innovation encompasses all anticompetitive strategies that, under the guise of being real

---

143 For example, a blockchain application call Omnity asks for an Ethereum Wallet Address. See Omnity Round 2 (OM), AIRDROP ALERT.COM, https://airdropalert.com/omnity-round-2-airdrop [https://perma.cc/RX5S-4SHY].
144 Id.
145 It will still be necessary, however, to demonstrate the anticompetitive effect.
innovations, aim at eliminating competition without benefiting consumers or users.

While the initial choice of the public or private nature of a blockchain should be exempt from antitrust scrutiny,\textsuperscript{148} the type of governance that is chosen implicates the likelihood of anticompetitive practices. What is particularly worrisome is that current legal concepts are blind to the full extent of predatory innovation.\textsuperscript{149}

Predatory innovation is expected on private blockchains, which highlights the need to tackle this practice using an effective regime.\textsuperscript{150} In the words of Ethereum creator Vitalik Buterin, “the consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc.”\textsuperscript{151} This may lead to predatory innovation, which should be more common on private blockchains where a change in the rules is easy and does not require any approval from the users.\textsuperscript{152} Private blockchains can indeed modify their governance design any time, since they do not need to convince users to adopt the change. The TrustJobs example shows how $X$ may modify its blockchain in order to eliminate $Y$ and $Z$.

Predatory innovation might even become a common practice on blockchain for several reasons. First, predatory innovation can be implemented at no cost by simply modifying the blockchain code. Its implementation can also be very fast, as interactions and validations via blockchain usually only take a few seconds or a few minutes at most.


\textsuperscript{149} Two concepts are generally used to analyze what may be considered predatory innovation—tying (see Telex Corp. v. Int’l Bus. Machs. Corp., 367 F. Supp. 258, 347 (N.D. Okla. 1973); United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001)) and leveraging (see C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340 (Fed. Cir. 1998)). See also Richard S. Markovits, \textit{Economics and The Interpretation and Application of U.S. and E.U. Antitrust}, 61 ANTITRUST BULL. 3, 19 (2014); Alan Devlin. & M. Jacobs, \textit{Anticompetitive Innovation and the Quality of Invention}, 27 BERKELEY TECH. L.J. 1 (2012). But their attendant analyses are ineffective in the blockchain context. Tying is inoperative because in the example only one product is involved. Leveraging analysis, which consists of analyzing whether a firm with market power exerts such power on another market, is also unhelpful because it requires two separate markets where a single blockchain only presents one. And leveraging analysis is also ineffective when only one competitor is foreclosed but a wide competitive field remains active.

\textsuperscript{150} See Schrepel, \textit{supra} note 147, at 55.


\textsuperscript{152} In fact, using a “godmode,” the blockchain owner can freeze any account or move the funds away, but chances are that people will eventually discover it and sell all the stocks, securities, or tokens.
Additionally, although transactions and modification are not invisible on public blockchain, they can be on private blockchains. And predatory innovation on blockchain can have a radical effect by allowing for the exclusion of targeted users who are also competitors. Lastly, predatory innovation practices can take different forms with multiple effects beyond mere exclusion from the blockchain. A company that owns a private blockchain can modify its governance design so that a user’s access is simply denied or so that the user can no longer read all the information on the blockchain, register transactions, or take part in the block validation process.

As far as public blockchain are concerned, predatory innovation could be implemented if a new governance design is adopted by a majority of the miners. This, however, seems unlikely. First, any change to public blockchain governance design requires coordination and consensus among all of the stakeholders.\textsuperscript{153} Second, it is impossible to replace the original blockchain.\textsuperscript{154} When the governance design is modified, a “hard fork” is created,\textsuperscript{155} a copy of the ledger is made, and miners switch their hardware to the new governance design. If they do not, the software running under the old rules sees the blocks produced according to the new rules as invalid.\textsuperscript{156} For that reason, as the community on public blockchains grows, it becomes increasingly difficult to reach a consensus on changing governance.\textsuperscript{157} And yet, future introduction of new governance models using off-chain and sidechain mechanisms in public blockchain may reduce these difficulties and therefore facilitate predatory innovation.

\textsuperscript{153}No rule, however, is set in stone. They can all be modified with a broad consensus.
\textsuperscript{154}This subject is still being discussed. The role of a hard fork depends on the governance system. Some blockchains, according to the chosen governance, will allow a modification of governance without the creation of hard forks.
\textsuperscript{156}This creates a situation in which the original blockchain is split into multiple blockchains. To read about the Ethereum “hard fork,” see Kevin D. Werbach, \textit{Trust, but Verify: Why the Blockchain Needs the Law}, 33 BERKELEY TECH. L.J. 487 (2018) [hereinafter Werbach, \textit{Trust, but Verify}] (“Whether or not the Ethereum Foundation made the right call, . . . the controversy raised questions that could not be answered within the framework of the blockchain. They required appeal to some higher-level principles. The viability of trustless trust is ultimately a matter of governance.”).
So, on the one hand, predatory innovation is subjected to legal analyses that are ill-adapted, especially to the blockchain context. On the other hand, predatory innovation remains one of the most anticipated and dangerous anticompetitive strategies that can be implemented on private blockchain. This should raise questions about the need to adapt current legal rules in this regard.

4. Predatory pricing. Attempting to drive a smaller competitor out of the market by systematically undercutting its prices is another anticompetitive practice. On blockchain, pricing occurs mainly in the form of costly transaction fees when a user is submitting a transaction to be registered into the chain. Predatory pricing is very unlikely on public blockchains because it would only be possible if enough users could be convinced to change the governance structure to facilitate such a change.

The situation is quite different for private blockchains. Private blockchains can change the protocol anytime without having to convince anyone to adopt the change. Accordingly, since the protocol can be changed easily, the pricing can also be changed easily in response to competitor pricing. One could imagine, accordingly, that one private blockchain may offer its users very low transaction fees in an attempt to eliminate competing blockchains from the market. The test related to the analysis of predatory pricing, taking into account average variable costs, would then apply.

5. Margin squeeze. Another related practice occurs when a vertically integrated dominant company operates on upstream and downstream markets and sets the upstream price high enough so that companies are unable to sustainably compete in the downstream market. Public

---

158 See Schrepel, supra note 140.

159 In the European Union predatory pricing is considered abusive if the prices charged by the dominant undertaking are below average variable costs or if the prices charged by the dominant undertaking are below average total costs and they are set as part of a plan for eliminating a competitor. See Case C-202/07 P, France Télécom v. Comm’n, 2009 E.C.R. I-2369. In the United States, in order to establish predatory pricing, the plaintiff must show below-cost pricing and a dangerous probability of recoupment by the monopolist once the rival has been driven from the market. See Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 223–24 (1993).

160 See How Do Ethereum Smart Contracts Work?, COIINDESK, https://www.coindesk.com/information/ethereum-smart-contracts-work/ [https://perma.cc/74G6-D73W]; see also DANNEN, supra note 33, at 47.

161 COMM’N OF THE EUROPEAN COMMUNITIES, GUIDANCE ON THE COMMISSION’S ENFORCEMENT PRIORITIES IN APPLYING ARTICLE 82 EC TREATY TO ABUSIVE EXCLUSIONARY CONDUCT BY DOMINANT UNDERTAKINGS 80 (Dec. 3, 2008), http://ec.europa.eu/transparency/regdoc/rep/1/2008/EN/1-2008-832-EN-F1-1.pdf [https://perma.cc/V7EC-C3TF] (asserting that margin squeeze occurs when a dominant undertaking may charge a price for the product on the upstream market which, compared
blockchains, by definition and by way of contrast, are horizontal. It is therefore very unlikely for a margin squeeze to be implemented on public blockchains.

The case is different, however, for private blockchains. Because they allow income-generating applications while maintaining a financial interest on the platform layer, one can imagine that a strategy of margin squeezing could be implemented. Doing so would require that the dominant company—here the blockchain gatekeeper—changes the price it charges in the upstream market (i.e. the blockchain platform). In the development phase of blockchain, such a strategy seems unlikely, but it will have to be closely monitored in the years to come.

6. Exclusive dealing. Another practice is the formation of agreements under which customers are contractually required to purchase particular goods or services exclusively from a dominant company. Such terms could be included in the user agreement which is signed before using the blockchain. It seems unlikely that such exclusive dealing will be imposed on a public blockchain because it would imply integrating such a term from the start. Moreover, once a transaction is registered on a blockchain, users have little interest in registering the transaction on another blockchain because doing so is costly. The technology itself, thus, reduces the incentive to use several blockchains for the same transaction.

The situation is quite different for private blockchains. Foreclosing competitors is an efficient way to increase the overall blockchain price for users and developers. Moreover, private blockchains have an interest in increasing their level of attractiveness by obtaining data that they alone can provide. In the TrustJobs illustration, for instance, $X$ may want to be the


162 For an overview of exclusive dealing, see Case T-155/06, Tomm Sys. ASA & Others v. Comm’n 2010 E.C.R. II-4361, and Case C-413/14 P, Intel Corp. v. Comm’n, 2017 E.C.R. 632. In the United States, exclusive dealing may constitute a violation of Section 2 of the Sherman Act if it forecloses competitors from accessing the market. The D.C. Circuit held that “a monopolist’s use of exclusive contracts, in certain circumstances, may give rise to a § 2 violation even though the contracts foreclose less than the roughly forty percent or fifty percent share usually required in order to establish a § 1 violation.” United States v. Microsoft Corp., 253 F.3d 34, 70 (2001).

163 For an example, see Ethereum Foundation, Legal Agreement, ETHEREUM.ORG, https://www.ethereum.org/agreement [https://perma.cc/57TB-G4NU].
only company listing some type of job offers. To this end, TrustJobs might want to impose exclusive dealing at the entry point of its blockchain. For this reason, it is highly likely that exclusive dealing practices will be implemented on private blockchains.

7. Rebates. Yet another related practice is to grant retroactive rebates or rebates that are conditional on a customer obtaining all or most of its goods or services from the dominant actor. Because all practices are recorded and visible on public blockchains, one user’s discount will be visible to all and granting loyalty rebates or discounts could lead to push-back from users who do not benefit from such a discount. This is more likely to occur if such benefits are perceived as unjustified by other users. Public blockchains therefore push for equal treatment of all users when there is no reason to differentiate among them.

Private blockchains do not necessarily benefit from this “visibility effect” because they can determine what information is visible to each user. They may also have a greater commercial incentive to attract reputable users by offering discounts. In the TrustJobs example, X may want to give a discount on transaction registration fees to some big users. Rebates are, therefore, expected to arise on private blockchains.

ii. Exploitative Abuses

This section is intended to describe how exploitative abuses could be implemented on blockchain. It should be noted that this type of abuse is theoretically not prohibited under U.S. law, which only punishes exclusionary abuses. But some of these exploitative practices are identified and prohibited in practice, especially when they are related to intellectual property and digital markets.

---


166 See Harry First, Exploitative Abuses of Intellectual Property Rights, in THE CAMBRIDGE HANDBOOK OF ANTI-TRUST, INTELLECTUAL PROPERTY, AND HIGH TECH 222, 223, 241 (Roger D. Blair & D. Daniel Sokol eds., 2017) (“It is the standard view in the United States that . . . antitrust law does not reach acts of exploitation by a monopolist . . . [W]ithout denying this substantial divergence in general between the United States and
Exploitative abuse entails directly or indirectly imposing unfair conditions on existing customers or suppliers.\textsuperscript{167} Such abuses could be created by the creation of a dual blockchain environment, one for those who pay the most and one for those who pay less and whose transactions may lag behind as a result.\textsuperscript{168} In the TrustJobs example, \(X\) may impose unfair conditions which users are unwilling to pay to gain visibility on TrustJobs. In fact, the rise of the term “fairness” in the European Commission’s language,\textsuperscript{169} whose definition and scope are still undefined,\textsuperscript{170} could be seen as a sign of European willingness to tackle all exploitative abuse practices more aggressively. In its Impact Assessment entitled \textit{Fairness in Platform-to-Business Relations},\textsuperscript{171} the European Commission identified several issues related to platforms. These include the guidance that “businesses cannot negotiate terms and conditions, the rest of the world, it turns out that there may be fewer differences between the United States and other jurisdictions when it comes to judging exploitative behavior by intellectual property rights holders with market power . . . .[C]ontrary to conventional wisdom, antitrust law is being used today to control the ability of intellectual property rights holders to exploit their licensees through excessively high prices or the imposition of particular nonprice terms.”). For cases, see Microsoft Corp. v. Motorola, Inc., 795 F.3d 1024, 1033 (9th Cir. 2015); Broadcom Corp. v. Qualcomm Inc., 501 F.3d 297, 310, 314 (3d Cir. 2007).

\textsuperscript{167} Article 102(a) of the Treaty on the Functioning of the European Union (TFEU) refers to the imposition of unfair purchase or selling prices as well as other unfair trading conditions. Consolidated Version of the Treaty on the Functioning of the European Union art. 102(a), 2008 O.J. C. 115/47 [hereinafter TFEU]. \textit{See} Case COMP/38.636, Rambus Inc., 2010 O.J. C 30 (the Commission had to deal with potentially abusive royalties for the use of patents).

\textsuperscript{168} This issue is similar to the one of net neutrality. \textit{See} Falk Schöning & Myrto Tagara, \textit{Blockchain: Mind the Gap! Lessons Learnt from The Net Neutrality Debate and Competition Law Related Aspects}, 3 \textit{CONCURRENCES}, at 6 (2018).


which are subject to unilateral and frequently unannounced changes” and that “the overall policy objective is to ensure a fair and innovation-friendly platform economy.” Everything suggests that blockchain issues will be tackled under this general policy.

An exploitative abuse could occur, under this policy, when blockchain creators provide services in exchange for preferential treatment\(^{172}\) or when one blockchain imposes unfavorable measures on another blockchain. However, because blockchain is still evolving rapidly, there is little use for focusing too much attention on exploitative abuses. The dynamism of the blockchain environment will likely correct these abuses themselves—see developments on the “token effect.”\(^{173}\) This type of abuse is nonetheless possible and will undoubtedly be the subject of legal proceedings.

### iii. Discriminatory Abuses

Discriminatory abuses occur when parties apply “dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage.”\(^{174}\) Several kinds of such abuse exist, although price discrimination is the most common.\(^{175}\) According to Judge Richard Posner, “price discrimination is a term that economists use to describe the practice of selling the same product to different customers at different prices even though the cost of sales is the same to each of them. More precisely, it is selling at a price or prices such that the ratio of price to marginal costs is different in different sales.”\(^{176}\) Because price discrimination involves favoring certain customers over


\(^{173}\) See discussion, supra Part I.B.1.

\(^{174}\) See TFEU art. 102(c); see also 2008 O.J. C. 115/47; ROBERT O’DONOGHUE & A. JORGE PADILLA, *THE LAW AND ECONOMICS OF ARTICLE 102 TFEU* 789 (2013).

\(^{175}\) In European judicial history, there are few cases in which price discrimination alone was found abusive. See Case T-301/04, Clearstream Banking AG v. Comm’n, 2009 E.C.R. 317 (referring to anticompetitive foreclosure when an ‘as efficient competitor’ cannot compete effectively with the price of the dominant undertaking); see also C-209/10, Post Danmark A/S v. Konkurrencerådet, 2012 E.C.R. 172, (ECJ clarifying that where prices are below average total costs while being above average incremental costs, a finding of abuse requires a demonstration of actual or likely exclusionary effects). In the United States, price discrimination by a monopolist violates Section 2 of the Sherman Act only to the extent that it is predatory or otherwise excludes competitors from the relevant market. See Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic, 65 F.3d 1406, 1413 (7th Cir. 1995). Price discrimination may also violate the Robinson-Patman Act. See Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 220 (1993).

others, it generally occurs in two ways: (i) charging different customers different prices for the same product, or (ii) charging only some customers the same price for different products.

Could price discrimination occur in the context of blockchain? Certainly. But let’s recall that because of the “visible effect” of public blockchains, occurrences of price discrimination will be limited. However, within private blockchains users may encounter discriminatory terms because the application of different terms to different users is an effective way to urge users to join and use the blockchain. Discriminatory pricing can incentivize some users to stay active on the blockchain by offering lower prices, thus creating a potential discrimination claim for others. Accordingly, discriminatory abuses are more likely to happen on private blockchains. In the TrustJobs example, X may initiate discriminatory terms to thank a user for a commercial advantage granted on another market. Once again, private blockchains will be the center of focus.

II. BLOCKCHAIN AND REGULATORY INFILTRATION

Anticompetitive practices that violate antitrust laws are stopped and sanctioned when they are detected. But what if the identity of the perpetrator is anonymous and therefore protected? Does this mean that all identities should be publicized on blockchain, even if this undercut a core tenet of the technology? Should disclosure rules be imposed? Also, considering the fact that blockchains are immutable, how can anticompetitive practices be remedied on blockchain?

This section examines the effectiveness of antitrust law in the context of blockchain by following questions: is there a “blockchain fortress,” and if so, how does one enter it?177 This section also develops blockchain principles that should be respected when using a “law is code” approach. To this end, this section introduces a voting mechanism that allows regulators to infiltrate blockchains without putting the technology at risk.

177 Please note that the law is not the only method of analyzing this issue. Market operations or social norms, for instance, could be used to do so as well. See De Filippi & Wright, supra note 13. Other distributed ledger technologies state that they “intend to work with governments to provide the same level of protection to distributed public ledgers as is currently present in the financial system.” Leemon Baird, Mance Harmon, & Paul Madsen, Hedera: A Governing Council & Public Hashgraph Network 7 (2018), https://s3.amazonaws.com/hedera-hashgraph/hh-whitepaper-v1.0-180313-2.pdf [https://perma.cc/C3FW-CF44].
A. Is Antitrust Law as We Know It Ineffective?

One of the major antitrust law issues related to blockchain is the detection of anticompetitive practices as well as the identification of those who engage in those practices.

First, algorithms drastically accelerate a company’s ability to engage in anticompetitive practices while limiting the antitrust authorities’ ability to detect and gather evidence of anticompetitive practices. But outside of blockchain, when algorithmic anticompetitive practices are recognized, the perpetrator is generally known as soon as the practice is identified because the perpetrator’s identity is not protected. Things are different within the blockchain ecosystem. As previously explained, blockchain is a technology that ensures the privacy of its users through pseudonymity. These pseudonymous nodes create obstacles to enforcement.

For that reason, tracking services are being developed, but they only work on some blockchains where users engage in millions of transactions. These tracking services are likely to improve, but at the same time, new technologies are being developed to further protect real-life identity. For instance, Monero is using “ring signatures,” a technology that groups cryptographic signatures with at least one real participant, with no way to tell which in the group is the real one as they all appear valid. Zcash is using “zero-knowledge proofs.” Concerns that predict the end of pseudonymity should therefore be kept in perspective.

In fact, there are currently two different paths in the blockchain sphere. One involves working with governments to develop legally compliant blockchains. Here, pseudonymity may indeed soon become a


180 What are zk-SNARKs?, Z CASH (2019), https://z.cash/technology/zksnarks.html [https://perma.cc/3RJU-LMVZ] (“Zero-knowledge proofs allow one party (the prover) to prove to another (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself.”).

The other involves developing a system where everything is encrypted in the blockchain, even the number of transactions. Along this path, “nobody knows you’re a dog,” and pseudonymity would be further entrenched, creating genuine legal issues. There is every reason to believe that technology will move faster than regulators or authorities on this subject, making this a serious enforcement issue.

Second, blockchain constitutes a real barrier to antitrust enforcement because of the distributed nature of its network architecture. No one is in control of public blockchains, but at the same time, everyone is. For that reason, even if a practice is identified as being anticompetitive, it cannot be deleted or stopped.

---


183 One of the notable projects is MimbleWimble. Bitcoin is working to make all amounts encrypted. For an explanation, see TAPSCOTT & TAPSCOTT, supra note 28, at 459 (“The biggest threat to bitcoin is that it becomes so heavily regulated at some point that a competitor that’s more private and more anonymous shows up and everybody switches to that.”) (quoting an interview with Stephen Pair that occurred on June 11, 2015).


185 Michael del Castillo, With Zcash Launch, Blockchain Enters the Age of Anonymity, COINDESK (Oct. 28, 2016), https://www.coindesk.com/zcash-launch-anonymous-blockchain/ [https://perma.cc/A72A-HTLE]; see also Steven Buchko, The Best Fully Anonymous Bitcoin Wallet Options, COINCENTRAL (Nov. 13, 2017), https://coincentral.com/anonymous-bitcoin-wallets/ [https://perma.cc/69VH-6VUW]; Tyler Durden, Is Bitcoin Really Anonymous? IRS Moves To Track Cryptocurrencies With New Chain Analysis Tools, ZERO HEDGE (Aug. 25, 2017), https://www.zerohedge.com/news/2017-08-25/bitcoin-really-anonymous-irs-moves-track-cryptocurrencies-new-chain-analysis-tools [https://perma.cc/8QPC-K6ZD]; DE FILIPPI & WRIGHT, supra note 13, at 39 (“Over time, however, blockchains may become increasingly anonymous, making transaction graph analyses and comparable tracing techniques increasingly difficult. Services already have sprung up to mix and scramble Bitcoin transactions to mask parties’ identities. Recently launched blockchains, such as Zcash and Monero, are hiding the source, destination, and amount of digital currency transferred within these blockchain-based networks by using advanced cryptography such as zero-knowledge proofs and ring signatures.”); Zuckerberg, supra note 95 (explaining that a recourse against blockchain is much harder than it is against tech giants and that blockchain increases privacy and reduces the signal towards illegal conducts to the point of eliminating them).

186 Huberman et al., supra note 55 (“Monopolies are often regulated to prevent or at least mitigate their abuse of power. Bitcoin is not regulated. It cannot be regulated. It need not be regulated because individually the miners are price takers.”).
Blockchain is in principle immutable, meaning that once information is stored on it, it is not possible to erase it.\textsuperscript{187} Also, because blockchain is governed under the \textit{lex cryptographica}, it will continue to function as long as the people who interact with it pay the transaction fees charged by miners who support the blockchain.\textsuperscript{188} For instance, Augur, “a decentralized oracle [and] prediction market platform,” has no central party that can stop its operation.\textsuperscript{189} This platform will continue to work even if governments impose strict regulation or penalties on the original parties who developed or promoted the blockchain.\textsuperscript{190} No “technically skilled people of goodwill”\textsuperscript{191} are needed to maintain the blockchain. Dapps cannot be shut down because there is no server to shut down.\textsuperscript{192} They can only be modified under specific and technical circumstances.\textsuperscript{193} In other words, if an anticompetitive smart contract is implemented on a blockchain with no possible entry to order it to stop, the blockchain will continue to perform the transactions. As a consequence, even if antitrust agencies find a way to identify an anticompetitive practice, there is no directly enforceable remedy.

This possibility has led some authors to ask for “regulatory instruments [that] could be used to prevent certain users from becoming dominant.”\textsuperscript{194} But these proposals in practice require outlawing—or at least condemning—dominant positions, which is inconsistent with principles of antitrust law which only sanctions abuses of dominance. It would amount, in a sense, to going back to a structuralist vision in which

\textsuperscript{187} This principle is debated in the blockchain community. \textit{See} Angela Walch, \textit{The Path of the Blockchain Lexicon (and the Law)}, 36 REV. BANKING & FIN. L. 713, 713 (2017); Werbach, \textit{supra} note 156.

\textsuperscript{188} \textit{See} DE FILIPPI \& WRIGHT, \textit{supra} note 13, at 144.

\textsuperscript{189} ROBERT P. MURPHY \& SILAS BARTA, \textit{UNDERSTANDING BITCOIN: THE LIBERTY LOVER’S GUIDE TO THE MECHANICS AND ECONOMICS OF CRYPTO-CURRENCIES} 78 (2017) (“Remember that no one is “in charge” of Bitcoin. So long as just one copy of the blockchain survives on someone’s hard drive somewhere on Earth, the Bitcoin network can quickly propagate to thousands of other computers once that person gets online.”).

\textsuperscript{190} \textit{See} DE FILIPPI \& WRIGHT, \textit{supra} note 13, at 104.

\textsuperscript{191} ZITTRAIN, \textit{supra} note 4, at 246 (“Our generative technologies need technically skilled people of goodwill to keep them going, and the fledgling generative activities above—blogging, wikis, social networks—need artistically and intellectually skilled people of goodwill to serve as true alternatives to a centralized, industrialized information economy that asks us to identify only as consumers of meaning rather than as makers of it.”).

\textsuperscript{192} \textit{See} RAVAL, \textit{supra} note 21, at 7 (“Data in a dapp is decentralized across all of its nodes. Each node is independent; if one fails, the others are still able to run on the network.”).

\textsuperscript{193} They could be linked to publicly available relevant legal provisions which, when they are modified, will automatically change smart contracts. These contracts could also be written with the option of inserting code later. \textit{See} Raskin, \textit{supra} note 108, at 326.

\textsuperscript{194} Østbye, \textit{supra} note 172, at 30.
dominant positions are punished in themselves.\textsuperscript{195} For that reason, such a proposal should not be adopted. Yet, because the antitrust laws contribute to consumer welfare, there must be a way to stop and prohibit anticompetitive practices committed on the blockchain.

B. Regulatory Infiltration

To date, effective ways to apply antitrust law to blockchain are yet to be found.\textsuperscript{196} Some propose extreme measures such as allowing governments to filter Internet service providers,\textsuperscript{197} criminalize software developers, blacklist decentralized autonomous organizations, or introduce backdoors on individual computers to monitor citizens’ behavior.\textsuperscript{198} In order to avoid such drastic measures that jeopardize blockchain technology and/or individual freedoms, such as the right of access to the Internet,\textsuperscript{199} regulators should encourage blockchains to be designed in compliance with a “law is code” approach.

\textsuperscript{195} This would be disconnected from the current state of economic science. For an explanation of how dominant positions may enhance innovation and benefit the consumer, see Philippe Aghion et al., Competition and Innovation: An Inverted-U Relationship, 120 Q. J. ECON 701 (2005).

\textsuperscript{196} Michèle Finck, Blockchains and Data Protection in the European Union 1 (Max Planck Institute for Innovation and Competition Research Paper No. 18-01, 2018) (“Regulators must . . . nudge blockchain developers to design their products in compliance with this important public policy objective.”).

\textsuperscript{197} Although this would have to be done at a worldwide level, which seems very unlikely to happen anytime soon. Jeff John Roberts, The Law of Blockchain: Beyond Government Control?, FORTUNE (May 11, 2018), http://amp.timeinc.net/fortune/2018/05/10/blockchain-law?__twitter_impression=true [https://perma.cc/NX7S-WSLJ] (“Even though blockchain ledgers like bitcoin are decentralized and run by computers across many countries, state authorities can still target chokepoints in their infrastructure to exert control. In the same way governments have targeted intermediaries like search engines and ISPs to tame unruly aspects of the Internet, they could do the same to put pressure on blockchain networks.”).

\textsuperscript{198} See DE FILIPPI & WRIGHT, supra note 13, at 184.

\textsuperscript{199} See Jay P. Kesan & Rajiv C. Shah, Shaping Code, 18 HARV. J.L. & TECH. 319 (2004) (“In considering regulatory actions, prohibitions can be an effective method of regulation, but current export prohibitions on encryption code are impractical. Similarly, there are regulatory trade-offs involved with technology-forcing regulation.”). But it is not even certain that these measures would be effective because the technology will keep developing. See RAVAL, supra note 21, at 31 (on decentralized bandwidth: “The latest example is the Firechat app for iOS, created by a company called Open Garden. Firechat lets phones speak to each other directly, peer to peer, using the iOS multipeer connectivity feature. No ISP is required. Firechat is an example of a mesh networking application. Mesh networks are the decentralized version of the standard centralized Internet. In a mesh network, users don’t need to go through a central gateway to access a site; they can connect directly to the nearest router, which would be a nearby computer.”).
In fact, the idea that “code is law,” according to which the use of a technology is influenced by the way it is designed, remains useful in understanding blockchain technology and what regulators should seek: influencing the design of technologies. Nonetheless, blockchain characteristics allow the spread of illegal activities, and because of that, “code is law,” which is more of a descriptive than a proactive approach, must be supplemented with a “law is code” regulatory approach, which explains how the regulator should act.

For the first time in history, it appears necessary to code and integrate legal requirements into the technology itself. This is the concept of “law is code.” Without implementing such an approach, technological barriers will deprive the law of any effect. Blockchain creates a technical fortress, and the practices that are carried out inside the blockchain—or via the blockchain—are very well-protected. Fortunately, there is a way for antitrust law to enter the fortress, thereby providing a role for regulators to supplement antitrust laws. The following is a schematic representation of the results expected by the application of a thoughtful “law is code” approach which will lead to “regulatory infiltration.”

Outside the blockchain, when unlawful practices are implemented and detected, antitrust officials can investigate them and find the perpetrator.

---

200 LESSIG, supra note 4, at 121. Lessig states that the “regulator could be a significant threat to a wide range of liberties, and we don’t yet understand how best to control it. This regulator is what I call ‘code’—the instructions embedded in the software or hardware that makes cyberspace what it is. This code is the ‘built environment’ of social life in cyberspace. It is its ‘architecture.’” See also Lawrence Lessig, The Code Is the Law, INDUS. STANDARD (Apr. 9, 1999), http://tech-insider.org/berkman-center/research/1999/0409.html [https://perma.cc/EF4R-7LK8]; Timothy Wu, When Code Isn’t Law, 89 VA. L. REV. 679 (2003).

201 See LESSIG, supra note 4, at 121 (“[I]n real space, we recognize how laws regulate—through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different “code” regulates—how the software and hardware (i.e., the ‘code’ of cyberspace) that make cyberspace what it is also regulate cyberspace as it is.”).

202 See Easterbrook, supra note 15, at 207 (“Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.”). The same caution must be exercised today with the blockchain.

203 Showing how laws affect community, see POSNER, supra note 82, at 214–19.

204 See e.g., Cong & He, supra note 9, at 32. Cong and He call for a “regulatory node in the blockchain” to detect anticompetitive practices. They add that “in the traditional world, in general it helps for regulatory agency to observe and collect more information about the market in order to better detect collusive behaviors.”
As previously discussed, a blockchain is protected by its technological structure. As a consequence, when anticompetitive practices are committed on the chain, antitrust law is ineffective. Here is what then happens when antitrust law attempts to work on blockchain without coding and implementing legal requirements.

As a consequence, only the coding of legal requirements and its implementation into the blockchain design will open the technology when necessary. It permits antitrust laws to enter and sanction anticompetitive practices. Here is what happens when the “law is code” approach is put into action.
C. Regulatory Humility

On the one hand, blockchain poses new challenges to antitrust agencies due largely to the structure of blockchain itself. On the other hand, regulators should not use the novelty of the technology as an excuse—i.e., the “blockchain excuse”—to regulate blockchain activities to the point of hindering innovation. For that reason, this article identified five key principles\(^{205}\) of blockchain technology that should not be challenged by regulators. If they are, the technology will be put at risk. In other words, these principles show where the “law is code” approach must be implemented: outside of the founding principles of blockchain.

1. Humility Towards the Key Characteristics of Blockchain

The law often lags behind technology,\(^{206}\) which generally benefits society since the lag enables the early developers of burgeoning

\(^{205}\) See discussion, supra II, C, 1.

\(^{206}\) For a precise example of the General Data Protection Regulation (GDPR) applied to blockchain, see Michèle Finck, *Blockchains and the GDPR*, OXFORD BUS. LAW BLOG (Feb. 13, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/blockchains-and-gdpr [https://perma.cc/HYV3-5LBF] (underlining that “most current blockchain projects are likely incompatible with the GDPR. This signals that even before the legal framework’s entry into force it already seems outdated in respect of the newest
technologies to build and discover attributes and uses of the technology without legal constraints of any kind.\textsuperscript{207} Then comes the time for regulatory regimes after the development and consolidation of new technologies.\textsuperscript{208} Giving the historical tendency of regulators to urge implementation of antitrust measures in emerging fields in an uninformed manner\textsuperscript{209} with little concern for type I and II errors,\textsuperscript{210} the same order (first technology, then regulation) seems to be desirable for blockchain. Furthermore, when “governments increase their control [over technologies], they replicate their vices,”\textsuperscript{211} an outcome that should be avoided.\textsuperscript{212}

And yet, the paradigm is quite different for blockchain. Without upstream regulation, it will be impossible—for technical reasons—for the law to catch up with the technology. As a result, prophylactic regulation is essential in this space so long as it takes into account that most uses of blockchain are still unknown, and their discovery should not be prevented by legal obstacles. Thus, regulators must proceed but with extreme developments in data management. While this is true in the blockchain context, the GDPR also cannot be easily applied to big data, machine learning and AI.\textsuperscript{207} See also Finck, supra note 198, at 28 (“Whereas the GDPR was fashioned for a world where data is centrally collected, stored, and processed, blockchains decentralize each of these processes,” adding that “blockchains (especially those that are public and unpermissioned) and the GDPR are profoundly incompatible at a conceptual level as the data protection mechanisms developed for centralized data silos cannot be easily reconciled with a decentralized method of data storage and protection.”).

\textsuperscript{207} TAPSCOTT & TAPSCOTT, supra note 28, at 57 (“Let’s be clear: regulation differs from governance. Regulation is about laws designed to control behavior. Governance is about stewardship, collaboration, and incentives to act on common interests. But experience suggests governments should approach regulating technologies cautiously, acting as a collaborative peer to other sectors of society, rather than as the heavy hand of the law.”).

\textsuperscript{208} See id. at 66 (“If the blockchain is as big and universal as the Net, we are likely to do a comparably bad job of predicting both its upsides and downsides.”) (quoting an interview with David Ticoll, December 12, 2015).

\textsuperscript{209} See DE FILIPPI & WRIGHT, supra note 13, at 57 (“regulating too soon could provide valuable guidance as to the legitimate uses of blockchain technology but could also stamp out potential benefits”).

\textsuperscript{210} Type I errors, also called “false positives,” occur when a judge or antitrust authority condemns an undertaking for having implemented one or more practices which, in reality, are not anticompetitive. Conversely, type II errors, or “false negatives,” occur when a judge or antitrust authority decides not to condemn a company which has implemented one or more practices which are in fact anticompetitive.

\textsuperscript{211} GOLDSMITH & WU, supra note 41, at 8. The authors also write that “government is often ugly and pathological.” Id. at 140.

\textsuperscript{212} Angela Walch, The Path of the Blockchain Lexicon (and the Law), 36 REV. BANKING & FIN. L. 713, 763 (2017) (“Taking a slow, inquisitive, and deliberative approach is in tension with the need to quickly get up to speed on the technology to ensure that imminent risks are identified and addressed efficiently.”).
caution. Regulations that are responsive to these concerns can be achieved by respecting five founding principles of blockchains, explained below.

The first principle is pseudonymity. Regulations must recognize this principle as essential to the blockchain, since imposing upstream regulations that mandate disclosure of users’ identities would be contrary to the very essence of blockchain technology and will actually eliminate an alternative model to most of the technologies in use today where users’ real-life identity is known and monetized by companies. Of course, pseudonymity does not come without its challenges; however, the concept remains core to blockchain’s existence. The second principle is the distributed architecture of blockchain. This core principle of blockchain creates distributed power, meaning that no central point of failure exists and the harm from one person’s reckless behavior is contained solely to that person. The third principle is peer-to-peer transmission between users. The existence of a transmission system, which is vital to the use of blockchain, must not be challenged by regulations. Doing so would amount to reintroducing middle-market companies into the blockchain ecosystem, artificially and unnecessarily making blockchain less attractive. The fourth principle is blockchain consensus. Creators must remain free to choose the consensus mechanism they wish to use. Therefore, blockchain users should be free to

213 For an overview of regulatory humility, see Friedrich A. Hayek, The Use of Knowledge in Society, 35 AM. ECON. REV. 519 (1945); see also Thibault Schrepel, Friedrich Hayek’s Contribution to Antitrust Law and Its Modern Application, GLOBAL ANTITRUST REV. 199 (2014).

214 For an explanation of these principles, see discussion, supra Part II.C.1.


216 See Malte Möser & Rainer Böhme, The Price of Anonymity: Empirical Evidence from a Market for Bitcoin Anonymization, 3 J. CYBERSECURITY 127 (2017). In fact, pseudonymity amongst blockchain’s users may lead societies to reveal themselves by moving in the direction consumers and citizens truly desire outside of legal boundaries.

217 See VIGNA & CASEY, supra note 21, at 224 (asking “can we afford not to tackle identity?”).

218 See Jeff Brito, We Must Protect Our Ability to Transact Privately Online, COIN CENTER (Feb. 6, 2019), https://coincenter.org/entry/we-must-protect-our-ability-to-transact-privately-online [https://perma.cc/L9KN-K375] (arguing for pseudonymity in crypto-currencies).

219 Mauri, supra note 32.

220 TAPSCOTT & TAPSCOTT, supra note 28, at 77.
participate in the block validation process they deem best without becoming liable for assenting to an anticompetitive practice the blockchain may be involved with at another time. The fifth and final principle is data immutability. Enabling an entity to delete data or stop transactions on blockchain would undermine the trust that is a core feature of this technology.

Regulations that challenge one of these five principles could cause blockchain to lose its utility. The way blockchain will evolve is uncertain, and choices made by blockchain communities will fundamentally affect what values are built into it as well as the outcome users and society can gain from it. For this reason, it is tempting for regulators to get involved in how blockchain will turn out. But the question is “whether we’re capable of making those choices,” knowing that “law tends to arrive at basic answers before the right questions have been asked.” The issues are too fundamental not to let blockchain transformations emerge on their own thanks to its millions of users. Regulatory humility in light of these bedrock blockchain principles will ensure that the blockchain continues to develop to its full potential.

2. What Remains Possible: Law is Code in Practice

Allowing blockchain technology to emerge does not mean that nothing should be done about the illegal practices implemented on it.

First, it should be stressed that in some situations, the identities of users engaged in anticompetitive practices will be reported to antitrust authorities, despite the pseudonymity principle of blockchain. Such a situation arises when the real-life identity of that user is known to other blockchain users. Accordingly, one might imagine a situation in which a company that is part of the production chain where an anti-competitive practice took place, or even an end-consumer, introduces an antitrust complaint. Thus, blockchain and pseudonymity do not protect blockchain users against all types of detection and identification. In fact, the anticompetitive effects caused by one practice on the market may also lead

---

221 It has been argued that without evolution, some blockchain could disappear. See, e.g., Campbell R. Harvey, *Bitcoin Myths and Facts*, 9 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479670 [https://perma.cc/CXD8-BHX9] (“It is likely that bitcoin will have to adapt and make changes if it is to survive. It is unlikely that the model proposed in 2008 is the best model.”).

222 LESSIG, supra note 4, at 311 (answering “my argument is that we’re not.”).

223 BORK, supra note 12, at 16.
an antitrust authority to launch an investigation. Here, a “law is code” approach is not necessary.

However, the real-life identity of users or blockchain creators is not always known, and in such situations, only a “law is code” approach will enable courts and regulators to enter the blockchain. Two challenges then arise: (i) one related to the applicability of legal requirements, (ii) the other one to the necessity not to frustrate blockchain technology’s key characteristics while making the law effective.

Regarding the first challenge related to the applicability of legal requirements, imposing fair regulatory mechanisms to blockchain communities through the implementation of code will only be successful if developers and users are incentivized to comply with the law. Indeed, the regulators’ usual ability to impose legal requirements is not effective on blockchain because its creators and users are covered by their pseudonymity and, therefore, not forced to comply with the law. As a consequence, because the law within blockchain cannot be imposed in the same way as it is imposed outside of blockchain, new mechanisms must be devised so that users agree to comply with it. This may involve the creation of legal incentives (the regulator may indeed promise legal advantages to blockchains who agree to integrate the proposed code) as well as economic incentives (for instance, tax advantages in exchange for code integration). In other words, the law must not be conceived as a threat or it will fail to be complied with. The law, within the blockchain environment, must be designed as an ally to blockchains. Developers and users must agree to facilitate legal enforcement by integrating the code proposed by the regulator.

Concerning the second challenge—making the law effective—new mechanisms must be developed in order to identify users and/or developers as well as making sanctions effective while keeping in mind the vital characteristics of the technology which must not be challenged. To this respect, regulators could first encourage the implementation of mechanisms allowing a qualified majority of blockchain users to vote in order to reveal the identity of another user. Such mechanisms could work in private blockchains where the user’s real-life identity is verified prior to granting access to the platform. This would be consistent with the idea of decentralization behind blockchain by preserving the will of the majority. As far as public blockchains are concerned, different types of governance could be promoted by establishing “safe harbors” for specific

224 Although detecting the actual effects of an anticompetitive practice, as opposed to the discovery of the practice, is not easy.
225 On the distinction between law as a "threat" or an "umpire", see BRONWEN MORGAN & KAREN YEUNG, AN INTRODUCTION TO LAW AND REGULATION 6 (2007).
configurations in the blockchain code to make it harder to use the blockchain for illegal purposes. Self-regulation and co-regulation should also be considered as serious alternatives.\(^{226}\) Second, regarding the effectiveness of sanctions and remedies,\(^{227}\) a real challenge is created by the absence of choke points on blockchain.\(^{228}\) And indeed, the structure of blockchain technology makes it difficult to seek injunctive relief because it is nearly impossible to enjoin a decentralized and autonomous organization. The only viable option seems to embed regulatory measures into the blockchain’s governance. Just as the mechanism by which users would vote to reveal the identity of an individual involved in anticompetitive practices on a private blockchain, a mechanism could be developed in which blockchain users vote on the creation of forks, determined by courts or antitrust agencies, in order to delete or stop transactions. Blockchain communities agreeing to introduce such mechanisms would be treated by regulators and courts as being more in line with the law than blockchains refusing to do so. Stricter measures challenging one of the five principles could be imposed on the latter, which could be a powerful tool at the disposal of public authorities.

In short, a delicate balance between the “law is code” approach and the need to protect key characteristics of blockchain must be found. The voting mechanism proposed above strikes this balance. The introduction of such voting mechanisms would be binding when used to determine whether an individual’s identity should be disclosed, whether to put an end to certain transactions, whether a ban on “layer 2” applications should be instituted, or whether there should be interference with a key aspect of a blockchain’s function. One may also consider the possibility that public authorities could mandate the presence of voting into blockchains without the need to ask for any permission, or even going further, to force the creation of hard forks. Time will show which mechanisms will be appropriate in specific situations.

In any case, the “law is code” approach seems inevitable given that antitrust law, if maintained as it operates today, will quickly become ineffective for technical reasons. The need to control anticompetitive

\(^{226}\) See Martijn Scheltema, **Balancing Public and Private Regulation**, 12 UTRECHT L. REV. 16 (2016); see also LINDA SENDEN ET AL., **MAPPING SELF- AND CO-REGULATION APPROACHES IN THE EU CONTEXT**, 10 (Utrecht Univ. 2015).

\(^{227}\) See DE FILIPPI & WRIGHT, *supra* note 13, at 44 (“Blockchains thus enable the creation of autonomous software programs run through the collaborative effort of parties with different incentives and in different locations scattered across the globe, none of which can unilaterally affect the code’s execution. Once deployed on a blockchain, these programs no longer need or necessarily heed their creators; they are run on a decentralized network, making it difficult to unwind or halt their execution.”).

\(^{228}\) A choke point is a point of congestion or blockage.
practices will lead to compelling policy debates. These debates will generate solutions, and as Lawrence Lessig observed, “we are at a stage in our history when we urgently need to make fundamental choices about values, but we should trust no institution of government to make such choices.” If a government regulates blockchain too strictly, innovation will be harmed as developers move away from the space to other more lucrative or less regulated fields. For instance, several New York startups decided to leave the state when they were required to register with the New York State Department of Financial Services and obtain a BitLicense. If developers cannot vote with their computers, they will vote with their feet by relocating their businesses, and if they cannot vote with their feet, blockchain technology will be at risk. Only regulatory humility will help blockchain to reach its full potential, while preventing anti-competitive practices.

III. GOING BEYOND: THE BLOCKCHAIN ANTITRUST PARADOX

Satoshi Nakamoto’s paper introducing Bitcoin was published just ten years ago, and Ethereum was created in 2015. In all likelihood, the 2010s will be remembered as the beginning of blockchain and distributed ledger technologies in the same way the 1990s are remembered for the beginning of the Internet. Blockchain has even been described as the “return of the Internet.” However, previous generations of technology were primarily concerned with the exchange of information while blockchain is all about the exchange of value.

It is difficult to predict how blockchain will evolve, as there are potentially infinite applications. Blockchain’s evolution will also depend

---

229 LESSIG, supra note 4, at 8 (referring to institutions, “[T]he government we now have is a failure. Nothing important should be trusted to its control, even though everything important is.”).
230 WERBACH, supra note 39, at 175.
232 See M. ETHAN KATSH, LAW IN A DIGITAL WORLD 243 (1995) (writing on the beginnings of the internet: “as we encounter cyberspace, we become linked to a light, a sun, that unleashes powerful energies for new and creative visions.”).
233 TAPSCOTT & TAPSCOTT, supra note 28, at 43.
234 WORLD ECON. FORUM, Blockchain Beyond the Hype: A Practical Framework for Business Leaders 4 (Apr. 2018) (White Paper) (“previous generations of technology were predominantly about the faster and more secure exchange of information; that is, they were aimed at delivering the same objectives faster . . . . Blockchain, meanwhile, is about the exchange of value; it is intended to enable individuals to exchange currency and other assets with one another without relying on a third party to manage the transactions.”).
235 See TAPSCOTT & TAPSCOTT, supra note 28, at 226–249 (listing streaming music, art galleries, free press, education). Blockchain may help dispute resolution. See Jeremy
on the development of its infrastructure layer, which is currently incomplete. As of today, there are two dominant blockchain platforms: Bitcoin and Ethereum. There are also a number of smaller networks under development, several of them are probably destined to become major players. In fact, alternatives to blockchain which allow decentralization through algorithms are already in development, notably Tangle and Hashgraph.

Because the future evolution of blockchain is unknown, it is difficult to evaluate the scope of the practices that will develop along with it. This article has identified several unilateral anticompetitive practices. They are most likely to occur on private blockchains. However, most of the usual mechanisms of antitrust law will be ineffective in the face of blockchain. Even with the “regulatory infiltration” proposed using a “law is code” approach, some of the instruments which are used today, such as emergency measures or commitments, will be ineffective in their current form. In the face of blockchain, current antitrust law may well be eliminated. In fact, three factor corroborate this hypothesis.

First, antitrust law will probably become ineffective without regulatory infiltration. For the first time in its history, antitrust law will have to be greatly supplemented by regulations taking the form of a “law is code” approach. Indeed, antitrust law will not have complete answers to three issues: how to detect the anticompetitive practices committed on the blockchain, how to identify the actor responsible for these practices, and finally, how to remedy them for the future. While the author of an


See WORLD ECON. FORUM, supra note 235 (“Given the relatively early stages of this technology, anchoring on blockchain without consideration of associated risks, including, among others, cost, security and the relevant industry’s regulatory environment, can be detrimental.”); see also DANNEN, supra note 33, at 14 (“[T]he Ethereum network is not yet complete. It is operational today, but will not be complete until sometime in 2019.”).

Timothy May, The Crypto Anarchist Manifesto, ACTIVISM (Nov. 22, 1992), https://www.activism.net/cypherpunk/crypto-anarchy.html [https://perma.cc/8MUC-AHLW] (“Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions.”).

KATSH, supra note 233, at 240 (“Law is not only a process that touches all other societal institutions, but it is, as I have stressed, an institution that is fundamentally oriented around information and communication.”).
anticompetitive blockchain can sometimes be identified, the effectiveness of sanctions and remedies may be crippled by blockchain’s immutability. Presciently, the home page of the Ethereum Project reads: “Build unstoppable applications.”

Thus, even where antitrust law finds a way to regulate blockchains, it may die because it is no longer a creator of welfare on its own. Think of it as the unfortunate death of jazz: the music still exists and has listeners, but jazz no longer creates debate or leads to any movement that ventures beyond its own framework.

Second, public blockchains will limit monopolization even when new governance mechanisms are implemented. In particular, predatory pricing and refusal to deal appear to be exceedingly unrealistic, while tying, margin squeezing, exclusionary dealing, loyalty rebates, and exploitative and discriminatory abuses are unlikely to occur. Furthermore, because the transactions implemented on public blockchains are visible to all, the incentive to engage in anticompetitive practices is reduced since market surveillance and industry monitoring can easily root out illegal activity. However, some perpetrators will be protected by the “opacity effect” created by the characteristics of the technology. This is particularly true for private blockchains where entering it, absent regulation infiltration, is technically impossible. In short, anticompetitive practices are expected to be rare on public blockchains, but these practices could be plentiful on private blockchains that operate below authorities’ radar. The same issues arise outside the scope of unilateral practices, namely, for collusive agreements where the identification of colluders and the unsuitability of existing mechanisms to stop and punish such practices is equally problematic.

The third and final reason to expect the death of antitrust law is tied to its foundations. Without a doubt, regulators will find ways to submit blockchains to the law, whether it is by way of regulatory infiltration—which is recommended—or other ways that place the technology at risk, such as the regulation of end users, transportation layers, information intermediaries, blockchain intermediaries, transaction processors or code, architecture or hardware manufacturers—which is not recommended. But even if antitrust law remains as a body of positive law, the regulator may end up protecting the existence of antitrust law even though its initial goals are no longer fulfilled. After all, modern

241 See Schrepel, supra note 57.
242 De Filippi & Wright, supra note 13, at 175–83.
243 Black’s Law Dictionary (5th ed., 1979) (defining positive law as “law actually and specifically enacted or adopted by proper authority for the government of an organized jural society”).
antitrust law is built on the premise that the Sherman Act is concerned with trusts. Without trusts, are antitrust laws needed? This is the “blockchain antitrust paradox”: antitrust laws’ potential lack of legitimacy (and efficacy) on the one hand and the need to stop anti-competitive practices on the other.

Furthermore, the death of antitrust law might not be solely linked to blockchain technicalities. The fate of antitrust law might also be determined by the inherent conflict between the logic of blockchain technology and the logic of antitrust law. Recall that there is no trustee in the sense of a third-party fiduciary within the framework of blockchain. In other words, the target of antitrust laws is absent. Blockchain challenges the raison d’être of antitrust law.

Conversely, antitrust law was created for, and is applied by, centralized regulatory agencies, such as the FTC, the DOJ, and the European Commission. Enforcing antitrust law amounts to imposing vertically designed rules and concepts on a technology built around the desire for decentralization. But blockchain is used not only for “philosophical” reasons related to its decentralized nature but also because it is practical, and in fact, blockchain’s practicability results from its decentralization. In short, this opposition between the vertical nature of antitrust law and the horizontal or decentralized nature of blockchain raises a legitimacy concern. The cultural and sociological factors that led to the development of blockchain technology cannot be ignored by the law.

As a consequence, on top of all the challenges related to blockchain technicalities, another concern is the legitimacy of antitrust law with respect to this technology. To address this concern, a way must be found to decentralize antitrust law and antitrust authorities. This will

---

245 See SWAN, supra note 3, at 69 (observing that “blockchain is a technology for decentralization.”). In fact, “blockchain technology could help achieve what some commentators are calling the promise of “Internet 3.0,” a re-architecting of the Net to assert the core objective of decentralization that inspired many of the early online pioneers who built the Internet 1.0.” VIGNA & CASEY, supra note 21, at 17; see also Sinclair Davidson et al., Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995 [https://perma.cc/W4D2-L4AZ] (describing DLT as “new institutional technology of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments.”).
246 WERBACH, supra note 39, at 76.
247 See Raskin, supra note 108, at 308.
248 Cf. MILTON FREEDMAN, CAPITALISM AND FREEDOM 50 (1962) (arguing for
require *a minima* to design\(^2\) and implement new governance models using blockchain.\(^3\) Antitrust authorities can no longer rely on pyramidal structures nor continue to operate in a closed circle on the model of nation-state-led government. Antitrust law as we know it must die and be reborn. If not, it soon will be illegitimate.

249 On how to design competition agencies, see Frédéric Jenny, *The Institutional Design of Competition Authorities: Debates and Trends* (2016). See also OECD, Roundtable on Changes in Institutional Design, DAF/COMP/M(2015)1/ANN6/FINAL; Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 420 (2016) (“Peer-to-peer law is likely to emerge slowly and in unpredictable ways, but it has the potential to create authoritative decisions without authoritative decision-makers. There may be decisive arguments against particular peer-to-peer institutions, but legal theorists should at least allow peer-to-peer institutions to join the menu of possible regulatory arrangements.”). Decentralized antitrust authorities could use futarchy, quadratic voting, liquid democracy or holacracy mechanisms.

250 See Abramowicz, *supra* note 249, at 420 (“Peer-to-peer law is likely to emerge slowly and in unpredictable ways, but it has the potential to create authoritative decisions without authoritative decision-makers. There may be decisive arguments against particular peer-to-peer institutions, but legal theorists should at least allow peer-to-peer institutions to join the menu of possible regulatory arrangements.”).
“DEEPFAKES": THE NEWEST WAY TO COMMIT ONE OF THE OLDEST CRIMES

Russell Spivak*

CITE AS: 3 GEO. L. TECH. REV. 339 (2019)

INTRODUCTION

Last year, a widely read technology blog turned heads with the deeply disturbing headline: “We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now.” While deliberately provocative, it was—and remains—unfortunately true. An unnamed individual on the popular discussion board, Reddit, superimposed images of celebrities such as Gal Gadot (Wonder Woman), Masie Williams (Game of Thrones), and Daisy Ridley (Star Wars) onto the bodies of adult video stars in pornographic films. That Reddit poster’s handle, or moniker, was “deepfake.” Hence, the term deepfake now refer to a video that superimposes hyper-realistic faces onto the bodies of others with the intent of creating a new video with fake representations.

The initial Reddit post containing the altered video led to the proliferation of computer-generated pornographic videos starring anyone and everyone. As The Atlantic correctly sums up, “[i]n a dank corner of

---

* J.D., Harvard Law School, 2017; B.S., Massachusetts Institute of Technology, 2013. All errors are my own. My deepest gratitude goes out to the editors of the Georgetown Law Technology Review, without whom this article would not be possible.


2 Id.

3 Note that deepfakes are not synonymous with simple face-swapping. As well, throughout this article, to distinguish between the anonymous individual versus the technology, the former will be indicated with an “@” to denote its status as a username handle.
the internet, it is possible to find actresses from *Game of Thrones* or *Harry Potter* engaged in all manner of sex acts.\(^4\)

Importantly, this image-based technology—which is simply an intelligent algorithm, explained in more depth *infra*—can perform similar mimicry for auditory sounds. In other words, it can match one’s vocal tone and pattern with user-generated scripts, à la lip-synching.

The purpose of this article is not to debate the morality of this technology and whether it ought to be legal to purchase or download; this article, instead, leaves these decisions to ethicists and, ultimately, policymakers.\(^5\) The article also does not attempt to address national security or political questions that this technology raises.\(^6\) Rather, this article endeavors to discuss the remedies available to private victims of this technology. Put plainly, how can Daisy Ridley et al. pursue legal recourse against their digital manipulators?

To do so, this article begins in Section I with an in-depth explanation of generative adversarial networks, the technology that enables deepfakes. Section II outlines whether lawmakers looking to


\(^6\) *See, e.g.*, Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?*, LAWFARE BLOG (Feb. 21, 2018, 10:00 AM), https://www.lawfareblog.com/deep-fakes-loomng-crisis-national-security-democracy-and-privacy [https://perma.cc/53AF-ZVVK] (Chesney and Citron offer the following examples: “[f]ake videos could feature public officials taking bribes, uttering racial epithets, or engaging in adultery”; “[p]oliticians and other government officials could appear in locations where they were not, saying or doing horrific things that they did not”; “[f]ake videos could place them in meetings with spies or criminals, launching public outrage, criminal investigations, or both”; “[s]oldiers could be shown murdering innocent civilians in a war zone, precipitating waves of violence and even strategic harms to a war effort”; “[a] deep fake might falsely depict a white police officer shooting an unarmed black man while shouting racial epithets”; “[a] fake audio clip might ‘reveal’ criminal behavior by a candidate on the eve of an election”; “[a] fake video might portray an Israeli official doing or saying something so inflammatory as to cause riots in neighboring countries, potentially disrupting diplomatic ties or even motivating a wave of violence”; “[f]alse audio might convincingly depict U.S. officials privately ‘admitting’ a plan to commit this or that outrage overseas, exquisitely timed to disrupt an important diplomatic initiative”; “[a] fake video might depict emergency officials ‘announcing’ an impending missile strike on Los Angeles or an emergent pandemic in New York, provoking panic and worse.”).
regulate this emerging technological field can do so under the First Amendment. Concluding no such regulation is constitutionally permissible, the article then turns to other available remedies notwithstanding any potential legislative solutions. Section III addresses the viability of potential state law causes of action, including defamation, privacy torts, and right of publicity that victims can pursue to redress their violated rights. Section IV looks to federal law and asks whether the Communications Decency Act, namely 47 U.S.C. § 230, would protect website hosts where deepfakes are housed. Section V then reviews the applicability of copyright law to the question of deepfakes. Finally, the article concludes with some final thoughts about deepfakes and how the United States should act quickly to develop and adopt stronger prevention mechanisms.

I. DEEPFAKES FOR DUMMIES

A. The Science

“[T]he earliest known surviving photograph made in a camera, was taken by Joseph Nicéphore Niépce in 1826 or 1827,” but 150 years passed before people began digitally editing photographs. Photoshop was developed in 1987 by Thomas and John Knoll. ""Thomas Knoll, a doctoral candidate in computer vision, was trying to write . . . computer code to display grayscale images on a black-white bitmap monitor."" After rewriting the code for color mapping and image formats, as well as creating Adobe’s hallmark feature Layers, Photoshop was born. Within a few years, the neologism “photoshopping” entered common vocabulary. By 2006, the verb “photoshop” was entered into the Oxford English Dictionary.

9 Id.
10 See id.
11 Dictionaries list its origin as the 1990’s. See Photoshop, ENGLISH OXFORD LIVING DICTIONARIES, https://en.oxforddictionaries.com/definition/photoshop [https://perma.cc/G9SZ-6YG].
Photoshop’s ubiquity has given way to “a general belief that manipulated photos are prevalent,” “mak[ing] people . . . generally skeptical about the veracity of photos . . . .” These “[c]onvincing Photoshop-esque techniques for video have arrived” in the form of deepfakes. A working knowledge of how deepfakes are made will help inform our ability to address its improper uses.

Deepfakes are created using discriminative algorithms and generative algorithms. “Discriminative algorithms try to classify input data; that is, given the features of a data instance, they predict a label or category to which that data belongs.”

For example, given all the words in an email, a discriminative algorithm could predict whether the message is spam or not-spam. [S]pam is one of the labels, and the bag of words gathered from the email are the features that constitute the input data. When this problem is expressed mathematically, the label is called y and the features are called x. The formulation $p(y|x)$ is used to mean “the probability of y given x”, which in this case would translate to “the probability that an email is spam given the words it contains.”

So discriminative algorithms map features to labels.16

16 Id; see also Andrew Ng, Lecture at Stanford University: Generative Learning Algorithms, http://cs229.stanford.edu/notes/cs229-notes2.pdf [https://perma.cc/CVD9-2XPZ] (“Consider a classification problem in which we want to learn to distinguish between elephants (y = 1) and dogs (y = 0), based on some features of an animal. Given a training set, [a discriminative algorithm] tries to find a straight line—that is, a decision boundary—that separates the elephants and dogs. Then, to classify a new animal as either an elephant or a dog, it checks on which side of the decision boundary it falls, and makes its prediction accordingly.”).
Unlike discriminative algorithms, generative algorithms do not just aim to classify the correct label; rather, a generative model provides a way to generate data that looks like it came from the dataset. Instead of predicting a label given certain features, it attempts to predict features given a certain label.\textsuperscript{17} Harkening back to the spam/not-spam example: “The question a generative algorithm tries to answer is: Assuming this email is spam, how likely are these features? . . . They allow you to capture . . . the probability of \( x \) given \( y \), or the probability of features given a class.”\textsuperscript{18} Said plainly, generative algorithms assume a classification and establish the particular features of the classification.

Generative Adversarial Networks, or GANs, pit these two types of algorithms against one another. GANs were introduced by Ian Goodfellow and other researchers at the University of Montreal.\textsuperscript{19} Goodfellow et al. describe it in the following way: GANs are a “framework for estimating generative models via an adversarial process, in which we simultaneously train two models: a generative model \( G \) that generates artificial samples, and a discriminative model \( D \) that estimates the probability that a sample came from the training data rather than \( G \).”\textsuperscript{20} In lay terms, researchers create two separate computer models: “One neural network, called the generator, generates new data instances, while the other, the discriminator, evaluates them for authenticity; i.e. the discriminator decides whether each instance of data it reviews belongs to the actual training dataset or not.”\textsuperscript{21} This is also the case with deepfake videos.

The generator is creating new images that it passes to the discriminator. It does so in the hopes that they, too, will be deemed authentic, even though they are fake. The goal of the generator is to generate passable hand-written digits, to lie without being caught. The goal of the discriminator is to identify images coming from the generator as fake.\textsuperscript{22}

\textsuperscript{17} A Beginner’s Guide to Generative Adversarial Networks (GANs), supra note 15.
\textsuperscript{18} Id.; see also Ng, supra note 16.
\textsuperscript{20} Id.
\textsuperscript{21} Id.
\textsuperscript{22} Id.
“After enough of this ‘training,’” the algorithm is refined enough to “convincingly manipulat[e] video on the fly,” meaning it will generate images into each individual video frame such that when played regularly, the video appears seamless. This process produces a deepfake.

A literary comparison may be instructive. Some of the most famous authors often have their own styles, be it Ernest Hemingway’s concise sentences, James Joyce’s stream of consciousness, David Foster Wallace’s “winding sentences and novelistic footnotes,” or Emily Dickinson’s non-traditional meter and punctuation. Even famous jurists are known for their distinct writing styles—e.g. Justice Scalia’s exceptional metaphors or Justice Kagan’s pragmatism. Well-versed readers may only need a few sentences—if not less—to determine the author.

Now imagine ‘training’ the discriminator to learn a particular author’s style so well that it can pinpoint the author’s style among numerous texts. The discriminator is then handed a new page of prose produced by the fraudster, or generator. He or she must then determine whether or not the new sample is written by the original author. Or

---


24 See, e.g., ERNEST HEMINGWAY, A FAREWELL TO ARMS 274 (Hemingway Library ed. 1929) (“She’s just having a bad time. The initial labor is usually protracted. She’s only having a bad time. Afterward we’d say what a bad time and Catherine would say it wasn’t really so bad. But what if she should die? She can’t die. Yes, but what if she should die? She can’t, I tell you. Don’t be a fool. It’s just a bad time.”).


consider an art forger trying to establish the legitimacy of a fake Vincent Van Gogh or Georges Seurat. The two, like many renowned painters, had particular styles and visions. If the counterfeiter hopes to make a passable replica, using the wrong color palette or the improper technique is a dead giveaway. A discerning eye could tell the difference.

Deepfakes simply apply this process from text or art to videos. With deepfakes, the generator constructs new video frames, while the discriminator tries to discern whether the frame, with its superimposed subject, is authentic (say, an actual video frame of the original actor) or fake (a doctored video frame of the actor in a compromising position). If the discriminator cannot tell the real images from the false images, a human may not be able to either.

B. Proliferation: Pornography and Otherwise

After Reddit user @deepfakes posted his creation, other users, called “Redditors,” caught on quickly. Within a month of Motherboard’s initial reporting of these altered pornographic videos, over 15,000 Redditors subscribed to @deepfakes’s dedicated discussion board, posting videos of their own. This rapid proliferation of deepfake videos was possible because the technology needed to create them was already widely available to the public. Additionally, another Redditor, wanting to break down barriers to entry for this technology even further, “created an app specifically designed to allow users without a computer science background to create AI-assisted fake porn. All the tools one needs to make these videos are free, readily available, and accompanied with instructions that walk novices through the process.”

The app—appropriately titled “FakeApp”—opened the door to even more deepfake creators.

Indeed, Gadot, Williams, and Ridley are not the only female celebrities that have had their likeness grafted onto adult films: Jessica Alba, Natalie Dormer, Scarlett Johansson, Chloe Bennet, Taylor

---

30 Cole, We Are Truly Fucked, supra note 1.

31 Id.


33 Cole, We Are Truly Fucked, supra note 1.

Swift, Sophie Turner, Katy Perry, Cara Delevingne, and Aubrey Plaza have become victims of this technology as well. In one example, “a deepfake of Emma Watson taking a shower was reuploaded by CelebJihad—a celebrity porn site that regularly posts hacked celebrity nudes—as a ‘never-before-seen video . . . from my private collection, [which] appears to feature Emma Watson fully nude and flaunting her naked sex organs while showering with another girl.”

Once Reddit itself got wind of this development, it shut down the discussion board where this was posted and banned similar content. Reddit additionally updated its site-wide rules regarding its ban on “involuntary pornography” and “sexual or suggestive content involving minors.” The ban on involuntary pornography includes revenge porn, the spreading of private nudes, and any sexualized image “apparently created or posted without [the subject’s] permission, including depictions that have been faked.” Reddit was not the only website to ban this type of content. For example, Pornhub, one of the Internet’s largest databases of online adult videos, established similar bans.

Deepfakers have also focused on generating celebrity videos outside the adult film industry. In a slightly more good-natured use of the technology, the deepfake community turned to one particular movie star for comedic relief—Nicolas Cage. Cage’s face was superimposed onto

---

35 Cole, AI-Assisted Fake Porn Is Here, supra note 23.
36 Cole, We Are Truly Fucked, supra note 1.
37 Cole, AI-Assisted Fake Porn Is Here, supra note 23.
39 Id.
40 Id.
41 Cole, AI-Assisted Fake Porn Is Here, supra note 23.
42 Cole, We Are Truly Fucked, supra note 1.
44 Id.
45 Id.
46 Warzel, supra note 38. In practice, it appears that Pornhub’s ban has been largely ineffective: “[w]hile banned material frequently slips through the cracks on large sites that allow users to upload content, the deepfake violations on Pornhub are especially flagrant.” Id.
Harrison Ford’s Indiana Jones in *Raiders of the Lost Ark* and onto Amy Adams’ Lois Lane in *Man of Steel.* In one particularly humorous and meta deepfake, Cage’s face was superimposed onto Andy Samberg’s face in a *Saturday Night Live* sketch in which Samberg was impersonating Cage. 

Unsurprisingly, deepfakes have already made their way into the political arena. Admittedly, the groundwork was there; disinformation campaigns have been effectively deployed as political weapons for decades. In a recent iteration of this disgraceful tactic, U.S. Ambassador to Russia Michael McFaul was targeted by a Russian disinformation campaign. McFaul recalled the episode in the *Washington Post:* “State propagandists and their surrogates crudely photoshopped me into pictures, spliced my speeches to make me say things I never uttered and even accused me of pedophilia.”


Deepfakes with specific face-swaps of U.S. elected leaders in compromising position have not yet been produced. They have, however, been deployed mockingly. For example, two random Internet posters turned President Trump into the main character from the television show *The Office*.\(^{52}\) Additionally, a quick Google search reveals President Trump’s likeness superimposed onto German Chancellor Angela Merkel,\(^{53}\) onto *Back to the Future* villain Biff Tannen,\(^{54}\) and onto *Austin Powers* villain Dr. Evil.\(^{55}\)

Deepfakes are also used to superimpose an average member of the public onto a celebrity’s body. As one blogger wrote, “we can leverage these celebrities for other things, such as inserting your friends and family into blockbuster movies and shows!”\(^{56}\) That blogger then turned his wife’s likeness—on the body of Anne Hathaway—into an interviewee opposite David Letterman and a film star opposite Steve Carrell.\(^{57}\) In his words:

I personally think it’s fun, can be innocent, and even makes for a nice surprise/gift. . . . [N]ow you can put your best friend into his favourite movie: have her dance with Patrick Swayze and have the time of her life, or have an alien burst out of his stomach.\(^{58}\)

---

52 Coburn, *supra* note 32.
57 Id.
58 Id.
C. The Current Status and Imminent Growth of Deepfakes: Better Technology, Better Source Material, and an Incentivized Private Sector

In some cases, current deepfakes are very “believable,” yet “[d]eepfake technology remains brittle and prone to failure in many scenarios,” according to Tim Hwang, the Director of the Ethics and Governance of AI Initiative at the Harvard Berkman-Klein Center and the MIT Media Lab. The computing power required to generate a believable fake remains a barrier for casual computer users. Thus, a deepfake video often comes out as “a blurry, semi-believable version” of the targeted victim. Nevertheless, as technology improves, these limiting factors will slowly fall by the wayside.

For example, computing power limitations are already dissipating. “According to [@]deepfakes—who declined to give his identity . . . to avoid public scrutiny—the software is based on multiple open-source libraries.” Moreover, “a decent, consumer-grade graphics card could process this effect in hours, but a CPU would work just as well, only more slowly, over days.” Thus, Dr. Hwang’s technological limitations may soon expire. As average graphics cards and CPUs continue to improve in performance, the time needed to turn individuals into un-

60 Jeremy Hsu, Experts Bet on First Deepfakes Political Scandal, IEEE SPECTRUM (June 22, 2018, 6:00 PM), https://spectrum.ieee.org/tech-talk/robotics/artificial-intelligence/experts-bet-on-first-deepfakes-political-scandal [https://perma.cc/W9AY-W3YY].
61 Id.
63 Cole, We Are Truly Fucked, supra note 1.
64 A computer processor unit, the main microchip powering a computer.
65 Id.
consenting subjects of videos, adult or otherwise, will shrink exponentially.

Another potential limiting factor is sufficient source material, but the digital era in which we live has rendered this factor a non-issue. With only one image of the victim, for example, a person—much less an artificially intelligent algorithm—cannot learn much about him or her. But the more one can augment the dataset, the more realistic the fake will be. For celebrities, a simple Google search provides enough source material. But for the general public, a Google search may be insufficient—for now. As more and more pictures populate the Internet, laypersons are no longer immune to the potentially harmful effects of deepfakes.

Aside from better technology and better source material, an additional propellant in the proliferation of deepfakes is the private sector. As told by Dr. Neil DeGrasse Tyson, one of the foremost advocates for scientific exploration—in truth, deepfakes are simply discoveries and explorations in computer science—“[t]he history of exploration has never been driven by exploration. But Columbus himself was a discoverer. So was Magellan. But the people who wrote checks were not. They had other motivations.”67 For example, in defending his work, @deepfakes pointed out “that he is using an algorithm similar to one developed by Nvidia,”68 a software capable of turning “snowy roads into summer, and day into night” instantaneously.69 That the private sector fuels the flame should come as no shock. Indeed, John Knoll, the aforementioned co-creator of Photoshop later worked at Industrial Light and Magic, the visual effects department of Lucasfilm.70

The private sector likely continues to see utility in these sorts of technological advances due to their commercial applications—imagine, for instance, paying to correct the fumbling of a best man’s toast or a commencement address. Given this success, companies will likely continue to devote substantial resources to advancing and finding new uses for them. How such advances may be misused is yet to be seen. Tellingly, when Mashable reached out to Nvidia after @deepfakes marshaled support for his work by citing the company’s work, “[t]he Nvidia researchers who developed the algorithm declined to comment on this possible application.”71

67 JAMES EGAN, 1000 HISTORIC QUOTES 144 (2015).
68 Cole, We Are Truly Fucked, supra note 1.
69 Id.
70 See Schewe, supra note 8.
71 Cole, We Are Truly Fucked, supra note 1.
D. Related, Truth-Defying Technologies

At least three other technological developments run parallel to deepfakes, arguably as destabilizing, albeit less popular: manipulating video with voice-overs, face-to-face capture and reenactment, and audio-to-video conversion.

1. Audio/Visual Manipulation

Audio/Visual manipulation is the ability to “manipulate and digitally alter the footage of [one speaker] to a script written and performed by [another].”72 Thus far, this technology has only made its appearance in popular culture once: comedian-filmmaker Jordan Peele produced a video with Buzzfeed CEO Jonah Peretti of Peele’s voice (impersonating Obama’s) onto a video of President Obama. The frightening part about it, however, is that President “Obama’s lips move in sync with Peele’s voice.”73 Though the distinct audio modification is enough to alert any casual observer, a more pitch-perfect match could fool even a keen ear.74

2. Face-to-Face Capture and Reenactment

Face-to-face capture and reenactment technologies internalize every movement of a speaker’s face. Then, the software recreates a digital face with the same movements. The researchers’ “goal is to animate the facial expressions of the target video by a source actor and re-render the manipulated output video in a photo-realistic fashion.”75 Not only can the technology capture—and replicate in a video—the speaker’s motions, it

74 Id.
can even capture “real-time facial expressions, including distinct movements such as eyebrow raises.” In practice, “[a]n actor speaks to the webcam and his facial expressions and speech are copied by George Bush, Vladimir Putin, Donald Trump, and Barack Obama.”

3. Audio-to-Video Conversion

The final technological development is the ability to “take audio of someone talking and turn that into a realistic video of someone speaking those words.”

University of Washington researchers have developed new algorithms that solve a thorny challenge in the field of computer vision: turning audio clips into a realistic, lip-synced video of the person speaking those words . . . . In a visual form of lip-syncing, the system converts audio files of an individual’s speech into realistic mouth shapes, which are then grafted onto and blended with the head of that person from another existing video.

These videos are not stilted or robot-like: these fakes include swaying, pacing, facial cues, and other distinctly human ticks. As one researcher stated, “We’re learning how to capture human personas.” One could take snippets of speeches and splice them together in a hyper-realistic way to create a video that has the look and feel of the speaker’s mannerisms.

---

77 Mark Burgess, *Make Putin Pout With This Creepy Face-Tracking Tech*, WIRED (Mar. 21, 2016), http://www.wired.co.uk/article/face2face-face-recognition-copy-putin-bush-trump [https://perma.cc/68JC-D4HH].
E. Prevention Mechanisms

Due to the realistic nature of the films, scientists are researching new methods to identify when an image has been faked. After the Lawfare blog published multiple essays promoting a grim and foreboding view of deepfakes, Dr. Herb Lin, a senior research scholar for cyber policy and security at the Center for International Security and Cooperation, and Hank J. Holland, Fellow in Cyber Policy and Security at the Hoover Institution, offered a “ray of hope”:

Consider the technology of digital signatures, which enable a party to sign a digital object in such a way that proves he or she was the one who signed it. Now imagine that a vendor produces cameras and sound recorders (i.e., devices) that digitally sign every video or audio file the user creates. Further, the vendor keeps records so that the purchaser of any given device is known in the future—that is, the device and its public signature key is registered in a database accessible to anyone. Any video or audio file released in the future, accompanied by a digital signature, could then be associated with a specific purchaser.

This scheme does not produce 100-percent confidence . . . . But this scheme would certainly provide more confidence in the authenticity of the video or audio than for a video that was not accompanied by a signature that could be traced to a registered device.81

The private sector is already deploying the first generation of this technology. For example, Canon’s Original Data Security Kit “enhances security by providing image data encryption and decryption features in addition to a verification function that authenticates image originality.”82 Nikon also offers a similar software package.83 Yet, it is worth noting that both such technologies have been hacked and, thus, “rendered useless.”84

Digital-watermarks are not the only possible solution. There are multiple large-scale projects in academia, industry, and government aimed at ferreting out manipulated and falsified images grounded in genuine ones. A Columbia University project, for example, is taking pedestrian reverse image search technology “to the next level, and starting to find parts of images that have been repurposed from other images.” Thus, if even part of an image is identical to another publicly available image, the technology can flag it as a potentially manipulated image. This technology may well be expanded to videos.

Additionally, digital color analysis may provide a possible solution. Dr. Hany Farid, a computer science professor at Dartmouth College, said:

Almost every image is stored in a JPEG file, which throws away some information to save on storage. There is a huge amount of variation in how each camera does that. If a JPEG is unpacked—opened in Photoshop—and then put back together, it is always repackaged slightly differently, and we can detect that.

---


86 See, e.g., Frequently Asked Questions, TINEYE, https://www.tineye.com/faq#what [https://perma.cc/VBN2-4ANT] (“TinEye is a reverse image search engine. You can submit an image to TinEye to find out where it came from, how it is being used, if modified versions of the image exist, or to find higher resolution versions. TinEye uses image recognition technology rather than keywords, metadata or watermarks.”).


88 Id.
Farid notes that that technology has an equivalent for videos “based on the observation that computer-generated content lacks the imperfections that are present in a recorded video. It’s created in almost too perfect a world. So one of the things we look at is, are we not seeing the statistical and geometric patterns we’d expect to see in the physical world?”

A final technological breakthrough is based on humans’ natural blood flow. An algorithm perceives “periodic pulsatile motion within a narrow temporal passband centered around the heart rate” in tissue. In lay terms, it can calculate one’s pulse by measuring the frequency of subtle color changes to tissue. This technology allows us to measure a person’s pulse in a video of him or her speaking into a camera. It can, therefore, flag computer-altered or computer-generated videos because a computer-generated video of humans would not exhibit these subtle changes.

F. In Defense of Technological Exploration

Despite the potential invidious uses of this technology, there are many possible benefits and important uses for this technology as well. For example:

Dr. [Louis-Philippe] Morency [the director of Carnegie Mellon University’s MultiComp Lab] said soldiers suffering from post-traumatic stress disorder could eventually video-conference with doctors using similar technology. An individual could face-swap with a generic model without sacrificing the ability to convey his or her

89 Id.
91 The Defense Advanced Research Projects Agency (DARPA) has also dedicated resources to the Medical Forensics, or MediFor, Project, which aims to “automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity of visual media to facilitate decisions regarding the use of any questionable image or video.” Dr. Matt Turek, Media Forensics, (MediFor), DEF. ADV. RES. PROJECTS AGENCY, https://www.darpa.mil/program/media-forensics [https://perma.cc/2CQT-GH5C].
emotions. In theory, this would encourage people to get treatment who might otherwise be deterred by a perceived stigma, and the quality of their treatment wouldn’t suffer due to a doctor being unable to read their facial cues.

Another one of Dr. Morency’s possibilities—and its own can of worms—would be to use models in video interviews to remove gender or racial bias when hiring.92

Additionally, deepfakes are created using advanced machine learning technologies, which have a wide array of applications, from driverless cars to facial recognition software. Derailing research that improves deepfake technology, thus, may inadvertently impact these other industries as well. Further, research into deepfake technology may have unexpected positive impacts. It is often the case that “great achievement has no road map. The X-Ray [and] penicillin[,] neither were discovered with a practical objective in mind. [W]hen the electron was discovered in 1897, it was useless. And now we have an entire world run by electronics.”93

Deepfakes have quickly permeated multiple facets of society, from parody to pornography, using this fascinating new technology. What’s more, deepfakes are on the rise: in part due to the private sector’s economic incentive, in part from academia’s push for exploration, and in concert with other interesting yet precarious technologies. With this deeper understanding of deepfakes—their history, proliferation, and related technologies—we can begin to apply it to the law.

II. DEEPFAKES AND THE FIRST AMENDMENT

Before questioning how victims of deepfakes can seek legal redress, a threshold question must be addressed: does the First Amendment protect deepfakes and deepfakers? More directly, can the government regulate, if not altogether ban, the production and dissemination of deepfakes?94 To address this question, we begin with first principles.

93 The West Wing: Dead Irish Writers (NBC television broadcast Mar. 6, 2002).
94 As stated previously, lawmakers are indeed considering legislative action. See Breland, supra note 5.
A. First Amendment, First Principles

The First Amendment provides that: “Congress shall make no law . . . abridging the freedom of speech.” Under that Clause, a government, including a municipal government vested with state authority, ‘has no power to restrict expression because of its message, its ideas, its subject matter, or its content.’ For that reason, “content-based restrictions on speech [are] presumed invalid[, and] the Government bear[s] the burden of showing their constitutionality.” In lay terms, this rule means that no matter how abhorrent one may find a message—from promoting Nazism to segregation—and no matter the size of the group that agrees with a position, disagreement with the message alone is insufficient to merit inhibiting the speaker’s permission to enter the “marketplace of ideas” without a compelling government interest.

Per the Supreme Court’s 2015 holding in Reed v. Town of Gilbert, Arizona, “[g]overnment regulation of speech is content-based if a law applies to particular speech because of the topic discussed or the idea or message expressed,” thereby distinguishing between the speaker and the message. While previous constitutional doctrine may have deployed case-specific rules depending on the subject matter of said speech, “[t]he majority opinion in Reed effectively abolishes any distinction between content regulation and subject-matter regulation.”

“If a law is unconstitutional [because] its restrictions ‘depend entirely on the communicative content’ of what is regulated, then any restriction of revenge pornography is in deep trouble.” This reasoning applies with equal force to deepfakes. Therefore, despite both federal and state officials’ recent interest in enacting legislation to curb

---

95 U.S. CONST. amend. I.
99 135 S. Ct. at 2227.
100 Norton v. City of Springfield, 806 F.3d 411, 412 (7th Cir. 2015).
102 See Breland, supra note 5.
103 See, e.g., Katyanna Quach, New York State is Trying to Ban 'Deepfakes' and Hollywood isn’t Happy, REGISTER (June 12, 2018, 10:22 PM), https://www.theregister.co.uk/2018/06/12/new_york_state_is_trying_to_ban_deepfakes_and_hollywood_isnt_happy [https://perma.cc/MP57-YLPJ].
deepfakes, any law banning, or even regulating, deepfakes would be presumptively invalid, given that such a law would fall squarely into content-based or message-based regulation.

Thankfully, that’s not the end of the story. Despite its sweeping language, “it is well understood that the right of free speech is not absolute at all times and under all circumstances.” As the Supreme Court has affirmed:

There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or ‘fighting’ words—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace.

And the government has indeed availed itself of this semi-permeable bar. To pass constitutional muster, deepfake regulations must fall into one of these exceptional categories; whether it in fact does so, however, is dubious at best.

B. Exceptions

Certain obscenities, including child pornography, are exempt from First Amendment’s protections. And indeed, deepfakes may be, and likely are, used to create obscene and child-pornographic videos. Thus, these issues are examined with regard to this new technology. Ultimately, a regulation or an outright ban on deepfakes is unlikely to fit neatly within the obscenity or child pornography exceptions set out in our nation’s First Amendment jurisprudential framework because not all uses of deepfakes

---

104 Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942); see also Whitney v. California, 274 U.S. 357, 371 (1927) (“That the freedom of speech which is secured by the Constitution does not confer an absolute right . . . is not open to question.”).
105 Chaplinsky, 315 U.S. at 571–72 (footnotes omitted).
107 See Chaplinsky, 315 U.S. at 571–72
are obscene. Therefore, such a law is unlikely to withstand judicial scrutiny.

1. Obscenity

That “obscenity is not within the area of constitutionally protected speech or press” is beyond contestation. The Supreme Court first recognized this in 1942.

It has been well observed that [lewd and obscene] utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.

The Court re-affirmed this notion in the following decade, explaining that the history of regulating obscene speech further supported the rejection of First Amendment protections for obscenities.

Implicit in the history of the First Amendment is the rejection of obscenity as utterly without redeeming social importance. This rejection for that reason is mirrored in the universal judgment that obscenity should be restrained, reflected in the international agreement of over 50 nations, in the obscenity laws of all of the 48 States, and in the 20 obscenity laws enacted by the Congress from 1842 to 1956.

The more complex question is what constitutes obscenity. This question remains particularly germane with respect to deepfakes. Justice Potter Stewart famously—or infamously—failed to delineate a bright line rule as to what constitutes obscenity: “I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it.” Yet, for lower courts and the rule of law, the Supreme Court later pronounced a three-pronged inquiry

110 Chaplinsky, 315 U.S. at 571–72.
111 Roth, 354 U.S. at 484–85.
in *Miller v. California*\(^{113}\) to determine when speech crosses from cringe-inducing, yet protected, speech into unprotected obscenities.

The basic guidelines for the trier of fact must be: (a) whether ‘the average person, applying contemporary community standards’ would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.\(^{114}\)

To this point, “[t]he *Miller* standard . . . was an accommodation between the State’s interests in protecting the ‘sensibilities of unwilling recipients’ from exposure to pornographic material and the dangers of censorship inherent in unabashedly content-based laws.”\(^{115}\) Given this multi-pronged standard, whether deepfakes, or computer-generated pornography, are obscene is not easily answered.

That being said, what constitutes obscenity is a decision left up to each individual state to decide for itself.\(^{116}\) For example, the District of Columbia has determined that under the District’s statute barring obscenity, materials depicting or live performances of oral sex are per se obscene, meaning “the Government need not proffer any evidence of national community standards.”\(^{117}\) Similarly, the Court of Appeals of South Carolina has determined “[n]ude dancing per se is not illegal.”\(^{118}\)

---

\(^{113}\) Justice Stewart’s *Jacobellis* concurrence was far from the only time the Justices were unable to determine a standard. “Apart from the initial formulation in *Roth*, no majority of the Court has at any given time been able to agree on a standard to determine what constitutes obscene, pornographic material subject to regulation under the States’ police power.” *Miller*, 413 U.S. at 22 (citing *Redrup v. New York*, 386 U.S. 767, 770–71 (1967)).

\(^{114}\) *Id.* at 24.

\(^{115}\) New York v. Ferber, 458 U.S. 747, 756 (1982); cf. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 874 (1997) (“In evaluating the free speech rights of adults, we have made it perfectly clear that ‘[s]exual expression which is indecent but not obscene is protected by the First Amendment.’”).

\(^{116}\) *Miller*, 413 U.S. at 32–33 (“It is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City. . . . People in different States vary in their tastes and attitudes, and this diversity is not to be strangled by the absolutism of imposed uniformity.”).


Because deepfakes are simply images dynamically superimposed onto preexisting videos, whether they are obscene depends solely on whether the underlying video is deemed obscene. As applied, deepfakes’ obscenity is therefore coterminous with the obscenity of the underlying video. For example, if a state were to ban a particular type of pornographic video (e.g., a video depicting rape) as obscene, this ban would extend to deepfakes superimposing one’s face onto an unedited video that violated this provision. However, if the state did not ban the original pornographic video, its deepfake counterpart would similarly be permitted. Therefore, deepfakes are not on their face obscene speech. As such they require some protection, meaning any legislation regulating deepfakes would not pass muster under this obscenity exception.

2. Child Pornography

“The Supreme Court has repeatedly recognized that children are different than adults, and that . . . justice systems must reflect that.” This difference is reflected in the treatment of child pornography. Despite the protections afforded to pornography, the Supreme Court has held that “States are entitled to greater leeway in the regulation of pornographic depictions of children.” In arriving at this conclusion, the Supreme Court in New York v. Ferber considered four

---

119 See infra notes 130–133 and accompanying text (explaining that, under Supreme Court precedent, a video that purported to depict child pornography was not per se obscene because the actual underlying video was of consenting adults modified via computer-generated images).

120 B.R. v. McGivern, 714 F. App’x 528, 538 (6th Cir. 2017) (Stranch, J., concurring) (citing Miller v. Alabama, 567 U.S. 460, 471, 473, 477–78 (2012)) (affirming that children are “constitutionally different” from adults and that the “characteristics” and “incompetencies” of youth, including their lack of sophistication in dealing with the criminal justice system, must be taken into account); see also J. D. B. v. North Carolina, 564 U.S. 261, 264–65 (2011) (holding that “a child’s age properly informs the Miranda custody analysis” because it is “beyond dispute that children will often feel bound to submit to police questioning when an adult in the same circumstances would feel free to leave”); Graham v. Florida, 560 U.S. 48, 68 (2010) (acknowledging “fundamental differences” between adults and youth); Roper v. Simmons, 543 U.S. 551, 569–70 (2005) (consulting scientific studies, among other sources, in recognizing that developmental and environmental differences, such as immaturity and lesser control over their environments, can result in young people being “more vulnerable or susceptible to negative influence”).

121 Miller, 567 U.S. at 480–81.

independent substantive reasons\(^\text{123}\) why child pornography is not protected by the First Amendment: (1) “a State’s interest in ‘safeguarding the physical and psychological well-being of a minor’ is ‘compelling’”\(^\text{124}\); (2) “[t]he distribution of photographs and films depicting sexual activity by juveniles is intrinsically related to the sexual abuse of children”\(^\text{125}\); (3) “[t]he advertising and selling of child pornography provide an economic motive for and are thus an integral part of the production of such materials, an activity illegal throughout the Nation”\(^\text{126}\); and (4) “[t]he value of permitting live performances and photographic reproductions of children engaged in lewd sexual conduct is exceedingly modest, if not *de minimis*.”\(^\text{127}\)

Thus, while adult pornography—save for truly obscene images therein—may not be obscene, the same images of children are deemed obscene. It would be reasonable to assume, therefore, that deepfakes involving children are necessarily not subject to the First Amendment’s strong shield, but the inquiry does not end there.

In 2001, the Supreme Court heard oral argument for *Ashcroft v. Free Speech Coalition*.\(^\text{128}\) The case concerned the expansion of the Child Pornography Prevention Act of 1996 to include not only pornographic images made using actual children but also “‘any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture,’ that ‘is, or appears to be, of a minor engaging in sexually explicit conduct.’”\(^\text{129}\)

The Court held, however, that banning virtual child pornography, or pornography depicting children created entirely through computer-generated graphics, went too far:

Where the images are themselves the product of child sexual abuse, *Ferber* recognized that the State had an interest in stamping it out without regard to any judgment

\(^{123}\) The Court’s fifth and final justification was that this determination was “incompatible with [its] earlier decisions.” *Ferber*, 458 U.S. at 763.


\(^{125}\) *Ferber*, 458 U.S. at 759.

\(^{126}\) *Id.* at 761.

\(^{127}\) *Id.* at 762.


\(^{129}\) *Id.* at 241.
about its content. The production of the work, not its content, was the target of the statute. . . .

*Ferber* upheld a prohibition on the distribution and sale of child pornography, as well as its production, because these acts were “intrinsically related” to the sexual abuse of children in two ways. First, as a permanent record of a child’s abuse, the continued circulation itself would harm the child who had participated. . . . Second, because the traffic in child pornography was an economic motive for its production, the State had an interest in closing the distribution network. . . . Under either rationale, the speech had what the Court in effect held was a proximate link to the crime from which it came. . . .

In contrast to the speech in *Ferber*, speech that itself is the record of sexual abuse, the CPPA prohibits speech that records no crime and creates no victims by its production. Virtual child pornography is not ‘intrinsically related’ to the sexual abuse of children, as were the materials in *Ferber*. While the Government asserts that the images can lead to actual instances of child abuse, the causal link is contingent and indirect. The harm does not necessarily follow from the speech, but depends upon some unquantified potential for subsequent criminal acts.\(^{130}\)

Deepfakes fall into this second *Ashcroft* category. Even if deepfakes were to involve children, they are not necessarily created with the sexual abuse and exploitation of children. As explained *infra*, an intelligent algorithm merely needs perfectly appropriate and normal pictures of minors—e.g. a child playing at the beach—to twist them into a child pornographic deepfake. Thus, as abhorrent as we may consider superimposed underage children in illicit videos, the First Amendment likely protects these deepfakes, notwithstanding the child exploitation exception.\(^{131}\)

\(^{130}\) *Id.* at 249–50.

\(^{131}\) It is worth noting that Justice Thomas concurred in the judgment but was taken by the government’s “prosecution rationale—that persons who possess and disseminate pornographic images of real children may escape conviction by claiming that the images are computer generated, thereby raising a reasonable doubt as to their guilt.” *Id.* at 259.
Due to deepfakes’ inputs and outputs, they are unlikely candidates to fall within the First Amendment’s obscenity or child pornography exceptions. Thus, laws barring or even regulating their creation are unlikely to survive First Amendment litigation. Victims must therefore utilize other means of protection—namely, deterrence via civil litigation.

III. STATE REMEDIES: DEFAMATION, PRIVACY TORTS, AND THE RIGHT OF PUBLICITY

In light of the potential havoc deepfakes and related technologies can wreak, scholars and legislators alike ought to consider how to structure relevant legal regimes. The constitutionality of proactive legislation is dubious (discussed supra). Thus, the focus on rectifying harms to victims should explore other methods to obtaining just ends.

Currently, scholarly literature is limited in its exploration of this subject. Discussions of deepfakes reside almost exclusively in newspapers, magazines, and online articles, many of which are cited throughout this article. In such periodicals, one conclusion is clear, although it lacks expounding analysis: the obvious remedy is state tort law. Indeed, Rebecca Crootof, executive director of the Information Society Project and a research scholar and lecturer in law at Yale Law School, “suggested that tort law may be the better mechanism for dealing

Government cannot prove that certain pornographic images are of real children. In the event this occurs, the Government should not be foreclosed from enacting a regulation of virtual child pornography that contains an appropriate affirmative defense or some other narrowly drawn restriction.

Id. It may well be the case that Justice Thomas—and potentially his robed brethren—consider deepfakes and the algorithmic technology powering them to have arrived at this point. However, Thomas noted that “the Government asserts only that defendants raise such defenses, not that they have done so successfully. In fact, the Government points to no case in which a defendant has been acquitted based on a ‘computer-generated images’ defense.” Id. Therefore, while deepfakes may bring us closer to Thomas’ perceived inflection point, there remains no such case in which deepfake technology served as the foundation of a successful defense. Until such a case occurs, Thomas and others are unlikely to view this as persuasive justification to overturn Ashcroft.  

At the time of this article’s publication, only one substantive law review-type paper has substantively evaluated deepfakes, though it approaches the subject far differently than this one. See Robert Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 CALIF. L. REV. (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 [https://perma.cc/2YLZ-LXVZ].
with Deepfakes technology on a ‘tailored, case-by-case basis’ in courtrooms.\textsuperscript{133}

This section surveys multiple state tort causes of action. Because common law tort actions are filed pursuant to state law, such actions must take into account two nuances of common law doctrines. First, different standards apply in each jurisdiction. While these causes of action are similar across all fifty states, they are not identical. However, for simplicity, this article uses a commonly accepted standard for the causes of action as captured in texts and treatises.

Second, in nearly all jurisdictions, liability standards are victim-dependent. When victims are private citizens, they are afforded an increased measure of protection.\textsuperscript{134} On the other hand, courts employ a heightened standard—“actual malice”—in privacy tort actions when brought by public officials and public figures.\textsuperscript{135}

\textsuperscript{133} Hsu, supra note 60.


\textsuperscript{135} What constitutes a public official or public figure is not clearly defined. In the Supreme Court’s own words:

In some instances an individual may achieve such pervasive fame or notoriety that he becomes a public figure for all purposes and in all contexts. More commonly, an individual voluntarily injects himself or is drawn into a particular public controversy and thereby becomes a public figure for a limited range of issues. In either case such persons assume special prominence in the resolution of public questions.

Gertz v. Robert Welch, Inc., 418 U.S. 323, 351 (1974). The designation has also been further bifurcated and delineated:

Extending the \textit{Sullivan} line of cases, the United States Supreme Court has identified two types of public figures for purposes of defamation: all purpose public figures, such as politicians, who are widely recognized, and limited purpose public figures, who may not be well known on every issue but who are sufficiently involved in a particular area to be considered as public figures for that purpose.

Use of the actual malice standard emanates from the Supreme Court’s “landmark” opinion in *New York Times Co. v. Sullivan*.\(^{136}\) In *Sullivan*, the *New York Times* published a full-page advertisement titled “Heed Their Rising Voices.”\(^{138}\) In the Supreme Court’s own words, “[i]t is uncontroverted that some of the statements contained in the [advertisement] were not accurate descriptions of events which occurred in Montgomery.”\(^{139}\) As a result, Sullivan, the subject of the inaccurate statement, filed a libel claim against both Alabama signatories to the ad\(^{140}\) and the *Times* itself.\(^{141}\)

Quoting Justice Brandeis’ famed concurrence\(^{142}\) in *Whitney v. California*,\(^{143}\) the Court held: “Believing in the power of reason as applied through public discussion, [the Founding Fathers] eschewed silence coerced by law—the argument of force in its worst form. Recognizing the

\(^{136}\) E.g., Obsidian Fin. Group, LLC v. Cox, 740 F.3d 1284, 1289 (9th Cir. 2014); Railey v. Webb, 540 F.3d 393, 404 n.4 (6th Cir. 2008); Moore v. Vislosky, 240 F. App’x 457, 464 (3rd Cir. 2007); Wells v. Liddy, 186 F.3d 505, 520 (4th Cir. 1999); Jefferson Cty. Sch. Dist. No. R-1 v. Moody’s Inv’r.’s Servs., Inc., 175 F.3d 848, 852 (10th Cir. 1999); Woods v. Evansville Press Co., Inc., 791 F.2d 800, 803 (7th Cir. 1986); Walker v. Pulitzer Pub. Co., 394 F.2d 505, 520 (4th Cir. 1968).

\(^{137}\) 376 U.S. 254 (1964).

\(^{138}\) *Id.* at 256. The advertisement, which was paid for and “signed at the bottom of the page by the ‘Committee to Defend Martin Luther King and the Struggle for Freedom in the South,’” *id.* at 257, purported to solicit funds to defend Dr. King against two charges of perjury, for which he was indicted in Alabama. *Id.* at 257, 259–60. In addition to this solicitation, the advertisement discussed other important incidents related to the Montgomery, Alabama Police department: arrests of Dr. King “for ‘speeding,’ ‘loitering’ and similar ‘offenses,’” *id.* at 258, as well as allegations that the police department attempted to “starve [protestors] into submission,” *id.* at 257. L.B. Sullivan, on the other hand, was one of the three elected Commissioners of the City of Montgomery, Alabama and was in charge of supervising, among other things, the Police and Fire Departments. *See id.* at 256. Moreover, Sullivan was not involved in Dr. King’s arrests, he was not elected when Dr. King’s home had been bombed, and his police department had not been subsequently implicated in the attack, despite allegations to the contrary in the advert. *Id.* at 259.

\(^{139}\) *Id.* at 258.

\(^{140}\) The signatories included celebrities such as Harry Belafonte, Marlon Brando, Nat King Cole, Sammy Davis Jr., Mahalia Jackson, Langston Hughes, Sidney Poitier, and Jackie Robinson as well as civil rights leaders and politicians like Rev. Ralph Abernathy, John Lewis, and Eleanor Roosevelt. *See Heed Their Rising Voices, N.Y. Times* (Mar. 29, 1960), [https://perma.cc/43MA-URSV].

\(^{141}\) *Sullivan*, 376 U.S. at 256.


\(^{143}\) 274 U.S. 357, 372–80 (1927).
occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.\textsuperscript{144} Therefore,

all officials are protected unless actual malice can be proved. The reason for the official privilege is said to be that the threat of damage suits would otherwise “inhibit the fearless, vigorous, and effective administration of policies of government” and “dampen the ardor of all but the most resolute, or the most irresponsible, in the unflinching discharge of their duties.”\textsuperscript{145}

The Supreme Court has since applied its “actual malice” standard to other torts involving public figures\textsuperscript{146} beyond defamation, including the intentional infliction of emotional distress,\textsuperscript{147} and state courts have also extended this standard to causes of action alleging a false light invasion of privacy.\textsuperscript{148}

All deepfakes, by definition, rise to the level of actual malice, should that standard apply.\textsuperscript{149} Per the Supreme Court’s \textit{New York Times Co. v. Sullivan} ruling, “actual malice” equates to “knowledge that it was false or with reckless disregard of whether it was false or not.”\textsuperscript{150}

Reckless disregard, it is true, cannot be fully encompassed in one definition . . . . [R]eckless conduct is not measured by whether a reasonably prudent man would have published, or would have investigated before publishing. There must be sufficient evidence to permit the conclusion

\begin{footnotes}
\item[145] \textit{Id.} at 282 (quoting \textit{Barr v. Matteo}, 360 U.S. 564, 571 (1959)).
\item[149] \textit{See, e.g.}, \textit{Ashby v. Hustler Mag., Inc.}, 802 F.2d 856, 860 (6th Cir. 1986).
\end{footnotes}
that the defendant in fact entertained serious doubts as to the truth of his publication. Publishing with such doubts shows reckless disregard for truth or falsity and demonstrates actual malice.151

Because deepfakers create a given deepfake video by combining two distinct sources into one, its creator must know the final result is fraudulent, thereby satisfying the standard.

A. Defamation

“In today’s world, one’s good name can too easily be harmed through publication of false and defaming statements on the Internet.”152 Deepfakes are an archetypal example of that.

Defamation is one means of civil recourse for pursuing deepfakers. “A defamatory statement is defined as a communication that tends to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.”153 “In American law, defamation is not about compensating for damage done to a false reputation by the publication of hidden facts. Instead, it protects a good reputation honestly earned.”154 Victims of deepfakes may be entitled to recovery under a defamation action. For example, an individual who spends a lifetime cultivating a given reputation only to have it obliterated by a fraudulent video depicting false actions, which he or she appears to partake in, when those actions run contrary to said reputation, likely has a cause of action that satisfies the standard for defamation.

“Defamation is the generic term for the twin torts of libel and slander.”155 But the line of demarcation between the two is neither clear nor settled. The Restatement reads:

(1) Libel consists of the publication of defamatory matter by written or printed words, by its embodiment in physical

154 Bustos v. A & E Television Networks, 646 F.3d 762, 764 (10th Cir. 2011); see also Hancock v. Variyam, 400 S.W.3d 59 (Tex. 2013) (“Defamation is generally defined as the invasion of a person’s interest in her reputation and good name.”).
155 RODNEY SMOLLA, 1 LAW OF DEFAMATION § 1:10 (2d ed. Nov. 2018).
form or by any other form of communication that has the potentially harmful qualities characteristic of written or printed words.

(2) Slander consists of the publication of defamatory matter by spoken words, transitory gestures or by any form of communication other than those stated in Subsection (1).

(3) The area of dissemination, the deliberate and premeditated character of its publication and the persistence of the defamation are factors to be considered in determining whether a publication is a libel rather than a slander.\textsuperscript{156}

A video, obviously, is neither written nor printed. As a result, whether a video should fall under libel or slander is not unanimously settled law.

As recently as 1998, the Tennessee Court of Appeals observed that “[t]here is no clear consensus among” courts as to “whether a television broadcast should be designated as libel or slander.”\textsuperscript{157} Indeed, some courts have adopted a more discerning test, mandating some proof of a prepared script or historical record.\textsuperscript{158}

The Restatement, however, states definitively that “[b]roadcasting of defamatory matter by means of radio or television is libel, whether or not it is read from a manuscript.”\textsuperscript{159} And indeed, many courts have adopted this reasoning,\textsuperscript{160} including more recent reviews of the

\textsuperscript{156} \textsc{Restatement (Second) of Torts}, § 568 (1977).
\textsuperscript{158} \textit{See} \textit{Charles Parker Co. v. Silver City Crystal Co.}, 116 A.2d 440, 443 (Conn. 1955) (“The basis of the distinction between libel and slander is the written or printed word or passage. Having been reduced to permanent form and published, the written or printed word has greater capabilities of harm. We can see no difference between the reading of defamatory words from a prepared manuscript to a group of people within the presence of the reader, which constitutes libel, and reading defamatory words from a prepared manuscript to be broadcast by the facilities of a radio station. The latter simply carries the defamatory words farther because the defamer has used a medium for dissemination which reaches listeners far beyond the ordinary limits of the human voice. The law of libel is applicable to the case at bar.”).
\textsuperscript{159} \textsc{Restatement (Second) of Torts}, § 568A.
\textsuperscript{160} \textit{See} \textit{Brown v. Hearst Corp.}, 862 F. Supp. 622, 627 (D. Mass. 1994), aff’d, 54 F.3d 21 (1st Cir. 1995) (“[B]ecause the allegedly offensive statements were fixed, recorded, and widely distributed in a television program, if defamation does exist in this case, it is libel and not slander.”).
question.\textsuperscript{161} Two separate policy justifications reinforce this reasoning. First, a broadcast's wide dissemination puts ‘the broadcaster upon the same footing as the publisher of a newspaper.’\textsuperscript{162} Second, with technological progress, few things are unrecorded and kept private in the way a conversation does. Therefore, the general rule applies that “[a] defamatory statement addressed to the eye, such as a writing or a photograph, is libel. One addressed to the ear, such as a spoken word, is slander.”\textsuperscript{163} Because a deepfake—as opposed to any captions or descriptions thereof—are permanent, defamation actions arising from deepfakes would likely be exclusively the purview of libel actions.\textsuperscript{164}

“Libel is governed predominantly by state law, and the elements of libel vary by jurisdiction.”\textsuperscript{165} But many, if not most, elements of libel remain common across state lines. Consider New York:

In order to state a cause of action for libel under New York law, a plaintiff must plead: (1) a written false and defamatory statement of fact concerning the plaintiff; (2) that was published by the defendant to a third party; (3) due to the defendant’s negligence or actual malice, depending on the status of the person libeled; and (4) special damages or \textit{per se} actionability.\textsuperscript{166}

\textsuperscript{161} See Sabino v. WOIO, L.L.C., 2016-Ohio-491, ¶ 41, 56 N.E.3d 368, 376 (Ohio Ct. App. 2016) (“defamatory matter broadcast by means of radio or television is classified as libel”).


\textsuperscript{163} Franco v. Diaz, 51 F. Supp. 3d 235, 244 (E.D.N.Y. 2014) (citation omitted); see also Hardesty v. Waterworks Dist. No. 4 of Ward Four, 954 F. Supp. 2d 461, 475 (W.D. La. 2013) (“Libel is defamation which is ‘expressed by print, writing, pictures, or signs’, while slander is communicated by ‘oral expressions or transitory gestures.’” (citation omitted)); Doe v. Mobile Video Tapes, Inc., 43 S.W.3d 40, 48 (Tex. App. 2001) (“Libel is defamation in written or other graphic form that tends to injure a person’s reputation, exposing the person to public hatred, contempt, or ridicule. Slander is orally communicated defamation.” (internal citations omitted)); Hardesty v. Waterworks Dist. No. 4 of Ward Four, 954 F. Supp. 2d 461, 475 (W.D. La. 2013) (“Libel is defamation which is ‘expressed by print, writing, pictures, or signs’, while slander is communicated by ‘oral expressions or transitory gestures.’” (citation omitted)).

\textsuperscript{164} And, relatedly, any discussions of defamation pertain exclusively to libel.


New York libel law, like other states, considers photographs as “statements” sufficient to allege libel.\textsuperscript{167} Elements two and three are also satisfied because any deepfaker clearly publishes the content to a third party, i.e. not to the subject of the fake, and exhibits actual malice, as he or she knowingly creates falsified content. Indeed, in some states, malice may entitle deepfake victims to additional punitive damages.\textsuperscript{168} However, evaluating deepfakes’ applicability to libel actions, then, requires further consideration of elements one and four: Is a deepfake defamatory? And what damages do deepfakes impose?

1. \textit{Is a Deepfake Defamatory?}

Defamation is broadly defined as a false “statement that tends to expose the [individual] to public contempt, ridicule, aversion, or disgrace, or induce an evil opinion of him in the minds of right-thinking persons, and to deprive him of their friendly intercourse in society.”\textsuperscript{169} Outside of clear parodies, which do not give rise to defamation action,\textsuperscript{170} determining whether something is defamatory can be particularly difficult when edited video is involved. As Judge Raymond Dearie of the Eastern District of

\begin{itemize}
\item\textsuperscript{167} See, e.g., Palmisano v. Modernismo Publications, Ltd., 98 A.D.2d 953, 954 (Sup. Ct. N.Y. 1983).
\item\textsuperscript{168} See, e.g., Gleason v. Smolinski, 125 A.3d 920, 948 (Conn. 2015).
\item\textsuperscript{170} See \textit{supra} notes 162–164 and accompanying text.
\end{itemize}
New York, now the namesake to the courthouse’s atrium,\textsuperscript{171} presciently observed in 1994:

\begin{quote}
[T]elevision broadcasts add new and potentially significant variables to the defamation analysis. Courts must scrutinize the juxtaposition of the audio and video portions of a television program. In subtle ways, a television director can alter the tone of an otherwise innocuous broadcast. With the emerging popularity of self-styled “magazine” news programs, courts should be sensitive to the possibility that a transcript which appears relatively mild on its face may actually be, when the total mix of creative ingredients are considered, highly toxic. Indeed, a clever amalgamation of half-truths and opinion-like statements, adorned with orchestrated images and dramatic audio accompaniment, can be devastating when packaged in the powerful television medium.\textsuperscript{172}
\end{quote}

Like such television broadcasts, deepfakes are primed to add further wrinkles to defamation analysis.

However, some deepfakes are quite simple to navigate with respect to defamation. Some, for example, are decidedly not defamatory. Consider the example referenced above in which a man, in homage to his wife’s favorite show, placed her in that show\textsuperscript{173} There is nothing disgraceful about such a video so as to invoke defamation.

Deepfakes made with an obvious humorous intent may also be easily disposed of should they prompt a victim to sue. A deepfake turning President Trump into Biff Tannen, the villainous character in \textit{Back to the Future}, was obviously made as a parody.\textsuperscript{174} The character is fictional, and the connection is meant to be a caricature of the President. To be sure, “[a] defendant cannot escape liability for defamatory factual assertions simply by claiming that the statements were a form of ridicule, humor, or

\textsuperscript{171} See Courthouse Atrium Dedicated to Judge Dearie, N.Y. L. J. (May 1, 2018, 10:00 AM), https://www.law.com/newyorklawjournal/2018/05/01/courthouse-atrium-dedicated-to-judge-dearie/ [https://perma.cc/8XL5-3FSQ].
\textsuperscript{173} See supra notes 56–58 and accompanying text.
\textsuperscript{174} See supra note 53.
sarcasm.” But “if the allegedly defamatory statement could not be reasonably understood as describing actual facts about the plaintiff or actual events in which he participated, the publication will not be libelous.” Deepfakes like Trump-as-Biff fall squarely into that category, which defamation law has long dealt with smoothly.

Deepfake pornography is different. Without question, falsely placing someone in an adult video without his or her consent could seriously “harm the reputation of [the victim] as to lower him [or her] in the estimation of the community or to deter third persons from associating or dealing with him [or her].” This conclusion is also analogically supported by case law in which courts have upheld defamatory causes of action where edited videos appear to show the subject acting in a way other than what in fact occurred. To immunize deepfakers from defamation action would undermine society’s “pervasive and strong interest in preventing and redressing attacks upon reputation,” the public policy driving defamation.

Content is not the only factor considered, however; the video’s context (e.g. its caption) play a role in defamation analysis. “[T]he rule of innocent construction” states “[a] written or oral statement is to be considered in context, with the words and the implications therefrom, given their natural and obvious meaning; if so construed the statement may reasonably be innocently interpreted . . . it cannot be actionable per se.” Applying this thinking, if the deepfaker is quite clear about the fact that the video is fabricated or fantastical, he or she has a stronger defense that the video does not inflict the same harm on the video’s subject. On the

---

178 See, e.g., Cummins v. Bat World Sanctuary, No. 02-12-00285-CV, 2015 WL 1641144, at *22 (Tex. Ct. App. Apr. 9, 2015); cf. N.B.C. v. Gonzalez, No.04-95-00219-CV, 1995 WL 624549, at *5 (Tex. Ct. App. Oct. 25, 1995) (“The portion that was broadcast was a truthful depiction of appellee’s conduct, and as such, is not defamatory. While inclusion of the entire video and audio may have been more flattering to appellee, this Court will not sit as a senior editor to television stations.”) (internal citations omitted); Newton v. Nat’l Broad. Co., 930 F.2d 662, 686 (9th Cir. 1990), cert. denied, 502 U.S. 866 (1991) (failure to broadcast complete statement of plaintiff is not indicative of actual malice).
other hand, if the individual creating and posting the video makes no effort to dispel the mistruth of the video’s subject, the video is more likely to be considered legitimate and thus harm one’s reputation. Ultimately, it is likely the case that a deepfake satisfies the first element of a libel action and clears the first hurdle, though not absolutely certain.

2. What Damages Regime Do Deepfakes Fall Under?

Assuming a deepfake is defamatory, a court must then determine appropriate damages. Defamatory statements can either be actionable per se or per quod. Per se actionable statements mean “its harm is obvious and apparent on its face.”181 “Statements falling outside of these categories may only be actionable as libel per quod which requires that special damages be alleged.”182 In the latter situation, the words’ “injurious nature appears only in consequence of extrinsic facts.”183

Typically, “[w]ords tending to impute criminal offense, loathsome disease, business misconduct, or serious sexual misconduct constitute defamation per se.”184 This final sub-category of per se defamatory is quite broad: for example, “[t]he traditional common law position is that the imputation of unchastity” meets this standard.185 To this end, courts have repeatedly affirmed that statements pertaining to one’s sexual life, including reports of one’s alleged extramarital affairs or sexual habits, are per se actionable.186 Thus, a falsified video that purports to demonstrate one’s sexual actions, the filming thereof, and its subsequent publication, could indeed be considered defamatory per se.

Even if a pornographic deepfake is not per se defamatory, the special damages requirement in a defamatory per quod cause of action is likely met. “In a defamation per quod action, damage to the plaintiff’s reputation is not presumed and the plaintiff must plead and prove special

185 2 LAW OF DEFAMATION § 7:18 (2d ed.).
186 See, e.g., Hoskins v. Fuchs, 517 S.W.3d 834, 843 (Tex. Ct. App. 2016), review denied (Feb. 16, 2018) (concluding that statements made in law student’s complaint to university’s office of equal opportunity services, alleging that student's girlfriend was having sexual relationship with professor, qualified as defamation per se); Moreau v. Brenan, 466 So. 2d 572, 574 (La. Ct. App. 1985) (holding that wife and husband were defamed by allegations that wife was having extramarital sexual relations, and those allegations constituted defamation per se).
damages.” Special damages are “actual damages of a pecuniary nature.” Thus, a plaintiff must plead that pecuniary damages are appropriate as a remedy to his or her cause of action.

In many instances, a deepfakes create substantial risk of financial harm for its victims because of the inherent value of one’s reputation, particularly when that person is a public official.

[A] public image is a valuable asset. A favorable public image enables a public figure to earn large fees for lecturing or for endorsing products. It is a source of influence in politics, entertainment, sports, religion, education, or other fields. It may be an important source of self-esteem and personal satisfaction. A person who enjoys a positive public image thus may be injured by defamation, even if there is no harm to his existing or future personal relations.

This problem is only amplified by the blindingly fast pace at which news, particularly harmful news, spreads on the Internet. One case is particularly instructive: In Stephen G. Perlman, Rearden LLC v. Vox Media, Inc., The Verge, a website that “examine[s] how technology will change life in the future for a massive mainstream audience,” published an article that Perlman claimed defamed both himself and his company, OnLive, following its bankruptcy. The statistics regarding the speed with which the article was shared are staggering:

In the first fifteen minutes after The Verge published the August 28 Article, various journalists and editors associated with The Verge, Polygon, and Vox

---

188. Imperial Apparel, Ltd. v. Cosmo’s Designer Direct, Inc., 882 N.E.2d 1011, 1018 (Ill. 2008).
189. David A. Anderson, Reputation, Compensation and Proof, 25 WM. & MARY L. REV. 747, 766 (1984); see also Denny v. Mertz, 318 N.W.2d 141, 151 (Wisc. 1982) (“A person’s reputation and good name is of inestimable value to him and once it has been besmirched by another through carelessness or malice restoration is virtually impossible.”) (internal footnote omitted).
191. Id. at *1.
promoted the article as the “definitive account” based on “exhaustive proof,” despite the fact that they had not fact-checked the article . . . using social media platforms such as Facebook, LinkedIn, Twitter, Tumblr, and Google+ to reach hundreds of thousands, if not millions, of readers. Readers quickly posted 300 comments (288 in the first two days) responding to the August 28 Article, and the article spread rapidly through social media networks. Soon the August 28 Article became a top Google search result for “OnLive,” behind only OnLive’s own corporate and service web pages and the OnLive Wikipedia page.\(^\text{192}\)

Additionally, the court took note of the permanence of the allegedly defamatory article:

> In fact, two years later the August 28 Article was still the fourth Google result for “OnLive.” Also, when Internet users use Google to search for “Steve Perlman,” Google provides three “In-depth articles,” which it identifies as “high-quality content to help [users] learn about or explore a subject;” the August 28 Article appears alongside two articles from www.businessweek.com and www.smithsonianmag.com, respectively, both highly credible publications.\(^\text{193}\)

> In no small part due to the article’s widespread dissemination and permanence, the court held that the damage done to Perlman was genuine, compelling the judge to deny Vox’s motion to dismiss.\(^\text{194}\)

> So, too, could be the fate of a deepfake victim. If the video is to be believed—whether sexual or otherwise—the reputational damage could be swift and lasting. Therefore, pending specifics, a cause of action for defamation may be the ideal avenue for any deepfake victim.

\(^{192}\) Id. at *5.
\(^{193}\) Id.
\(^{194}\) See id. at *21.
B. Privacy Torts

The right to privacy “dates back to a law review article published in December of 1890 by two young Boston lawyers, Samuel Warren and Louis Brandeis.”\(^{195}\) "A specific suggestion of [Warren’s], as well as [Warren’s] deep-seated abhorrence of the invasions of social privacy . . . led to [their] taking up the inquiry."\(^{196}\) The first cases recognizing an actionable invasion of the right to privacy were heard and decided a decade later.\(^{197}\)

Despite the Supreme Court’s statement that its right to privacy jurisprudence “def[jed] categorical description,”\(^{198}\) Dean William Prosser, the father of modern American tort law, described the state of privacy law as follows:

The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley “to be let alone.”\(^{199}\)

The four privacy torts are intrusion upon seclusion, publicity given to private life, publicity in false light, and wrongful appropriation. Each tort, and its application to deepfakes, is examined herein.

---

\(^{195}\) Dorothy J. Glancy, _The Invention of the Right to Privacy_, 21 ARIZ. L. REV. 1, 1 (1979).

\(^{196}\) _Id._ at 6 n.29 (1979) (first and second alterations in original) (quoting Letter from Brandeis to Warren (April 8, 1905)). Glancy offers an excellent glimpse into the publication’s critical and popular acclaim. _See id._ at 6–7 (citing _The Right to Be Let Alone_, 67 ATLANTIC MONTHLY 428–29 (1891)); _The Defense of Privacy_, 66 SPECTATOR 200 (Feb. 7, 1891); _Comment_, 3 GREEN BAG 524, 525 (1891).


1. Intrusion Upon Seclusion

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.200

Intrusion upon seclusion is not dependent on the “the truth or falsehood of the information itself”; instead, it “deals with the manner in which Defendant obtained the information.”201 For example, in Peterson v. Moldofsky202 the plaintiff “claim[ed] that Defendant intruded on her privacy by emailing photographs of her engaged in group sex to several people.”203 However, the court held that “no intrusion occurred, as [the Plaintiff] knew of and consented to [the Defendant’s] presence and his taking of pictures during the sex acts [meaning] there ‘is no evidence of an intrusion as based on the manner in which the information is obtained[,]’”204

The import of Peterson’s reasoning is made clear when compared with DePiano v. Atlantic County.205 In that case, the plaintiff, Gregory DePiano, was a corrections officer and Sergeant at the Atlantic County Justice Facility (ACJF).206 While DePiano served in that capacity, an ACJF warden and internal affairs officer, Gary Merline, disseminated photographs from DePiano’s personnel files in which he was dressed in women’s clothing, which he admitted “is, or at some point was, part of his sexual life.”207 Merline, by abusing the access afforded by his position, therefore intruded upon DePiano’s seclusion.208

Juxtaposing Peterson and DePiano demonstrates that it is the manner of the intrusion that makes all the difference. In Peterson, the purported “intrusion” occurred with one’s consent to obtain information—
photographs—of the plaintiff in compromising situations, even if the plaintiff failed to restrict how such information was disseminated. On the other hand, in DePiano, the victim in no way permitted the intruder access to such information. In sum, “the tort of intrusion upon seclusion is based upon the manner in which an individual obtains information,” not whether the private information was thereafter disseminated.

Deepfake creators are more likely in the Peterson camp rather than the DePiano camp. True, the victim’s did not consent to the way in which the photos were used. But as in Peterson, the victims knowingly consented to their creation in the first place, not to mention their dissemination into and throughout the public domain. In many (though not all) cases, the deepfake subject has either put the photos into the public by posting them online or consented to their collection by posing for paparazzi. Deepfakers have not violated anyone’s personal space to obtain the necessary information to create and publish their work. Thus, as was the case in Peterson, a deepfake victim is unlikely to prevail on an intrusion of seclusion claim.

2. Publicity Given to Private Life

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

- (a) would be highly offensive to a reasonable person, and
- (b) is not of legitimate concern to the public.210

This second tort is not a candidate for a deepfake victim for one reason: “an essential element of the tort of public disclosure of private facts is that the facts at issue be true.”211

In the “earliest non-consensual pornography lawsuit,”212 the infamous publication Hustler was adjudged to have invaded LaJuan

209 Haehn, 702 F. Supp. at 1531.
Wood’s privacy by publishing a stolen photograph of her in the nude with a “falsely attributed lewd fantasy.”213 The court held Hustler liable for publicity in a false light—discussed substantively infra—rather than a private facts theory because the fantasy did not truthfully reflect Wood’s private life.214 The same reasoning holds true for all deepfakes, in which “none of the facts disclosed by the picture are alleged to be true.”215 This theory of liability is thus altogether foreclosed.

3. Publicity in False Light

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

- (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
- (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.216

Dean Prosser identified the seminal false light invasion of privacy case: the successful 1816 suit by the famous English poet Lord Byron to enjoin circulation of a volume of bad poetry falsely attributed to him.217 Two centuries later, false light has a distinct application to deepfakes.

Deepfakes, by definition, place an individual before the public in a false light. Deepfakes, “[n]onconsensual [videos] created through digitally manipulated images of victims[, are] entirely false because the victim never posed for the image.”218 This is most certainly the case with non-pornographic videos.219

214 Id. at 1090 (citing RESTATEMENT (SECOND) OF TORTS §§ 652D cmt. a, b, 625E cmt. b (1977)).
218 Levendowski, supra note 212, at 434 (citing Tsoulis-Reay, supra note 212).
219 While the idea of acting in a traditional film may seem innocuous enough, one need only look to the actors who have sworn off working with Woody Allen in light of
Consider again the aforementioned *Wood v. Hustler* case. There, the court was persuaded that Hustler was liable for falsely representing that Wood consented to the submission and publication of a photograph depicting her in the nude in the coarse and sex-centered magazine. Moreover, the publication falsely attributed a lewd fantasy to Wood.\(^{220}\) To be sure, the same could be said for any actor that “appears” in a sexually explicit video via a deepfake, or any deepfake for that matter. Without question, the fabricated video would ascribe conduct to an actor, which he or she did not participate in, nor would such an actor likely consent to the dissemination of video suggesting they did participate in these illicit acts.

### 4. Wrongful Appropriation

*One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.*\(^{221}\)

A victim of a deepfake may have a cognizable claim for wrongful appropriation, otherwise called misappropriation.\(^{222}\) “The tort of wrongful appropriation requires that the defendant appropriate the plaintiff’s likeness to his own use or benefit.”\(^{223}\) Usually, such use or benefit is attributed to a commercial or financial benefit.

Though opponents may rebut that they are not benefitting commercially,\(^{224}\) victims have two substantial arguments. First,
individuals who drive consumers to the website hosting the videos, particularly those that advertise the purported video alongside “promotional images,” are acting with a commercial purpose. Consider, for example, an individual who publishes his or her own blog that hosts the deepfake and offers pedestrian digital ads on the very same page. By driving traffic to the page via the deepfake, he or she stands to earn additional revenue because advertisers pay more money to advertise on pages visited more frequently.

Moreover, only four states—New York, Oklahoma, Utah, and Virginia—specifically articulate that the appropriation must “be for advertising, or for purposes of trade.” Thus, deepfakers are unlikely to successfully defend themselves on the argument that because they acted without a commercial purpose, they are not liable for a wrongful appropriation cause of action.

Second, deepfakers are nevertheless using the individual’s likeness without consent and “injure[] the economic interests of the plaintiff due to commercial exploitation[].” Whether the individual in question is a celebrity or layperson is irrelevant; it is not a requirement that one be a public official to have his or her likeness appropriated without her consent for economic reasons.

Moreover, a deepfaker cannot hide behind “the general rule . . . that incidental use of a name or likeness does not give rise to liability for invasion of privacy by appropriation.” Because a deepfake tries to attract attention based on the false premise of its purported subject and because the victim is the chief—and ever-present—subject in the deepfake, its use cannot be considered incidental.

---

227 Ault, 860 F.2d at 883.
228 See generally Manger v. Kree Inst. of Electrolysis, 233 F.2d 5 (2d Cir. 1956) (affirming the general ‘right of privacy’ violation for manipulating a contest winner’s submission for an advertisement and running the altered material without her consent); Colgate-Palmolive Co. v. Tullos, 219 F.2d 617, 619 (5th Cir. 1955) (affirming a right of privacy violation for misappropriating one’s likeness in an advertisement when the individual in question was not a celebrity).
229 Aligo v. Time-Life Books, Inc., No. C 94-20707 JW, 1994 WL 715605, at *2 (N.D. Cal. Dec. 19, 1994) (collecting cases). To determine if a use is incidental, consider (1) whether the use has a unique quality or value that would result in commercial profit to the defendant, (2) whether the use contributes something of significance, (3) the relationship between the reference to the plaintiff and the purpose and subject of the work, and (4) the duration, prominence or repetition of the name or likeness relative to the rest of the publication. See id. at *3 (citations omitted).
Ultimately, appropriation may yet be a lost cause (of action). Wrongful appropriation cases, particularly those involving digital images of one’s likeness, are almost always using the victim’s likeness to endorse or advertise a particular product. A deepfake, thus, presents an atypical fact pattern because deepfakers may not be attempting to create their own commercial benefit like the typical defendant in a wrongful appropriation case. For example, a deepfaker that creates an explicit video of a celebrity and posts it online to a site from which they derive no revenue does not serve an economic purpose.

So, courts may be reluctant to recognize that a deepfaker’s personal use and enjoyment of a fabricated video, even if it is disseminated on the Internet for others’ personal, analogous use and enjoyment. Without any promise of monetary value, personal deepfakes are likely insufficient to satisfy the elements of appropriation.

C. Right of Publicity

What may instead prove to be the most direct source of redress is a cause of action alleging a violation of the victim’s right of publicity, an interrelated but distinct right. Plainly, “the right of publicity is an economic right to use the value of one’s own celebrity.”

The right of publicity exists to “prevent[] unjust enrichment by the theft of good will. No social purpose is served by having the defendant get free some aspect of the plaintiff that would have market value and for

---

231 See Toffoloni v. LFP Publ’g Grp., LLC, 572 F.3d 1201, 1205 (11th Cir. 2009) (defining the “right of publicity [as] protect[ing] against ‘the appropriation of another's name and likeness’”) (quoting Martin Luther King, Jr., Ctr. for Social Change, Inc. v. Am. Heritage Prods., Inc., 296 S.E.2d 697, 703 (Ga. 1982)).
232 In re NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1284 n.1 (9th Cir. 2013) (Thomas, J., dissenting); see also ETW Corp. v. Jireh Publ’g, Inc., 332 F.3d 915, 928 (6th Cir. 2003) (“The right of publicity is an intellectual property right of recent origin which has been defined as the inherent right of every human being to control the commercial use of his or her identity.”) (citing McCARTHY ON PUBLICITY AND PRIVACY, § 1:3); Comedy III Prods., Inc. v. Gary Saderup, Inc., 21 P.3d 797, 807 (Cal. 2001) (“[t]he right of publicity holder possesses is not a right of censorship, but a right to prevent others from misappropriating the economic value generated by the celebrity’s fame”).
which he would normally pay.”233 In light of this reasoning, “[a]ll that a plaintiff must prove in a right of publicity action is that she has a pecuniary interest in her identity, and that her identity has been commercially exploited by a defendant.”234

But “[t]he distinctive aspect of the common law right of publicity is that it recognizes the commercial value of the picture or representation of a prominent person or performer, and protects his proprietary interest in the profitability of his public reputation or ‘persona.’”235 Thus, unsurprisingly, the quintessential right of publicity cases involve cases in which celebrities’ distinct yet replicable traits are used without their permission—“so-called ‘impersonator’ cases”236—including Midler v. Ford Motor Co.237 and Waits v. Frito-Lay, Inc.238 In both, famous actors with distinct voices refused to partake in advertisements, and companies responded by circumventing their refusal and recreating celebrities’ trademark voices with sound-alike voice actors after the stars declined to participate in the advertisement themselves.239

The same is true with deepfakes: celebrities are deprived of their ability to control their likeness or image. And while [d]amages from such evident abuse of a plaintiff’s property right in his public reputation are plainly difficult to measure by monetary standards,240 courts, depending on relevant state law, are open to awarding both the “market value”241 of the celebrity’s persona used and damages to compensate for any “induce[d] humiliation, embarrassment, and mental distress.”242 Therefore, celebrity deepfake victims may succeed on a right to publicity claim against the deepfaker. However, a right to publicity cause of action is far

234 Parks v. LaFace Records, 329 F.3d 437, 460 (6th Cir. 2003) (citations omitted).
237 Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1989).
239 See Faber, supra note 236.
240 Ali, 447 F. Supp. at 729 (citing Myers v. U.S. Camera Publ’g Corp., 167 N.Y.S.2d 771, 774 (City Ct. N.Y. 1957)).
241 Waits, 978 F.2d at 1103.
242 Id. (quoting Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 824 (9th Cir. 1974)).
from a certain victory for the victim; deepfakers have substantial counterarguments in the form of satire.

In some instances, defendant deepfakers have a substantial defense against right of publicity claims: parody. “The right of publicity derived from public prominence does not confer a shield to ward off caricature, parody and satire. Rather, prominence invites creative comment.”

Political cartoonists, for example cannot be held civilly liable for depicting a celebrity or politician in what any observer reasonably recognizes is a lampoon. This rule should similarly hold true for other obvious forms of parodies, including deepfakes, such as the aforementioned parody deepfake depicting President Trump as television or movie characters.

But even satire has its limits; the Supreme Court, in its Bresler–Letter Carriers–Falwell line of cases, provides protection for statements that cannot “reasonably [be] interpreted as stating actual facts” about an individual. The very point of though deepfakes is to create video so seamlessly superimposed that the reasonable person cannot discern fact from fiction. Common sense tells us that videos falsely portraying individuals in compromising and intimate affairs cannot be considered a parody.

“The right of publicity a holder possesses is not a right of censorship, but a right to prevent others from misappropriating the economic value generated by the celebrity’s fame.” But the right is not conditioned on celebrity; in the last nearly forty years, the right of publicity doctrine has dramatically expanded to include laypersons.

In 1982, the Supreme Court of Georgia compared one’s “right not to have another appropriate one’s photograph” in two cases—one involving a private person, one involving a public figure. The court concluded that “private citizens have the right of privacy, public figures have a similar right of publicity, and that the measure of damages to a

244 See id. at 460 n.12 (“For example, Garry Trudeau, creator of the satiric cartoon strip ‘Doonesbury,’ regularly fictionalizes events and dialogue involving prominent political figures. It cannot be seriously maintained that one such satirized notable could successfully pursue an action for an infringement on his right of publicity based on such use.”).
245 See supra notes 53–55 and accompanying text.
public figure for violation of his or her right of publicity is the value of the appropriation to the user.”

To be sure, given the very nature of celebrity, in right of publicity causes of action involving high-profile plaintiffs, “the mere allegation that the plaintiff was not compensated has been deemed sufficient to satisfy the injury prong.” But courts now recognize that this right belongs to the entire population.

A California statute codified this right. “The [relevant] statutory text makes no mention of preexisting value, and in fact can be read to presume that a person whose name, photograph, or likeness is used by another for commercial purposes without their consent is ‘injured as a result thereof.’” Consequently, “California courts have clearly held that ‘the statutory right of publicity exists for celebrity and non-celebrity plaintiffs alike.’”

Logic similarly dictates this result. In *KNB Enterprises v. Matthews*, the copyright owner of erotic photographs of non-celebrity models brought a cause of action when said photos were displayed without authorization, and for profit, on the Internet. The court specifically noted that in terms of damages, the models’ “anonymity . . . is allegedly a valuable asset in the marketing of erotic photographs.” Further, “[i]n a society dominated by reality television shows, YouTube, Twitter, and online social networking sites, the distinction between a ‘celebrity’ and a ‘non-celebrity’ seems to be an increasingly arbitrary one.” Therefore, the deepfake “need not be a national celebrity to prevail” in a right to publicity action.

---

249 Id.
250 Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 807 (N.D. Cal. 2011) (citing Solano v. Playgirl, Inc., 292 F.3d 1078, 1090 (9th Cir. 2002); Newcombe v. Adolf Coors Co., 157 F.3d 686, 693 (9th Cir. 1998)).
253 Id. at 807 (quoting KNB Enterprises v. Matthews, 92 Cal. Rptr. 2d 713, 722 n.12 (Cal. Ct. App. 2000)).
255 Id. at 718.
IV. THE VIABILITY OF A § 230 DEFENSE

Even when deepfake victims are able to successfully sue the deepfaker, the deepfaker, likely an individual, may simply not have sufficient monetary funds to compensate the victim. Facing the potential to recoup only paltry sums, the victim may also choose to go after the publisher, namely the website, that hosts the video, a (likely) wealthier entity. However, the publisher would likely assert a defense from liability under § 230 of the Communications Decency Act (CDA). Yet, this famous—or infamous, depending on one’s perspective—shield may in fact be penetrable by deepfake victims.

A. The History, Text, and Exceptions of § 230 of the Communications Decency Act

Understanding § 230’s protections and exceptions requires a thorough review of § 230’s verbiage, Congress’s intent in enacting it, and the interpretation of the act since the 1990s.

In October 1994, an anonymous Internet user wanted to alert the public to what he felt was fraudulent and illegal securities trading activity by Stratton Oakmont. To do so, the user posted his suspicions on a message board entitled Money Talk, which was run by Prodigy Communications Corporation (Prodigy), a leading Internet Services Provider at the time. Stratton, none too pleased at the accusation, sued Prodigy as well as the particular administrator of the Money Talk message board for libel in New York Supreme Court. Because Prodigy “held itself out to the public and its members as controlling the content of its computer bulletin boards” and “implemented this control through its automatic software screening program,” the court ruled that Prodigy was

259 This is the same Stratton Oakmont whose founders and executives would be jailed for perpetrating myriad frauds that were given notoriety by co-founder Jordan Belfort’s novel The Wolf of Wall Street and thereafter by Martin Scorsese’s eponymous film.
indeed a publisher that could be found liable.\textsuperscript{263} The court also found that the administrator acted as Prodigy’s agent and thus could similarly be found liable.\textsuperscript{264}

After the enactment of Section 230, the court noted that Congress was aware of the \textit{Stratton} decision and:

remove[d] the disincentives to selfregulation [sic] created by the \textit{Stratton Oakmont} decision. . . . Fearing that the specter of liability would . . . deter service providers from blocking and screening offensive material, Congress enacted § 230’s broad immunity “to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.”\textsuperscript{265}

But the \textit{Stratton} decision was not Congress’s sole impetus for § 230. At that time, the public was just starting to understand the vast potential of the Internet and was, thus, just beginning to comprehend the sheer quantity of data and information that it could transmit. As Judge Wilkerson writes in \textit{Zeran v. America Online, Inc.}, the “seminal case”\textsuperscript{266} explicating the statute:

The amount of information communicated via interactive computer services is . . . staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.\textsuperscript{267}

\textsuperscript{263} Id. at *4.
\textsuperscript{264} Id. at *6.
\textsuperscript{266} Bennett v. Google, LLC, 882 F.3d 1163, 1166 (D.C. Cir. 2018).
\textsuperscript{267} Zeran, 129 F.3d at 331.
With dual purpose, Congress enacted § 230. The operative part reads:

(1) . . . No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) . . . No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

So, to summarize, the provision protects:

[Websites against suits based on torts committed by users. For instance, Wikipedia cannot be held liable for defamation posted by a user. This intermediary liability protection encourages websites to engage in content moderation without fear that their efforts to screen content will expose them to liability for defamatory material that slips through.]

As the D.C. Circuit described, “the intent of the CDA is thus to promote rather than chill internet speech.” And in light of such protections, it has understandably been “lauded as ‘the most important law protecting internet speech’ and called ‘perhaps the most influential law to protect the kind of innovation that has allowed the Internet to thrive.’”

270 Bennett, 882 F.3d at 1166 (citing Zeran, 129 F.3d at 331).
271 First Amendment Rule, supra note 269 (footnotes omitted).
On the other hand, the statute can, and does, protect online platforms and publishers from defamation suits brought by those who claim to have been defamed. Thus, if a victim wishes to pursue the publisher for monetary or equitable reasons, defamation causes of action, among others, may be foreclosed. Other causes of action, however, may be available through § 230’s exceptions.

Despite its broad protections, § 230 is not without limits. Congress carved out four important exceptions in which an ISP is liable for what resides on its (digital) pages:

(1) No effect on criminal law
   Nothing in this section shall be construed to impair the enforcement of . . . any . . . Federal criminal statute.

(2) No effect on intellectual property law
   Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law
   Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law
   Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.\(^{272}\)

Via these carve-outs, the CDA incentivizes service providers to actively curate their platforms and excise impermissible content.\(^{273}\)

Of late, the outer bounds of these exceptions have been tested. Most notably, the first exception has come under fire, as litigants have questioned whether social media giants like Facebook and Twitter should be held liable for the actions terrorists have taken by using their platforms

\(^{272}\) Communications Decency Act, 47 U.S.C § 230(e) (2018).

\(^{273}\) See Bennett, 882 F.3d at 1166 (quoting Zeran, 129 F.3d at 331).
to help carry out attacks. But the second exception, which withholds the statute’s protections for violations of intellectual property, may create sufficient judicial daylight for deepfake victims seeking federal redress.

B. Clarifying the Intellectual Property Exception

The intellectual property exception under § 230 states, in lay terms, that individuals may still sue digital content platforms if the platform publishes copyrighted material. Digital platforms are thus heavily incentivized to remove all such content. Because deepfakes manipulate likely copyrighted videos, it is worth examining whether copyright law can provide a basis for victims’ legal redress.

But a deepfake victim’s ability to assert a cause of action under this exception is not a guarantee. Indeed, copyright protections may be inapposite for deepfake victims for two reasons. First, the victim likely does not own the copyright interest in the manipulated video and thus cannot claim a cause of action pursuant to property he or she does not own. Second, the manipulation may be so egregious as to render the video transformative.

However, intellectual property law is not solely constrained to copyright protections. Instead, victims may still pursue a cause of action against platforms that publish harmful and destructive deepfakes by asserting a right of publicity, a different intellectual property right. But legal hurdles and defenses, as well as strategic considerations, may foreclose this avenue of remediation. This theory of liability and two of its potential hurdles are discussed below.

---

276 See infra Section V.A on Fair Use.
1. Privacy or Intellectual Property?

“[O]ne might argue that the right of publicity is a privacy issue, not an intellectual property right at all.”

To be sure, “[t]he right of publicity is, somewhat paradoxically, an outgrowth of the right of privacy,” but that does not mean that the right is solely a question of a right to privacy, which would not be actionable under § 230. To the contrary, the Eleventh Circuit wrote that “there appears to be no dispute that the right of publicity is a type of intellectual property right.” Legal scholars agree.

Therefore, the right of publicity should clear this first legal hurdle, fitting within the intellectual property exception, without tremendous obstacle.

2. What Laws Define Intellectual Property under Section 230?

Were a victim to pursue a right of publicity claim under the intellectual property exemption to § 230, other issues would arise. One of these issues is whether § 230’s intellectual property exception includes both state intellectual property law and federal intellectual property law. Courts are divided on this issue. The Southern District of New York, the First Circuit, and the Middle District of Florida have said “[c]laims based on intellectual property laws are not subject to § 230 immunity,” while the Ninth Circuit Court of Appeals has said otherwise.

In Atlantic Recording Corp. v Project Playlist, Inc., a corporation named Project Playlist (Playlist) “operate[d] a website . . . that provides an index of links to songs available on third-party websites . . . [that allowed users to] download the songs from the third-party websites.”

---

279 Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1323 (11th Cir. 2006).
282 Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1108 (9th Cir. 2007).
[Plaintiffs,] six of the world’s largest record companies[,] sue[d] Playlist for copyright infringement and unfair competition. Plaintiffs own[ed] copyrights to the majority of sound recordings in the United States, and claim[ed] that most of the songs on the third-party websites to which Playlist provides links are posted without plaintiffs’ permission, and therefore infringe[d] plaintiffs’ copyrights.\(^{284}\)

Facing this state law copyright claim, Playlist tried to limit the CDA to apply only to federal claims, filing a motion to dismiss under § 230 on the basis that the exception in question “means that nothing in the CDA should be construed to limit any federal intellectual property law.”\(^{285}\) The court disagreed and found that § 230’s plain text did not support that contention.\(^{286}\)

The fact that Section 230(e)(3) addresses state law does not mean that a reference in another subsection to “any law” is meant to only encompass federal law. Indeed, Section 230(e)(1) refers specifically to federal criminal law, see 230(e)(1) (referring to “any other Federal criminal statute”), and the specific reference would be unnecessary if Playlist were correct that subsections (1), (2), and (4) covered only federal law. Playlist’s contention is also contradicted by subsection (4), which refers to, inter alia, “any similar State law.”\(^{287}\)

The First Circuit reached the same conclusion, albeit without similarly rigorous analysis.\(^{288}\) And, relying on these two decisions, district

\(^{284}\) Id. at 693.
\(^{285}\) Id. at 702.
\(^{286}\) See id. at 702–04.
\(^{287}\) Id. Playlist also argued that the CDA “preempts all state laws relating to intellectual property, because those laws are inconsistent with the CDA.” Id. Judge Chin similarly discarded this claim. See id.
\(^{288}\) See Universal Commc’n. Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 422–23 (1st Cir. 2007) (stating “[c]laims based on intellectual property laws are not subject to Section 230 immunity”).
courts in the Middle District of Florida and the District of New Hampshire have parroted this conclusion.

Setting up a potential Supreme Court battle due to circuit split, the Ninth Circuit takes the opposing stance. In *Perfect 10, Inc. v. CCBill LLC*, Perfect 10, the publisher of an adult entertainment magazine and the owner of the subscription website perfect10.com, alleged that CCBill and CWIE violated copyright, trademark, and state unfair competition, false advertising, and right of publicity laws by providing services to websites that posted images stolen from Perfect 10’s magazine and website.

As the *Perfect 10* court notes, “[t]he CDA does not contain an express definition of ‘intellectual property,’ and there are many types of claims in both state and federal law which may—or may not—be characterized as ‘intellectual property’ claims.” The panel held that the lack of uniformity among state intellectual property laws foreclosed the possibility that the patchwork state law could form the basis of the intellectual property exception:

Such laws may bear various names, provide for varying causes of action and remedies, and have varying purposes and policy goals. Because material on a website may be viewed across the Internet, and thus in more than one state at a time, permitting the reach of any particular state's definition of intellectual property to dictate the contours of this federal immunity would be contrary to Congress’s expressed goal of insulating the development of the Internet from the various state-law regimes. In the absence of a definition from Congress, we construe the term “intellectual property” to mean “federal intellectual property.”

That is the extent of Ninth Circuit’s analysis.

---

291 *Cf. Braxton v. United States*, 500 U.S. 344, 347 (1991) (“A principal purpose for which we use our certiorari jurisdiction, and the reason we granted certiorari in the present case, is to resolve conflicts among the United States courts of appeals and state courts concerning the meaning of provisions of federal law.”).
292 488 F.3d 1102, 1108 (9th Cir. 2007).
293 *Id.* at 1118.
294 *Id.* at 1118–19.
The Southern District has the better of the argument. Indeed, Judge Chin convincingly grappled with—and summarily disposed of—the Ninth Circuit’s reasoning to show that its reasoning “lacks any support in the plain language of the CDA.”

In four different points in § 230(e), Congress specified whether it intended a subsection to apply to local, state, or federal law. It is therefore clear from the statute that if Congress wanted the phrase “any law pertaining to intellectual property” to actually mean “any federal law pertaining to intellectual property,” it knew how to make that clear, but chose not to.

Moreover, the modifier “any” in Section 230(e)(2), employed without any limiting language, “amounts to ‘expansive language [that] offers no indication whatever that Congress intended [a] limiting construction.’” This conclusion is bolstered by the fact that, as discussed above, the “surrounding statutory language” supports the conclusion that Congress intended the word “any” to mean any state or federal law pertaining to intellectual property.

Therefore, state law intellectual property claims—such as the right of publicity—ought to fall under the intellectual property exception, thereby clearing another hurdle. But even if the right of publicity is considered a state intellectual property claim, and further, if state intellectual property claims are considered within the § 230 intellectual property exception, liability of the deepfaker is not guaranteed. That is, while the deepfaker may not shield itself from liability under § 230 because of the intellectual property exception, the elements under a right of publicity claim, discussed supra Section III.B, must still be met and its relevant defenses considered.

Unsurprisingly, more courts not bound by either court’s opinion as precedent favored the Southern District. See, e.g., Malibu Media, LLC v. Weaver, No. 8:14-CV-1580-T-33TBM, 2016 WL 1394331, at *8 (M.D. Fla. Apr. 8, 2016); Parisi v. Sinclair, 774 F. Supp. 2d 310, 318 (D.D.C. 2011) (“I am not inclined to extend the scope of the CDA immunity as far as the Ninth Circuit.”).

This was prior to his elevation to the Second Circuit.


Id. at 703–04 (citations omitted).
V. COPYRIGHT LAW IS NO WHITE KNIGHT, BUT THE DMCA MAY BE

Unlike in the case of revenge pornography, copyright law is unlikely to provide victims an avenue of redress against perpetrators of deepfakes, despite the assertions of some commentators. The Patent and Copyright Clause of the Constitution affords Congress the power “[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.” But because the victims of deepfakes do not own the underlying copyright of the source material, victims have no copyright claim. Additionally, only the owner of the copyrighted source material from which the deepfake was created could file a copyright infringement suit, and given the expense of litigation and the limited returns that a copyright holder may receive from a deepfake creator, it is unlikely a copyright holder would pursue a copyright infringement suit to vindicate deepfake victims. Nevertheless, the Digital Millennium Copyright Act (DMCA) may still provide victims with some reprieve.

A. Copyright Infringement

The Copyright Act effectuates that power bestowed on copyright owners as envisioned in the Patent and Copyright Clause of the U.S. Constitution. Section 102 of the Copyright Act reads:

Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise

\[299\] See generally Levendowski, supra note 212 (arguing that copyright law provides a persuasive vehicle for revenge porn victims).


\[301\] U.S. CONST. art. I, § 8, cl. 8.
communicated, either directly or with the aid of a machine or device. 302

“To establish infringement, two elements must be proven: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original.” 303 First, ownership can be established by demonstrating that the claimant is the initial author or that the work was a work for hire. 304 Second, copying may occur in two different ways: through exact copying or by making a substantially similar copy. Obviously, deepfakes, because elements of the original video have been changed, are not exact copies, and thus, a court would only need to consider, under this second element, whether the deepfake was substantially similar to the original video.

A deepfake victim does not have a copyright infringement claim because he or she is not the original author and would not have created the deepfake as a work for hire. Thus, the victim is not the copyright owner, removing any viable argument for a copyright infringement claim. However, a production company—presumably the creator of the original work—is the likely owner of the copyright. Yet, even though such a production company, as the copyright owner, likely satisfies this first element, they have little economic incentive to invest in and pursue a lawsuit on behalf a deepfake victim for two reasons: (1) the uncertainty of litigation in its pursuit of an infringement claim is likely not worth the financial risk, and (2) even if the copyright owner succeeds, the deepfaker (whether attempting to create explicit videos or setting out to make a non-pornographic parody) will likely not have the funds to pay any damages. So, under element two, copying, regardless of whether the deepfake is substantially similar or not to the original work, the owner of the original work is unlikely to bring suit. 305

Additionally, while a producer might pursue a deepfaker for their own economic purposes, it is unlikely they will pursue a cause of action for a victim’s economic benefit, again given the substantial cost of

---

305 In the event a copyright owner pursued an infringement suit on moral or principled grounds, the parties would need to consider whether the deepfake and the original video were substantially similar and whether the deepfaker had a fair use exception to infringement. For fair use factors, see 17 U.S.C. § 107.
litigation.\footnote{306} In other words, even if the copyright owner succeeded in the litigation and even if a deepfaker paid a damages award, the monetary damages paid to the copyright owner would not help the deepfake victim.

B. An Alternative to Litigation

While the copyright owner of the underlying original video may lack a financial interest to pursue a cause of action against deepfakers in litigation, the copyright owners may be willing to pursue a substantially less costly alternative to litigation—a DMCA takedown notice.

The Digital Millennium Copyright Act (DMCA)\footnote{307} provides an alternative to litigation that may help reduce the harm to victims. The DMCA provides a safe harbor to online services from copyright infringement for hosting copyrighted material on their platform if, and only if, the platform makes a good faith effort to take down the material upon being notified of its existence.\footnote{308} “Merely by sending a proper takedown notice, a copyright owner can prompt an Internet Service Provider (‘ISP’) to swiftly remove an allegedly infringing item from its servers; ISPs earn immunity from infringement liability if they provide that swift removal and thus are incentivized to comply.” \footnote{309}

Therefore, if the copyright owner of a video is informed by a deepfake victim of the deepfake and if the copyright owner informs the video hosting platform...
that the deepfake has been posted, the online service provider will likely take down the video to protect itself from litigation.

Given the choice between a resource-intensive and time-consuming lawsuit and a swift, viable alternative, copyright owners are likely to prefer enforcing their rights with a DCMA takedown. Additionally, the relatively low cost and minimal effort of the DMCA takedown process may even incentivize copyright owners to file takedown notices on behalf of deepfake victims. So even though a victim may not be able to procure monetary damages from a copyright lawsuit, because they do not own the underlying copyright of the original work, the DMCA takedown provision, with the cooperation of the copyright owners, provides a promising alternative to litigation that might achieve what the deepfake victim really desires: removal of the victimizing video from the Internet.

CONCLUSION

Deepfakes are a problem. That much is certain. The technology is easily deployable, growing in prevalence, and seeing its technological underpinnings improve. Additionally, deepfakes have the potential to be weaponized in serious and global ways. Simultaneously, efforts to combat deepfakes, though growing, do not appear to keep pace with the technological prominence.

As this article demonstrates, this problem lacks a clear-cut solution. Neither an outright ban of deepfakes nor a bill seeking only to regulate their production is unlikely to survive a court challenge. The First Amendment likely provides sufficient refuge for deepfakers to guard against such measures.

As discussed, four possible state tort remedies may intuitively come to mind—intrusion upon seclusion, publicity given to private life, publicity in false light, and wrongful appropriation. But wrongful appropriation is likely the only tort action in which a deepfake victim may successfully seek refuge.

Irrespective of the theory pursued, § 230 of the Communications Decency Act creates a shield for content providers, preventing victims from naming the host platform as a defendant, thereby limiting recovery to

the deepfake creator. Moreover, the costs of litigation—temporally and monetarily—when counterbalanced against potentially limited damages, will likely dissuade a victim from pursuing legal action.

The lack of available remedies should compel reflection on both the legal frameworks at play, as well as the technical precipice on which we sit. Reconsideration of what speech is and is not protected by the First Amendment may be warranted, and courts may want to consider whether non-consensual pornography of any kind, revenge porn or deepfakes, should be the foundation of a new exception to the First Amendment’s broad protections.\textsuperscript{311} By the same token, Congress may want to reflect on to whether or not § 230 needs revisiting to accommodate an Internet that has changed considerably since 1996.

\textsuperscript{311} See Mary Anne Franks, “Revenge Porn” Reform: A View from the Front Lines, 69 Fla. L. Rev. 1251, 1312 (2017).
NOTES
THE BONA FIDE ACQUISITION RULE APPLIED TO CRYPTOCURRENCY

Andrew Balthazor*

CITE AS: 3 GEO. L. TECH. REV. 402 (2019)

I. INTRODUCTION

Cryptocurrency is an attractive target for theft. This digital property is compact, portable, and subject to conversion by simply acquiring the private key, giving unfettered control to the key’s associated cryptocurrency. Crypto-theft may occur without any physical interaction with the true owner. Crypto-thieves are difficult to identify and—even when identified—are often out of the practical jurisdictional reach of owners seeking recovery. The blockchain, a public ledger underpinning any cryptocurrency, creates a permanent record of all transactions. A victim of theft can follow the digital transaction trail to identifiable third-parties several orders removed from the actual theft. A true owner’s only available remedy may be asserting claims against these innocent third parties. However, the bona fide acquisition rule works to protect good faith purchasers who acquire property without notice of misconduct. Are the principles justifying the bona fide acquisition rule fulfilled if applied to cryptocurrencies?

Users of cryptocurrencies largely rely on third-party services to exchange their value in one virtual currency into traditional fiat currencies or other cryptocurrencies.\(^1\) Cryptocurrency exchanges provide this service,

* Florida International University (FIU) College of Law, J.D. Candidate 2019; United States Military Academy, B.S. Computer Science 1999; Holland & Knight LLP, Blockchain Technology Law Clerk. I am grateful to Josias Dewey, Holland & Knight’s blockchain expert, for suggesting and discussing with me the topic of this paper. Thank you to Professor Hannibal Travis of FIU for brainstorming ideas relating to this topic, reviewing my work, and providing substantive feedback. I also owe a debt to FIU Professors M.C. Mirow for loaning me a book on property principles and suggesting other useful titles and Scott Norberg for letting me pepper him with UCC-related questions.

\(^1\) See generally Andrew Balthazor, Comment, The Challenges of Cryptocurrency Recovery, 13 FIU L. REV. (forthcoming 2019) (manuscript at 13–14) (describing the role
like commodities or securities exchanges.\textsuperscript{2} Using these services generally requires cryptocurrency owners to surrender possession to the third-party exchange.\textsuperscript{3} This creates hoards of virtual assets consolidated and entrusted to exchanges. Exchanges, in turn, become targets of thieves.

In 2013—the early days of Bitcoin—Tokyo-based Mt. Gox was the global king of cryptocurrency exchanges.\textsuperscript{4} Users relied on Mt. Gox to shepherd hundreds of millions of dollars in bitcoin, and in 2013 those users saw bitcoin’s value explode over 9,230\%.\textsuperscript{5} Mt. Gox’s software and security did not keep up with the rapidly increasing value of assets under its care.\textsuperscript{6} Hackers struck repeatedly.\textsuperscript{7} Over a period of several years, crypto-thieves siphoned off approximately 850,000 bitcoins,\textsuperscript{8} worth billions of U.S. dollars in today’s value.\textsuperscript{9} Mt. Gox collapsed into bankruptcy.\textsuperscript{10} Mark Karpeles, the owner and operator of Mt. Gox, allegedly squirreled away a significant sum\textsuperscript{11} from his company’s fiat currency bank accounts.\textsuperscript{12} The users of the exchange filed a class action against Karpeles and Mizuho Bank, the Japanese bank with which Karpeles conducted business.\textsuperscript{13} Notably absent as defendants were the thieves themselves, who were the primary cause of the plaintiffs’ loss. While Karpeles and the bank may bear some responsibility for the stolen bitcoin, why not pursue the crypto-thieves themselves? The hackers had control of the stolen assets, after all.


\textsuperscript{5} See id. (describing Bitcoin prices jumping from $13 to over $1200).

\textsuperscript{6} See id.

\textsuperscript{7} Id.

\textsuperscript{8} Id.


\textsuperscript{10} McMillan, supra note 4.

\textsuperscript{11} Id.

\textsuperscript{12} Greene v. Mizuho Bank Ltd., 206 F. Supp. 3d 1362, 1368 (N.D. Ill. 2016). Fiat currencies are traditional, government-backed currencies.

\textsuperscript{13} See id. at 1369–70.
The publicly viewable ledger technology underpinning all cryptocurrencies—the blockchain—allows users to trace virtual currency transactions. A wrongfully dispossessed cryptocurrency owner with a simple web browser can follow the digital trail of stolen assets. But, while the blockchain allows transaction tracing, it is pseudonymous: users conducting blockchain-based transactions are only identified by an alphanumeric public address, the functional equivalent of a conventional bank account number. Linking a cryptocurrency public address with an identifiable individual requires information not available on the blockchain. For example, some cryptocurrency exchanges maintain records personally identifying users in response to know-your-customer (KYC) regulations. A user could trace a series of blockchain transactions to a cryptocurrency exchange that maintains KYC records and identify the cryptocurrency recipient.

Crypto-thieves are necessarily motivated to avoid blockchain transactions that could reveal their identity. But while this anonymity may prevent identification of the bad actors directly responsible for a cryptocurrency theft, the stolen virtual assets are still tied to the blockchain and, consequently, traceable. Eventually, thieves realize the value of their stolen cryptocurrency by selling the stolen currency for another virtual currency, fiat currency, or real-world goods.

---

14 See John Bohannon, Why Criminals Can’t Hide Behind Bitcoin, SCI. MAG. (Mar. 9, 2016), https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin [https://perma.cc/G9DN-NBC5]; e.g., Nathaniel Popper, Bitcoin’s ‘First Felon’ Faces More Legal Trouble, N.Y. TIMES (Nov. 2, 2018), https://www.nytimes.com/2018/11/02/technology/bitcoin-charlie-shrem-winklevoss-twins.html [https://perma.cc/NBV8-8C2B] (“When he purchased $4 million in real estate, two Maseratis and two powerboats, we decided it was time to get to the bottom of it,’ Mr. Winklevoss told The New York Times. The brothers hired an investigator, who found that 5,000 Bitcoins were transferred in 2013 through addresses associated with Mr. Shrem and onto the Bitcoin wallet services Xapo and Coinbase, according to the complaint. The investigator traced the money on the blockchain, the public ledger where all Bitcoin transactions are recorded.”).


16 Bohannon, supra note 14.

17 See id.


20 See Singh, supra note 18 (“[M]oney laundering in Bitcoin usually bleeds outside of the virtual network eventually. If the owner converts her bitcoins into USD at another Bitcoin
these buyers may be innocent purchasers unaware that they are acquiring stolen cryptocurrency.

Unlike crypto-thieves, innocent purchasers of stolen cryptocurrency have no reason to take measures to disguise their identity (at least, no reasons connected to the stolen cryptocurrency). An innocent purchaser is thus more likely to interact with vendors or cryptocurrency exchanges that maintain KYC records. Accordingly, there is a better chance of identifying innocent purchasers of stolen cryptocurrency than identifying the crypto-thieves themselves.

Whether a wrongfully dispossessed owner of cryptocurrency may recover cryptocurrency from an innocent purchaser depends on the application of the bona fide acquisition rule. Bona fide purchasers of value who purchase stolen property in good faith, without notice that the property is stolen, acquire title to that stolen property free from prior claims in some contexts but not in others. Whether the bona fide acquisition rule should apply depends on the purposes of the rule and whether the rule’s purposes are fulfilled as applied to particular property types.

This paper discusses the application of the bona fide acquisition rule to cryptocurrencies. In Section II, this paper provides a brief functional primer on cryptocurrency and crypto-theft. Section III describes the practical and policy reasons for the bona fide acquisition rule, why it applies to some types of property and not others, and the unsatisfactory outcome of treating cryptocurrency as if it were one of these property types. Section IV concludes that harnessing the power of cryptocurrencies would achieve the practical and policy objectives of the bona fide acquisition rule. Cryptocurrencies could protect the property interests of owners by incorporating robust transactional information—giving notice of illicit transactions and secured interests—which would use the potential of cryptocurrencies’ distributed public ledger. Such improvements would place cryptocurrencies into a property class unto themselves, able to efficiently protect earlier-in-time possessory and security interests, while simultaneously allowing free-flowing transactions and giving purchasers confidence that their acquired cryptocurrency is devoid of prior adverse claims.
II. A PRIMER ON CRYPTOCURRENCY AND CRYPTO-THEFT

Modern cryptocurrencies are distributed software systems that allocate units of value to addresses and allow for the exchange of those units between addresses on the same system. When dealing with the Bitcoin cryptocurrency, those value units are bitcoins, or fractions thereof. Because Bitcoin is the original blockchain-based cryptocurrency, this paper uses bitcoin as a generic term for cryptocurrency value units. Many derivative cryptocurrencies now exist, but most cryptocurrencies share the same functional characteristics described herein.

New bitcoin is generated through a process called mining, which is an incentive-based process that contributes to transaction authentication and is reliant on encryption. Every bitcoin is allocated to a public key address represented by alphanumeric characters; when bitcoin is generated by mining, that bitcoin is credited to the miner’s public address. Sending bitcoin from a public key address requires that address’s private key, a separate alphanumeric code. The private key is the exclusive means of initiating outgoing transactions from an address, and anyone with access to the private key has unrestricted control over the associated address’s bitcoin. The cryptocurrency software authenticates a transaction by checking that the private key is correct and that the requested bitcoin is available to the sending address. Once a transaction is authenticated, the bitcoin is essentially debited from the sending address, credited to the receiving address, and the transaction is added to the blockchain. Transactions are authenticated in batches, called blocks, and then strung together to form a chain of transactions: the blockchain.

The blockchain provides a publicly viewable history of all transactions, beginning with a bitcoin’s generation. Perhaps counter-intuitively, the blockchain does not maintain a static list of “account

---

21 See generally Balthazor, supra note 1, at *6 (describing cryptocurrencies).
24 See id. at *7.
25 Id.
26 See id. at *10.
27 Id. at *8.
28 Id.
29 Id.
30 Id. at *10.
balances” for all bitcoin addresses. Software interfacing with the bitcoin’s blockchain determines the amount of bitcoin associated with an address by calculating the sum of all incoming and outgoing transactions relating to an address. But this sum is an abstraction of bitcoin’s reality: ownership of bitcoin is instead “a share in an informally organized social process,” and that share’s value is only recognized by knowing all of an address’s incoming and outgoing transactions. For example, take real-world cash: a person can count their money by opening their wallet. With bitcoin, your “wallet” only contains a reference to a list of all receipts and expenditures you have ever made. You only know how much bitcoin you control by calculating the sum of those transactions. Transactions added to the blockchain are functionally irrevocable due to the cryptography involved and distributed software authentication, an intentional feature designed to prevent double-spending.

Crypto-theft occurs when a person dispossesses the rightful owner of the address’s bitcoin without the true owner’s consent. This may happen because the private key (which controls the bitcoin address) was compromised, which is what occurred in the Mt. Gox hack. Private keys are stored in any number of ways: digitally, online, offline, encoded into devices, or written down on paper. Crypto-thieves acquire an address’s private key by hacking, malware, social engineering, coercion, or any other manner of taking the private key from a person. The thief then uses the stolen private key to send the address’ bitcoin to another address under

31 *Id.* at *8.
32 *Id.*; see, e.g., BLOCKCHAIN, https://www.blockchain.com/btc/address/3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r [https://perma.cc/SE65-9Y6B] (displaying the transactions and amount of bitcoin associated with an address—one of the largest hoards of bitcoin at the time of writing).
34 See Nakamoto, *supra* note 23, at *1. Some cryptocurrency development teams have implemented or considered controversial “forks” to reverse the effects of vast amounts of illicitly transferred cryptocurrency. These forks are changes to the software underlying a cryptocurrency to reset a blockchain to a prior state or to create wholly new cryptocurrencies to compensate victims. See, e.g., Stan Higgins, *8 Million Vericoin Hack Prompts Hard Fork to Recover Funds*, COINDESK (July 14, 2014), https://www.coindesk.com/bitcoin-protected-vericoin-stolen-mintpal-wallet-breach [https://perma.cc/TBW6-RPB5].
the thief’s control, stealing the bitcoin from the true owner.\textsuperscript{38} Alternatively, an owner may be extorted or forced to transfer cryptocurrency to a thief’s address without necessarily surrendering private keys. For example, criminals may infect a system with ransomware (a form of malicious computer code), which infects a system and denies access to user files until a bitcoin payment is made to a specific address.\textsuperscript{39}

The cryptocurrency system itself provides no recourse to the victim of crypto-theft. Cryptocurrency transactions are irrevocable. Victims may trace transactions through the blockchain, but criminals with the skills to steal cryptocurrency are generally careful to avoid transactions that would allow a victim to identify them. Eventually, an innocent third party will acquire the stolen cryptocurrency. Unlike criminals, innocent third parties are not motivated to maintain anonymity by fear of prosecution. A victim of crypto-theft may identify the innocent third party through their transactions with entities like retail stores or cryptocurrency exchanges, which may have records tying the innocent third party to the transactions.

After a victim identifies the third-party possessor of the stolen cryptocurrency, can the victim assert claims against them? Answering this question requires examining the purposes of the bona fide acquisition rule and the results of applying it to cryptocurrencies.

\textbf{III. RECOVERING STOLEN PROPERTY AND THE BONA FIDE ACQUISITION RULE}

At common law, the general principle is that a true owner—one with a valid first-in-time interest—may recover their stolen property from whomever possesses it, even when the thief sells the stolen property to an innocent purchaser: a bona fide purchaser who, in good faith, purchases for value the property without notice of the theft.\textsuperscript{40} This principle, originating in Roman law, was modified and adapted to suit the needs of changing economies with an exception for certain types of property: the bona fide acquisition rule.\textsuperscript{41} The bona fide acquisition rule allows an

\textsuperscript{38} See, e.g., \textit{id.}


\textsuperscript{40} Kenneth G.C. Reid, \textit{Banknotes and their Vindication in Eighteenth-Century Scotland}, in \textit{Money in the Western Legal Tradition: Middle Ages to Bretton Woods} 556, 564 (David Fox & Wolfgang Ernst eds., 2016) (“The principle was the familiar one of \textit{nemo plus iuris ad alienum transferre potest, quam ipse haberet.”)."

\textsuperscript{41} See \textit{id.} at 566–68, 571–72.
innocent purchaser to acquire certain types of stolen property free from the risk that the property may be claimed by the former rightful owner. The rule arises from the concept that possession is strong evidence of ownership, and thus, an innocent purchaser is justified in relying on that presumed ownership. When the rule applies, the former owner’s remedy is limited to an action against the thief only.

For example, say a thief steals a unique piece of art and a pile of cash. An innocent third party with no notice of the theft then acquires the art for a substantial sum. This third party does not have clean title; the true owner of that artwork may bring an action against the third-party purchaser, subject to certain limitations, and recover their stolen property. If the same innocent third party sold the thief a car—thereby acquiring the thief’s stolen pile of cash—that innocent third party acquires the pile of cash with good title, free and clear of any prior claims.

Thus, a true owner seeking to recover property from an innocent purchaser faces two possible scenarios dependent on the nature of the stolen property: (1) the innocent purchaser acquires the stolen property free from any prior adverse claim, preventing recovery by the true owner; or (2) the innocent purchaser acquires the stolen property subject to the claims of the true owner, allowing the true owner to recover. The bona fide acquisition rule represents a compromise between the competing interests of transaction efficiency and protection of ownership. Understanding this compromise requires a discussion of the rule’s purpose and application with respect to money, personal property, and secured interests in intangible property and a determination as to whether the rule’s purposes are served by treating cryptocurrency like any of these defined property types.

---

42 See id. at 566, 571.
43 See UGO MATTEI, BASIC PRINCIPLES OF PROPERTY LAW: A COMPARATIVE LEGAL AND ECONOMIC INTRODUCTION 107 (2000) (discussing that possession of a physical object is strong evidence of ownership, creating a presumption that a possessor may rightfully transfer ownership to another).
44 See Reid, supra note 40, at 568.
46 See id. at 867 (“[I]f the paintings were stolen, the thief acquired no title and could not transfer good title to others regardless of their good faith and ignorance of the theft.”).
A. An Economic Explanation of the Two Legal Treatments of First-in-Time Interests in Stolen Property

An economic view of property law explains the different approaches to protecting the property interests of either the true owner or a later innocent purchaser. Property rules must protect ownership interests because there would be little incentive to own property and use it productively without such protection.48 Property rules must also allow for efficient transfers of those interests to attain the most economic use of property.49 To this end, a property system must reduce disputes between claimants with competing interests or allow for efficient dispute resolution. If there are too many disputes resulting in costly enforcement actions, then the high cost of dispute resolution reduces the efficiency of the overall system.50

An economic property system encourages transfers of property to those people who value it most because those owners would be the most motivated to make the property most productive.51 Reducing the transaction costs of exchanging property is thus the lynchpin of any economic system.52 Transaction costs include all private and public costs of policy development and enactment, record searches, negotiations (transfer-related costs), dispute resolution, and enforcement.53 Transaction costs tend to rise with the value of the property transacted because value attracts more competing parties and results in potentially conflicting claims.54

48 See Hans-Hermann Hoppe, The Ethics and Economics of Private Property, in THE ELGAR COMPANION TO THE ECONOMICS OF PROPERTY RIGHTS 48, 57 (Enrico Colombatto, ed., 2004) ("Men pay most attention to what is their own; they care less for what is common; or at any rate they care for it only to the extent to which each is individually concerned.") (quoting Aristotle).
50 See id. at 111.
51 See Hoppe, supra note 48, at 57 (explaining that people apply themselves to increasing the value of property when that property belongs to them).
52 See Libecap, supra note 49, at 108–09 (discussing the historical development of more economic property systems and concluding that “transaction costs mold bargaining for changes in property rights, influencing the positions of the parties involved and the nature of the institutions that ultimately result”).
53 Id. at 109; see also Joshua Fairfield, Bitproperty, 88 S. CAL. L. REV. 805, 845 (2015) (“[P]roperty can best be explained as the process of optimizing property rights by reducing information costs for search, verification, or transfer.”).
54 See Libecap, supra note 49, at 112.
These economic principles are manifested in the bona fide acquisition rule and its application (or not) to certain types of property. Innocent purchasers of property are protected where (1) frequent transactions in that property are critical to commerce and (2) title searches are so impractical as to place too great a cost or burden on each transaction relative to the value of the transacted property. Thus, the use of money favors bona fide purchasers: money is frequently transacted and impractical to trace.\footnote{See discussion, infra Section 1.} Property that is traded less frequently, that has existing title registration systems, or that retains significant value after exchange, such as security interests or vehicles, justifies having higher transaction costs without a disproportionate impact on the free exchange of property.\footnote{See Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24 U. MIAMI BUS. L. REV. 1, 36 (2016) (describing a rule requiring inquiry into title for certain classes of interests not overly burdensome because it would only affect a small class of property that are usually subject to title registration systems and that retain post-transaction value).}

B. Protecting the Free Flow of Commerce over First-in-Time Interests

One of the earliest exceptions to the general rule that a first-in-time true owner may recover their property from an innocent purchaser was grounded in practical evidentiary concerns. The exception is rooted in Roman law, the starting point of many Western common legal principles:

Should another’s coins be paid, without the knowledge or volition of their owner, they remain the property of him to whom they belonged; should they have been mixed, it is written in the books of Gaius [Cassius Longinus] that should the blending be such that they cannot be identified, they become the property of the recipient so that their [former] owner acquires an action for theft against the man who gave them.\footnote{See Reid, *supra* note 40, at 568 (quoting *THE DIGEST OF JUSTINIAN* (Alan Watson ed., 1985) (alterations in original)).}

Thus, a true owner cannot recover stolen fungible property that is mixed with other like property because the stolen property is indistinguishable from property that belongs to another. This exception was based on issues of evidence, not of policy. English courts refined this exception for money, introducing an economic justification for the rule.
1. Money and the Bona Fide Acquisition Rule

Money is a broad category. Black’s Law Dictionary defines money as “[t]he medium of exchange authorized or adopted by a government as part of its currency . . . . Assets that can be easily converted to cash . . . . Capital that is invested or traded as a commodity . . . . [and] Funds.”58 Courts have also defined money to mean “an object used to buy things,”59 “a medium of exchange [convertible] into a currency which can pay for things,”60 and “a measure of value, or a means of payment.”61

The modern version of the bona fide acquisition rule came into being in the mid-18th century. The introduction of paper currency in late 17th century England and Scotland forced courts to decide matters involving bank notes stolen from true owners and presented for payment at banks.62 Early decisions regarding stolen bank notes denied true owners an action against an innocent possessor, relying on the maxim “money has no earmark.”63 True owners simply could not prove that a specific bank note belonged to them.

A Scottish attorney, Hew Crawfurd, challenged this maxim when he signed and recorded the serial numbers of two Bank of Scotland £20 notes—thereby specifically identifying them—prior to their theft in 1748.64 Crawfurd had mailed the notes to a Glasgow merchant. When the notes failed to arrive, Crawfurd notified the Bank of Scotland and advertised the missing notes in newspapers, including the notes’ identifying details: their serial numbers and Crawfurd’s signature on each note. One of the missing notes turned up several months later, presented for payment to the Bank of Scotland. Crawfurd demanded return of the note; the Bank refused, believing itself obligated to pay the bearer. Crawfurd brought an action against the Bank for return of the note in Crawfurd v. The Royal Bank.65 Crawfurd argued the general rule that possession is insufficient to transfer an interest in stolen property: “[T]he bare Possession of a Bank-note without the Consent of the Proprietor, will

58 Money, BLACK’S LAW DICTIONARY (10th ed. 2014).
60 Id.
62 Reid, supra note 40, at 568 & n.108 (citing Fox, supra note 47, at 559).
63 See Fox, supra note 47, at 548.
64 Reid, supra note 40, at 559.
65 See id. at 561, 564.
no more transfer the Property than the bare Possession of a Table or a Chair.”

In retort, the Bank argued in favor of a rule benefiting a purchaser who acquires stolen money in good faith: “a rule of bona fide acquisition ‘is agreeable to the Practice of all trading Nations at this Day, who possibly without having much Regard to the Subtilties [sic], have embraced it for this very good Reason, that the contrary would at once put a Stop to all Trade.”” The Bank was fundamentally making a policy argument.

Trade, it was argued for the banks, rested on the free circulation of money, and free circulation rested in turn on the reliability of notes and coins. If Crawfurd was able to vindicate the banknote, no merchant could risk taking money in payment “without being informed of the whole History of it from the Time that it was first issued out of the Bank or the Mint till it came to his Hand, which is so apparently absurd, that is seems hardly to merit a Consideration.” And as banknotes would thus be rendered “absolutely useless,” this would “in a great Measure deprive the Nation of the Benefit of the Banks, which could hardly subsist without the Circulation of their Notes.” . . . . If money could be vindicated, counsel for the Bank of Scotland concluded, “no Man could be sure, that one Shilling in his pocket was his own, and . . . Banks might shut their doors.”

The above argument has four components: (1) modern economies rely on money; (2) if a dispossessed owner could bring a claim for money, then everyone using money would have to inquire into the transaction history of money before accepting it as payment; (3) tracing the transaction history of money is “so apparently absurd, that is seems hardly to merit a Consideration”; and (4) because transaction tracing is so difficult, people would stop using money to avoid the risk of a true owner recovering money from their possession.

The Bank prevailed. The Court created an exception for money, preventing victims of theft from asserting claims against innocent third-

---

66 Id. at 564 (quoting MINUTES, THE GOVERNOR AND DIRECTORS OF THE BANK OF SCOTLAND AGAINST THE GOVERNORS AND DIRECTORS OF THE ROYAL BANK AND OTHERS 8 (Lord Strichen ed., 1749) (hereinafter BANK OF SCOTLAND MINUTES)).
67 Id. at 566 n.90 (quoting BANK OF SCOTLAND MINUTES, supra note 66, at 5).
68 Id. at 566 (internal citations omitted).
69 BANK OF SCOTLAND MINUTES, supra note 66, at 5.
party purchasers and thereby conceived the modern bona fide acquisition rule. English courts adopted—without reference to the Scottish decision—the same rule ten years later in *Miller v. Race*.\(^7^0\) American courts are in accord:

> It has long been considered necessary for practical business transactions that one who receives money in due course of business shall not be put on inquiry as to the title of the one paying the same. The reason frequently assigned is that money bears no earmarks, and therefore cannot be traced. But this argument is not tenable, for in many states we find that even though the money can be traced directly into the payee’s hand, still no recovery may be had even though the money has been stolen . . . . The real reason for such decision lies in the fact that money constitutes the currency of the nation, and by its use a civilized community is carried beyond the stage of barter.\(^7^1\)

However, this American summary neglects a logically required component of the policy argument in favor of the bona fide acquisition rule. The absurdly high burden of tracing the transaction history of money, relative to the importance of preserving the free flow of money in a modern economy, justifies applying the bona fide acquisition rule and allowing the use of money without inquiry as to its provenance.\(^7^2\)

It follows that if the cost of tracing a transaction evolves to have little or no impact on the free flow of money, then this erodes the economic justification for the bona fide acquisition rule. Cryptocurrencies may represent this evolution in transaction tracing.

2. *Treating Cryptocurrency as Money*

Courts treat cryptocurrency as money or currency when they apply statutes that reference those terms and the statute itself provides no definition. Relying on plain meaning and dictionaries, courts classify

---

\(^7^0\) *See generally* Miller v. Race, (1758) 97 Eng. Rep. 398 (K.B.); Reid, *supra* note 40, at 571.

\(^7^1\) C. Severin Buschmann & Leo M. Gardner, *Recovery of Stolen Money or Negotiable Instrument from Holder in Due Course—Is There an Indiana Rule?*, 5 IND. L.J. 195, 195 (1929).

\(^7^2\) In situations involving certain high value transactions we may require provenance of the funds used. Know-your-customer regulations and similar rules work to prevent money laundering and easy transfer of illicitly earned funds but are not intended to settle competing property interests. *See* Singh, *supra* note 18, at 45–46.
bitcoin as a medium of exchange and means of payment, meeting the definition of “money” or “funds” for statutes criminalizing conduct relating to money or funds. The Court has determined that bitcoin met the definition of money for property forfeiture relating to a money transmitting business.

The court’s decision was limited to determining that Bitcoin met a certain forfeiture statute’s definition of money but did not consider cryptocurrency in a broader property-rights context: whether the same property rules that apply to money should apply to cryptocurrency. The Uniform Commercial Code (UCC), a codification of common law principles governing commercial property transactions, excludes non-government-backed cryptocurrency from its definition of money: “Money means a medium of exchange currently authorized or adopted by a domestic or foreign government. The term includes a monetary unit of account established by an intergovernmental organization or by agreement between two or more countries.” Few cryptocurrencies are government-backed; major currencies like Bitcoin are not. Without governmental adoption or agreement, cryptocurrencies do not meet the UCC’s definition of money. Thus, it seems unlikely that a court would apply the same property rules relating to money to cryptocurrencies, which—under the common law as codified in the UCC—are not money.

Additionally, some of the justifications for treating money as favored property for conveyances do not apply to cryptocurrencies. Notwithstanding Mr. Crawfurd’s attempt to keep track of his £20 note, money has no practical transaction recording system, and thus, there is no way to check its provenance. Cryptocurrencies are the exact opposite. The blockchain reveals transaction histories of cryptocurrencies to the entire world. Thus, the transaction costs of verifying that any transaction involves only unburdened cryptocurrency are theoretically low. Low transaction costs for title-checking weigh in favor of protecting earlier-in-time interests against later innocent purchasers of stolen property.

---

75 U.C.C. § 1-201(b)(24) (AM. LAW INST. & UNIF. LAW COMM’N 2013).
77 See Schroeder, supra note 56, at 20.
78 See discussion, supra Section 1.
79 See discussion, supra Section A.A.
To treat cryptocurrencies like money for the purposes of the bona fide acquisition rule, a court would have to conclude that society’s interest in free-flowing cryptocurrency transactions outweighs the transaction costs of verifying that a transaction was free from prior adverse claims. For example, although the blockchain maintains transaction histories, it does not indicate when certain transactions are the product of crypto-theft. Purchasers would need to perform searches on third-party sites to verify that the addresses and transactions associated with a contemplated cryptocurrency transaction are free from reported misconduct. Even then, such searches may come up with nothing if a crypto-thief sufficiently obscures their transaction trail. A court may determine that this onerous process is too great a burden on commerce.

Applying the bona fide acquisition rule to cryptocurrencies would protect innocent purchasers but would eliminate the only likely remedy true owners can employ to recover stolen bitcoin. The Internet-based nature of cryptocurrencies and crypto-theft presents two challenges to a wrongfully dispossessed owner seeking to recover stolen bitcoin. First, crypto-thieves take measures to maintain anonymity. They are motivated to avoid engaging in blockchain-traceable transactions that could personally identify them. Second, even where a crypto-thief is identified, they may be in a jurisdiction that makes enforcement actions against them impractical.

80 See id.
82 See, e.g., Guillaume (@city19akro), TWITTER (Mar. 18, 2018, 5:04 AM), https://twitter.com/city19akro/status/975342278146428928?lang=en [https://perma.cc/7EEH-JSJJ] (“There’s an interesting story about how @CypheriumChain (a project where @Disruptpreneur & @el33th4xor are advisors to) got funds from their private sale hacked and they’re hiding it from solicited investors. Eth ended up here 0x94f20ccff70d82d1579d8b11f2985f8dc9b287cf.”).
85 See, e.g., Angela Morris, Judge Orders $30 Million in Bitcoin to Be Returned in Cryptocurrency Class Action, MIAMI DAILY BUS. REV. (Aug. 3, 2017), https://advance.lexis.com/api/permalink/e067ba8f-6e83-4192-a430-dec793182938/?context=1000516 [https://perma.cc/Z3FD-2PA5] (Plaintiffs secured a judgment against an embezzler who stole bitcoin, but they are unlikely to recover from the defendant who fled to China.).
Leaving true owners without any effective remedy for wrongful dispossession of cryptocurrency is unsatisfactory. Such an outcome would incentivize crypto-theft and discourage wide adoption of cryptocurrencies.

C. Protecting First-in-Time Interests Over Free-Flowing Transactions

The general principle of property law is to protect the earlier possessor—the true owner—against wrongful dispossession. This principle creates tension between owners and good-faith purchasers who have a possessory interest in property. Mere possession is sometimes insufficient to justify unfettered ownership when the earlier owner was dispossessed without their consent. The law produces different outcomes because the bona fide acquisition rule applies to some types of property but not others. Understanding the reasoning for this differing legal treatment of personal property or secured interests in intangible goods illustrates why applying the same rules to cryptocurrencies produces an unsatisfactory result.

1. Personal Property, Goods, and the Bona Fide Acquisition Rule

Legal systems protecting the rights of first-in-time owners against innocent purchasers do so within restrictions bound in both practice and policy. When dealing with personal—as opposed to real—property, legal treatment of the property depends on the property’s characteristics: tangibility (books versus contract rights), fungibility (artwork versus the hardware used to hang it), and consumability (a hamburger versus a car). These factors affect how strongly a legal system will protect true owners over innocent possessors; they create a loose taxonomy of property types. However,

[T]hese taxonomies are neither precise nor strict and their variety is staggering if one describes a multiplicity of legal systems. It is important to consider at our level of abstraction that different things may fit in a variety of taxonomies. The use of such taxonomies is justified by the need to handle with precision, to accommodate, and to submit to common rules objects whose nature may be different but whose legal regime for certain purposes should be the same. For example, a brand new car is a

---

88 See id.
fungible, nonconsumable, tangible good. A pound of bread is a fungible, consumable, tangible good.\(^{89}\)

While tangibility and fungibility are discussed herein, consumability is not relevant to a discussion relating to property rules and bitcoin. Bitcoin is not consumed but merely exchanged.

Tangibility argues for a recognition of good-faith possessory interests free from prior ownership interests because physical possession is widely recognized as a reliable indicator of ownership; innocent purchasers are justified in relying on possession in such circumstances and should be protected.\(^{90}\) This is not a hard and fast rule. Under UCC § 2-403, an innocent purchaser may not acquire good title to stolen tangible goods unless the purchaser acquired the goods in the ordinary course of business from a merchant who deals in goods of that kind and to whom the stolen goods were entrusted.\(^{91}\) Property that is intangible is necessarily harder to physically “possess” but is instead controlled by excluding others.\(^{92}\)

Laws that evolved around controlling physical property are not well-suited to intangible property.\(^{93}\) In particular, the presumption that possession indicates ownership\(^{94}\) is not as strong when dealing with control of intangibles, where control may be non-exclusive.\(^{95}\) Therefore, systems of control of intangibles tend to be governed by their own rules, such as the laws governing intellectual property or the laws of contract controlling the transfer of contract rights.\(^{96}\) These systems are grounded in property law principles, which have been adapted to the means of control of the intangibles in question.\(^{97}\)

Fungibility favors good-faith possessory interests. A possessor of a fungible item will have the stronger claim to it because it is generally impractical to distinguish one specific fungible item from another.\(^{98}\)

\(^{89}\) Id.

\(^{90}\) See id. at 107.

\(^{91}\) U.C.C. § 2-403 (AM. LAW INST. & UNIF. LAW COMM'N 2013); see also U.C.C. § 2-105 (AM. LAW INST. & UNIF. LAW COMM'N 2013) (defining goods).

\(^{92}\) See MATTEI, supra note 43, at 69.

\(^{93}\) See id. at 69–70.

\(^{94}\) Id. at 107.

\(^{95}\) See generally Fairfield, supra note 53, at 864–65 (employing the term “rivalrousness” as a “measure of exclusivity of possession” and discussing how physicality as a measure of possession has been inadequately analogized by courts to intangible digital property).

\(^{96}\) MATTEI, supra note 43, at 70. See generally Fairfield, supra note 53, at 865–68 (discussing how the law of intellectual property has intruded on and hampered the development of digital property law).

\(^{97}\) See MATTEI, supra note 43, at 70.

\(^{98}\) See Reid, supra note 40, at 570 (quoting JAMES DALRYMPLE STAIR, THE INSTITUTIONS
However, if fungible property is identifiable in some way, then that may allow assertion of an earlier ownership interest over a later possessor. For example, coins are fungible. But coins in a sealed sack, with an unbroken seal indicating they are the same coins that were lost, are discernable.99

Regardless of the above taxonomic divisions, certain property with peculiar ownership recording systems favors first-in-time owners against innocent purchasers who acquire stolen property.100 Here, first-in-time owners are favored because property tracked by recording systems is accepted by society as sufficiently valuable or important to protect ownership interests over even innocent possessors.101 A public recording system for certain property also serves a notice function to purchasers, who bear responsibility for checking the title of property prior to purchasing. For these special types of property interests, we accept the burden of title searches as necessary to protect the valuable or important associated interests. Property with a recording system tends to be high-value and not frequently exchanged. For example, vehicles and secured interests in certain property have a specific system of recording interests, paralleling the recording systems used for real property.102

For personal property and goods, the presumption is to protect earlier-in-time ownership interests.103 However, there are circumstances that may defeat that presumption and allow innocent purchasers to acquire good title to property.104 Whether the bona fide acquisition rule applies to non-consumable personal property depends on the property’s tangibility, fungibility, and the existence of a title registry. No one factor is dispositive. The determination distills into two inquiries, applied below: (1) whether the purchaser was justified in relying on the seller’s apparent control of the property as evidence of undisputed ownership and (2) whether the property is discernable and thus provably the property of another.

99 See Reid, supra note 40, at 571.
100 See Mattei, supra note 43, at 68, 87–88 (emphasizing, however, that it is the danger represented by vehicles and the need to attach liability that justifies vehicles’ recording system).
101 See id. at 88.
102 See id. at 88.
103 See Ziff, supra note 86, at 433.
104 See Fairfield, supra note 53, at 860 (“Error clearing rules also abound in the law of property. For example, rules of many different stripes protecting the rights of bona fide purchasers and buyers in the ordinary course of business clear accumulated clouds on title.”).
2. Treating Cryptocurrency as Traceable Personal Property

There appears to be little agreement as to what property classification is appropriate for cryptocurrency.\(^\text{105}\) For the purposes of the bona fide acquisition rule, a better approach is to consider whether cryptocurrency property characteristics support application of the rule to this novel sort of digital property.\(^\text{106}\)

Cryptocurrency has some peculiar characteristics that distinguish it from traditional notions of personal property. Whereas only one owner may physically possess tangible property, several people may share a private key controlling some amount of bitcoin.\(^\text{107}\) A private key may be printed out on a piece of paper. Thus, it is tangible and able to be physically held, but this does not restrict others from controlling the associated bitcoin if they know the private key.\(^\text{108}\) The bona fide acquisition rule depends on possession or control as a reliable indicator that the possessor is entitled to exercise ownership rights over property. If possession or control is not necessarily exclusive, then it is unreasonable to presume rightful ownership of the property merely because a person has control.

More importantly, cryptocurrencies are inextricably bound up in their own public recording system. Cryptocurrencies rely on the blockchain’s public ledger of transaction histories for their very existence. This is because the amount of bitcoin associated with a bitcoin address is really the sum total of all bitcoin transactions relating to that address.\(^\text{109}\) Take our earlier wallet example. A person could pick up anyone’s wallet, count the real-world cash, and know how much cash value they possessed. They can spend that cash ignorant of any prior transactions. But if a person were to come across the private key of a bitcoin address—thereby picking up another’s cryptocurrency “wallet”—that wallet only contains a reference to the ledger of all of that address’s transactions contained on the blockchain. A share of a cryptocurrency has relative value and utility inseparable from the blockchain, and the blockchain is a publicly viewable ledger of all transactions on which that cryptocurrency relies. This vast


\(^{106}\) See Fairfield, supra note 53, at 863–64 (arguing that digital property should “dispense with physicality (or conversely, intangibility) as the characteristic used to sort asset categories” and replace it with a more functional approach).

\(^{107}\) Raskin, supra note 36, at 994.

\(^{108}\) Id. at 990–91.

\(^{109}\) See discussion, supra Section II.
amount of transactional information is presented in an abstract form to users, but is required nonetheless.

If a complete knowledge of all transactions is required to use cryptocurrencies, then knowing that transaction history adds no costs to bitcoin transactions. Theoretically, this appears to completely undermine the justification for the bona fide application rule to cryptocurrencies. There are no transaction costs adding friction to commerce, and there is perfect knowledge of prior transactions: the best of both worlds. We can allow first-in-time owners to assert claims against later third parties because no purchaser would ever be acquiring cryptocurrency without knowledge of prior bad transactions.

This would be true, but for the fact that current blockchain variations maintain only basic transaction information. Current cryptocurrencies do not distinguish between “good” and “bad” transactions.110 On the blockchain, the aforementioned hacks of Mt. Gox (which resulted in almost a million stolen bitcoin) look the same as any other transaction.111 This information limitation places an unfair burden on innocent purchasers, who have no simple method for determining whether a contemplated bitcoin purchase involves stolen property or any other adverse claims.

3. Secured Interests in General Intangibles and the Bona Fide Acquisition Rule

A special category of property interests bears mentioning: secured interests in general intangibles under Article 9 of the UCC. The general intangible category is a catchall for personal property not included in other definitions under Article 9.112 The category includes intellectual property, software, and payment intangibles—rights to payment not included in other Article 9 categories.113 A secured, perfected interest in a general intangible is created when a debtor presents the intangible as collateral for

---

110 See Kaminska, supra note 81 (“Bitcoin’s public ledger records a transfer of digital access rights in the eyes of the clearing network. It does not, however, record or see the terms and conditions of that transfer. Indeed, as far as the clearing network is concerned all it knows is that a transfer has occurred.”).

111 Some third-party websites have recently begun flagging cryptocurrency addresses involved in crypto-theft based on user-generated reports. See, e.g., Address 0xaA923Cd02364Bb8A4c3d6f894178d2e12231655C, ETHERSCAN, https://etherscan.io/address/0xaA923Cd02364Bb8A4c3d6f894178d2e12231655c [https://perma.cc/SL6S-6LMN] (flagging this address with text on a red background stating, “[w]arning! This address is involved in Cryptopia’s hack.”). This information is limited to users of that particular website and is not embedded in the blockchain itself.

112 U.C.C. § 9-102 cmt. 5.d (AM. LAW INST. & UNIF. LAW COMM’N 2013).

113 U.C.C. § 9-102(42) & cmt. 5.d (AM. LAW INST. & UNIF. LAW COMM’N 2013).
a debt and the creditor has properly recorded their interest in it.\footnote{114} Once perfected, a security interest in a general intangible persists through transfers of the property, even to bona fide purchasers for value without notice.\footnote{115} This is different from the UCC’s treatment of a security interest in money, which applies the bona fide acquisition rule to protect innocent purchasers.\footnote{116}

4. Secured Interests in Cryptocurrency

The text of the UCC appears to bring secured interests in cryptocurrencies within the scope of Article 9.\footnote{117} Article 9’s catchall “general intangibles” category includes cryptocurrencies, which do not meet the UCC’s definition of money or any other UCC property category.\footnote{118} Furthermore, “Article 9 applies to secured transactions, regardless of the form of the transaction. No matter how the parties characterize their transaction, if the substance is a secured transaction in personal property, UCC Article 9 applies.”\footnote{119}

Security interests in general intangibles survive “even after multiple transfers to third parties.”\footnote{120} This presents a significant problem for buyers of cryptocurrencies because there will always be a risk that a bitcoin has been subjected to a perfected security interest by a creditor.\footnote{121} Current versions of cryptocurrencies have no mechanism for knowing when a bitcoin has a lien or other earlier adverse claims.\footnote{122} Consequently, a good faith innocent purchaser of bitcoin has no way to prevent the risk

---

\footnote{114} See Schroeder, supra note 56, at 29–30.
\footnote{115} Id. at 30 (“Article 9 has no negotiation rule for the buyers of general intangibles that are subject to a perfected security interest. That is, once a security interest in a general intangible is perfected, it survives even after multiple transfers to third parties.”).
\footnote{116} See Louis F. Del Duca, The Commercial Law of Bitcoin and Blockchain Transactions, 47 UCC L.J., 1, 8 (2017) (“Article 9 protects innocent transferees of money from an account (a rule intended to facilitate commerce, because otherwise anyone receiving payment might have to first do due diligence on the bank account, which would put considerable friction into commercial transactions.”).
\footnote{117} Schroeder, supra note 56, at 10.
\footnote{118} Id. (“[A]lthough bitcoin proponents would like it to function as currency, it is does not and cannot be made to fit within the U.C.C.’s narrow definition of money. By process of elimination, it falls within the catchall category of ‘general intangibles.’”).
\footnote{119} Del Duca, supra note 116 (citing U.C.C. § 9-109(a) (AM. LAW INST. & UNIF. LAW COMM’N 2013)).
\footnote{120} Schroeder, supra note 56, at 30.
\footnote{122} See Kaminska, supra note 81.
of creditors pursuing claims against them.\textsuperscript{123} And creditors could continue to follow the bitcoin collateral’s transaction trail indefinitely because secured interests in bitcoin persist through multiple transactions—all recorded on the blockchain.\textsuperscript{124} The inability of an intended transferee to effectively perform due diligence on a cryptocurrency transaction hampers the liquidity of these virtual currencies and will slow their adoption for commercial use.\textsuperscript{125}

This is unsatisfactory and unworkable if bitcoin is ever to be widely adopted because it will undoubtedly be used (and is likely currently used) as collateral for debts.\textsuperscript{126} Conveyance rules that favor earlier-in-time owners, relative to later purchasers, place the obligation on those purchasers to inquire as to the title of property. \textit{Caveat emptor} applies even where there is no formal recording system to indicate clean title. But if the earlier ownership interest is never extinguished, under any circumstance, then there must be some mechanism for purchasers to perform a title inquiry. At the time of writing this article, no major cryptocurrency provides such a mechanism;\textsuperscript{127} putting good-faith purchasers—indeed, any purchasers—in an unfairly precarious position regarding acquired bitcoin.

\section*{IV. Cryptocurrencies’ Unfulfilled Potential}

In the United States, the law confusingly treats cryptocurrencies based on the context of their use.

[T]he bitcoin asset itself can be simultaneously classified four separate ways:

\begin{itemize}
\item \footnote{123} Del Duca, \textit{supra} note 116 (“[A]nyone that takes bitcoin may have the risk that the bitcoin is someone's collateral, meaning its possible that the bitcoin will be traced and returned to the creditor.”); Schroeder, \textit{supra} note 56, at 30.
\item \footnote{124} See Kaminska, \textit{supra} note 81 (“[U]nder the United States’ UCC code (uniform commercial code) as long as bitcoins are treated as general intangibles, no high value investor can be sure that an angry Tony Soprano won’t show up one day to claim that the bitcoins they thought they received in a completely unencumbered manner are actually his.”).
\item \footnote{125} See id. (suggesting legislative changes to reduce the friction in commercial bitcoin transactions).
\item \footnote{126} See Lawless, \textit{supra} note 121 (“Up until now, bitcoins have not become a substantial part of mainstream commerce such that the Article 9 problem may have been of little consequence, but if bitcoins are to become part of mainstream commerce, the Article 9 problem must be solved.”); see also Schroeder, \textit{supra} note 56, at 30.
\item \footnote{127} Kaminska, \textit{supra} note 81 (“Bitcoin’s public ledger records a transfer of digital access rights in the eyes of the clearing network. It does not, however, record or see the terms and conditions of that transfer.”).
\end{itemize}
1. “Currency” or “Convertible Portable Currency” as classified by guidance issued by the Financial Crimes Enforcement Network (FinCEN) for the purposes of their regulatory structure and the Bank Secrecy Act (BSA);
2. “Security” by guidance from the SEC;
3. “Commodity” by the US Commodity Futures Trading Commission (CFTC); and
4. “Property” by the Internal Revenue Service (IRS).128

The above classifications are driven by regulators seeking authority over cryptocurrencies within their different spheres of control. Courts have not yet considered the applicability of the bona fide acquisition rule to cryptocurrencies. If courts were to do so, they would likely reach one of three conclusions: (1) cryptocurrencies should be treated like money, and innocent purchasers acquire it free of any prior claims; (2) cryptocurrencies are traceable personal property, and earlier-in-time owners may assert claims against good-faith purchasers; or (3) a creditor has a secured interest in the cryptocurrency at issue, and UCC Article 9 allows the creditor’s claims against innocent purchasers.129

Whether we apply the bona fide acquisition rule to cryptocurrency or not produces an unsatisfactory result for someone: either the first-in-time owners who suffer from crypto-theft or innocent purchasers who acquire in good faith with no notice of wrongdoing. This stems from trying to fit the square peg of digital property into the round hole of a rule designed to address competing interests in physical property.

What makes cryptocurrencies unique is that they are more than just digital property; they are the framework for a complete digital property system. They are a means of storing and exchanging value, paying for goods, and tracking transactions. Bitcoin was created to eliminate intermediaries from transactions and allow owners complete control over their assets.130 But the creators of these new digital property systems did not appreciate that they were creating the perfect target and vehicle for theft: valuable, compact, and portable.131 Owners of cryptocurrencies must

130 See Nakamoto, supra note 23, at 1.
131 See generally Nathaniel Popper, As Bitcoin Bubble Loses Air, Frauds and Flaws Rise to Surface, N.Y. TIMES (Feb. 5, 2018),
take extensive precautions to avoid crypto-theft because stolen cryptocurrency is virtually impossible to recover. These security measures, and the investigation and litigation arising from crypto-theft, add substantial costs to a system that was designed to be as frictionless as possible.132

Cryptocurrency’s strength is its backbone: the blockchain. This public ledger can maintain more information about transactions than cryptocurrencies do currently; it represents unfulfilled potential. Cryptocurrencies could (and should) have built-in mechanisms for flagging transactions subject to liens or adverse claims, including a flag for stolen cryptocurrency. Information costs for due diligence could be negligible; imagine an immediate warning prior to a transaction that the cryptocurrency you are purchasing is secured as collateral or the product of crypto-theft. Cryptocurrencies would need to address how to properly file an interest on assets, how to resolve competing interests, and how to clean title to property. These are problems suited to a programmatic approach, and cryptocurrencies are programs at their core. The title registry and notice rules for real property or security interests could serve as inspiration for systemic improvements, but the blockchain has the potential to be more responsive to problems with digital title and give users active actual notice of transactional irregularities as compared to conventional registry systems.

Cryptocurrencies were designed as a means of digital property ownership free from interference by third-party authorities. Making cryptocurrencies a more fully fleshed-out property system by adding to the functionality of the blockchain would further the private-law goals of these new digital property frameworks. But until cryptocurrencies make better use of the blockchain to avoid and resolve competing claims arising from wrongful transfers, users will continue to pursue satisfaction in sovereign legal systems. Reducing the need for interventional dispute resolution by courts or regulators will result in a more efficient and fair system and work to keep cryptocurrencies free from unnecessary external controls.

[https://perma.cc/RT3V-PKQ3].  
132 See Nakamoto, supra note 23, at 1 (stating that one objective of Bitcoin was reducing transaction costs of a system reliant on trusted intermediaries).
A NORMATIVE APPROACH TO BROADBAND REGULATION: CURBING THE ANTI-COMPETITIVE BEHAVIOR OF INTERNET SERVICE PROVIDERS

Laura Ashley Harris*

CITE AS: 3 GEO. L. TECH. REV. 426 (2019)

I. INTRODUCTION

Policy makers have sought to ensure that Internet access is cost-effective, not unduly discriminatory, and of sufficient quality. To this end, the Federal Communications Commission (FCC) passed the Open Internet Orders and the Restoring Internet Freedom Order. But has the FCC truly succeeded in meeting its goals? This paper argues primarily no. In place of prior regulation, this paper suggests a normative approach in light of antitrust considerations and recommends conduct-focused broadband regulation that addresses these public interest concerns—an approach not unlike the 2015 Open Internet Order. The Open Internet Orders\(^1\) and the Restoring Internet Freedom Order are used as source material to arrive at a recommendation because these orders provide valuable insights into what type of conduct produces performance consistent with the public interest, serving as actual test cases for whether these regulations succeed in the objective of effectively regulating Internet service providers (ISPs).

A new conduct-focused regulation or a reversion back to the 2015 Open Internet Order, on its own, is insufficient to further the public interest. The current statute from which the FCC derives its authority to

---

\(^*\)Georgetown University Law Center, J.D. Candidate 2019; California Polytechnic State University San Luis Obispo, M.S. Engineering with a concentration in Integrated Technology Management, B.S. Industrial Engineering 2013. Thank you to the wonderful editors of GLTR, without whom this piece would not have been possible. Thank you also to Scott Hempling for teaching the class that inspired the work.

\(^1\)Two regulations with similar rules were both coined Open Internet Orders: the Open Internet Order of 2010 and the Open Internet Order of 2015. See infra Section III.B.
regulate ISPs is whittled with conflicting judicial and executive agency interpretations rendering the distinction between information services and telecommunications services, as applied to ISPs, arbitrary. Yet, how to classify broadband—as either an information or telecommunications service—is a critical question because it determines the scope of authority the FCC has to regulate broadband providers. To avoid further political, market, and public confusion as to the classification of ISPs, Congress must first make a policy decision and answer this threshold question.

ISPs are the entities that deliver broadband to consumers. Broadband is a general term that encompasses all services that provide high-speed Internet, but not all Internet services are broadband.\(^2\) Broadband is the most common form of Internet service used in the United States today.\(^3\) This paper focuses on the regulation of broadband providers, also known as ISPs, because net neutrality principles primarily apply to high-speed Internet access; lower-speed Internet providers do not exhibit the same discriminatory behaviors.\(^4\)

First, this paper defines the public interest to establish the purpose of a regulation directing ISP conduct. Second, the paper demonstrates that the current market structure for broadband is not effectively competitive; nor is the current regulatory framework appropriately addressing the conduct of ISPs, leading to the conclusion that the current status quo does not produce performance consistent with the public interest. Finally, the paper recommends that Congress amend the Telecommunications Act of 1996 to provide more explicit guidance on the scope of the FCC’s authority to regulate ISPs and that the FCC pass a new regulation that directs ISP conduct to better serve the public interest.

II. REGULATION IS NECESSARY TO ACHIEVE THE PUBLIC INTEREST IN BROADBAND PERFORMANCE

The public interest in broadband service includes four primary aspects: quality, universality, non-discrimination, and affordability. This interest is derived from the purpose of the Communications Act of 1934 (later revised as the 1996 Telecommunications Act) to “regulate[e] interstate and foreign commerce in communication . . . to all people of the

\(^2\) For example, dial-up is an Internet service, but dial-up is not a broadband service.

\(^3\) For the same reason, the terms Internet Service Providers and Broadband Providers will be used interchangeably.

\(^4\) For example, a dial-up service provider would be hard-pressed to stream videos or significantly prioritize data transmission at all.
United States, without discrimination\(^5\) . . . [and with] a rapid, efficient, Nation-wide . . . communication service with adequate facilities at reasonable charges.”\(^6\)

Historically, the net neutrality debate focused on how to achieve statutory public interest. “Net Neutrality means that [I]nternet service providers should enable access to all content and applications regardless of the source, without favoring or blocking particular products or websites.”\(^7\)

While the debate is not merely two-sided, two primary views have arisen from the most recent FCC broadband orders, the Open Internet Orders and the Restoring Internet Freedom Order, which provide context for understanding some of the most common concerns with broadband regulation. On one side, supporters of “net neutrality” hold that an open Internet—meaning, free from blocking, throttling, and paid prioritization—stimulates economic growth by removing barriers to entry\(^8\) and preventing or penalizing unduly discriminatory behavior.\(^9\)

The opposing position believes regulation of ISPs is “unnecessary”\(^10\) and that

---

\(^5\) Telecommunications Act of 1996, 47 U.S.C. 151. Under the purposes of the Act, discrimination is prohibited “on the basis of race, color, religion, national origin, or sex . . . .” Further into the Act, under § 202, discrimination is defined even more broadly in the following way:

(a) It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service, directly or indirectly, by any means or device, or to make or give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage (emphasis added).

\(^6\) Id.

\(^7\) Net Neutrality is an ambiguous term and is extremely broad. In this paper, Net Neutrality will adhere to the definition provided by Fergus O’Sullivan, *What Is Net Neutrality and Why Is It Important?*, CLOUDWARDS (Mar. 7, 2018), [https://www.cloudwards.net/net-neutrality/][https://perma.cc/56UM-BHD5].


the removal of “heavy-handed” regulations will lead to “a free and open Internet, and Americans will have access to better, faster, and cheaper broadband.”

These two positions represent two different viewpoints on how to achieve the public interest. But before deciding how to regulate an industry’s actors, the question of whether to regulate must be answered by considering the market structure and the desired conduct of the market participants. In other words, regulation is necessary to the extent that the “deregulated markets are likely to fail [to achieve performance consistent with the public interest] even in the presence of reasonably strict antitrust enforcement.”

III. THE STATUS QUO IS NOT PRODUCING PERFORMANCE CONSISTENT WITH THE PUBLIC INTEREST

Effective regulation is intended to “align private behavior with the public interest.” The structure of the broadband market and current regulations promote certain private interests, rather than the public interests described in Part I. ISPs do not behave consistently with the public interest because (A) absent regulation, broadband’s anti-competitive market structure encourages ISPs to pursue private interests and (B) the current broadband regulation does not promote conduct consistent with the public interest.

A. Unregulated, the Broadband Market Promotes Anti-Competitive Conduct

“Effective competition describes a market structure where the sellers and buyers lack ‘market power.’” Market power is the “power to control prices and exclude competition.” Because ISPs operate as either a

Freedom Initiative] (explaining the FCC’s reasoning for the Restoring Internet Freedom Order).

11 Id. (quoting FCC Chairman Ajit Pai).
12 See HEMPLING, supra note 9, at 120–22.
14 HEMPLING, supra note 9, at 3.
15 Id. at 120.
monopoly or an oligopoly depending on the region, the market is not effectively competitive. Thus, these ISPs have market power that allows them to partake in conduct inconsistent with the public interest.

1. The Broadband Market Structure Is Not Effectively Competitive

Historically, Internet technologies evolved out of telecommunications technologies, giving telephone and cable companies an advantage in market participation as incumbents because they owned the underlying infrastructure required for Internet access. This incumbency initiated the monopolistic broadband market, giving consumers limited options to choose between ISPs. Additionally, high infrastructure costs for new Internet technologies create barriers to entry, limiting the ability for new market participants to provide effective competition.

To understand why the broadband market is not effectively competitive, this paper first defines the market participants and the underlying technologies of broadband. The market consists of four participants: backbone networks, broadband providers, edge providers, and end users. Backbone networks are the physical infrastructure of the Internet, including fiber optics, copper wiring, and routers that enable the transmission of large amounts of data. Broadband providers “are the businesses and organizations that provide users with Internet access and related services.” Edge providers, also known as content providers, are

17 HEMPLING, supra note 9, at 11.
18 See id. (“Market structure, describes (a) the geographic area in which transactions occur; (b) the products and services being sold in the geographic area; (c) the characteristic and market shares of the sellers and buyers of those products and services in the geographic area; and (d) the entry costs and entry barriers.”).
19 See Kate Cox, Why Starting a Competitor to Comcast is Basically Impossible, CONSUMERIST (May 10, 2014), https://consumerist.com/2014/05/10/why-starting-a-competitor-to-comcast-is-basically-impossible/ [https://perma.cc/E6JK-MJYW] (discussing how regulatory history in the broadband market has created barriers to entry for new market participants, leaving consumers with limited choices between ISPs).
20 Id.
entities that “provide content, services and applications over the Internet.”

End users are individuals or entities that “consume [or use] the content, services, and applications.” In some circumstances, participants may fall into more than one category. For example, a blogger may be both an end user and an edge provider because he or she uses the applications on the Internet while providing content to the Internet. Data travels across the backbone of the Internet through an ISP from an edge provider or end user to other users by breaking down the “messages . . . into ‘packets’ . . . and . . . reassemble[ing]” them on the other side.

Broadband is available through a number of different technologies: cable modem, digital subscriber line (DSL), fiber-to-the-home (FTTH), and wireless satellite services. DSL started using the existing telephone wiring to homes to deliver broadband service in the early 1990s. Cable-modem is delivered to homes mostly on hybrid fiber coax (HFC) cables which is in turn delivered to neighborhood nodes using existing cable networks. FTTH does not rely on existing in-home connections. Instead, FTTH requires a provider to complete the “last-mile” infrastructure from the Internet backbone to each individual home using a fiber optic cable.

Existing public utilities had fewer barriers to entry because

24 Verizon, 740 F.3d at 629.
25 Id.
28 Id. (noting that DSL and FTTH are typically provided by local telephone companies; a primary difference between DSL and FTTH is the underlying technology, which allows FTTH “virtually unlimited bandwidth” by running fiber directly to a customer’s home).
29 Id. at 77 (indicating that wireless services typically offer lower speeds than wired connections but allow for greater mobility and greater access to Internet services where wired connections may be unavailable, such as in rural areas).
32 The speed across each type of service varies based on the underlying technology. For example, wireless, typically the slowest form of broadband, is delivered over airwaves; DSL and cable are delivered over copper wiring; and fiber is delivered by transmitting light over fiber-optic cables. See Anderson, supra note 31.
they owned the underlying Internet infrastructure. Because the technology behind high-speed Internet relies on telephone and cable lines, the companies that owned this infrastructure for these existing technologies were functionally incumbents with fewer barriers to entering the broadband market. Absent regulation requiring ISPs to share the underlying infrastructure, the high infrastructure cost of laying new cable or telephone lines creates barriers to entry for potential new broadband providers.

High infrastructure costs create barriers to entry. While DSL and cable were enabled through the existing infrastructure of telephone and cable, FTTH does not have a complete built-in infrastructure. Exorbitant costs for completing the FTTH infrastructure across the U.S. creates barriers to entry that few entities can risk investment in, as evidenced by two of the primary providers competing in this market—Verizon and Google. For example, analysts estimate the cost of Google Fiber’s nationwide expansion plan to be $3,000–$8,000 per home. With 127.59 million households in the United States, the total cost of installation would equate to a $378,660,000,000 infrastructure investment.

There is no meaningful choice for consumers to choose between ISPs. The lack of competition between ISPs in a particular

---

33 Cox, supra note 19.
34 FCC, 2016 BROADBAND PROGRESS REPORT 12 (Jan. 29, 2016), https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report [https://perma.cc/KW3B-B354] (finding, from a 2016 survey, that 88% of people in the U.S. who have broadband subscribe to DSL or Cable-Modem). The report found that fifty-nine percent of broadband subscriptions are cable-modem (Id. at para 26), and twenty-nine percent of subscriptions are DSL (Id. at 12, n.79).
35 Cox, supra note 19.
36 Anderson, supra note 31.
38 This estimate and analysis assumes that no household today has FTTH and that one entity would be responsible for the entire investment of connecting all U.S. households. Neither assumption is likely, but the extrapolation of cost demonstrates the extreme investment required to connect each home across the U.S. Even assuming that half of the homes in the United States have fiber, fiber rollout to the remaining half would nonetheless be a multi-billion dollar investment.
geographic area leaves consumers with no meaningful opportunity to choose between broadband providers, giving ISPs more market power to control prices and to unduly discriminate. In 2015, only twenty-two percent of households had an option between two or more ISPs with a 25Mbps download speed and a 3Mbps upload speed. Two years later, using FCC data, a survey “found that 129 million Americans only have one option for broadband internet service in their area, which equals about 40 percent of the country.” As one article ironically states, “You can pick any ISP you want . . . as long as it’s Comcast.”

Where barriers to entry limit the number of retail providers of broadband to one or two sellers, these sellers have less incentive to act in the public interest. Instead, broadband providers have more incentive to act in an anti-competitive manner and/or exclude new competitors from the broadband market. Such behavior is prominent where the public interest is in tension with the private interests of ISPs, edge providers, and

---

40 The geographic area for a particular set of consumers is defined by the area served by sellers that are accessible to those consumers.
41 Le, supra note 39 (finding that ISPs “make an estimated 97 cents in profit for every dollar they charge”).
42 HEMPLING, supra note 9, at 288 (“Undue discrimination includes rate differences not justified by cost differences and rate differences with anti-competitive effect.”).
end users. The proposal outlined in Section IV seeks to account for the inherent conflict of interests present as a result of this market structure.

2. **Given the Non-Competitive Market Structure for Broadband Service, Unregulated ISP Conduct Does Not Produce Public Interest Performance**

ISPs have historically participated in conduct that does not conform to the public interest. As explained above, this conduct is not a shocking conclusion given the significant market power ISPs hold. The public interest—defined as a universal, high-quality, not-unduly-discriminatory Internet service available to consumers at a reasonable cost—requires a competitive broadband market. A competitive market would create incentives for ISPs to conform to the public interest because unsatisfied customers would have the ability to shop for a service that most closely conforms to their wants and needs.

The most commonly discussed and desired aspects of ISP conduct—at least by proponents of net neutrality—are transparent operations, no blocking, and no throttling. Absent regulation, ISPs have demonstrated their ability and intent to engage in behaviors antithetical to these goals. Transparency is the requirement that ISPs disclose their behavior towards end users thereby giving consumers the knowledge necessary to make a meaningful choice in selecting an ISP. Yet, transparency is only an effective tool to promote competition when users

---


Any person providing broadband internet access service shall publicly disclose accurate information regarding the network management practices, performance characteristics, and commercial terms of its broadband internet access services sufficient to enable consumers to make informed choices regarding the purchase and use of such services and entrepreneurs and other small businesses to develop, market, and maintain internet offerings. Such disclosure shall be made via a publicly available, easily accessible website or through transmittal to the Commission.
already have a meaningful choice between services.\textsuperscript{48} As previously discussed, consumers lack this meaningful choice.

Blocking is any means of preventing end user access to legal content, applications, services, or non-harmful devices.\textsuperscript{49} Throttling means degrading or impairing access to lawful Internet traffic based on its content, application, service, users, or use of a non-harmful device.\textsuperscript{50} For example, in 2008 Comcast was sued both for throttling and blocking.\textsuperscript{51} The Electronic Frontier Foundation and the Associated Press independently found that Comcast interfered with the Internet traffic from BitTorrent and Gnutella.\textsuperscript{52} In this case, Comcast took specific steps to prioritize—or conversely, discriminate against—certain types of content when it degraded the Internet protocols used to deliver this traffic. Around the same time, Comcast was also sued in a class action for blocking certain traffic in peer-to-peer (P2P) file transfers.\textsuperscript{53} Further, certain ISPs

\textsuperscript{48} Gulf States Util. Co. v. La. Pub. Serv. Comm’n, 578 So. 2d 71, 85, n.6 (La. 1991) (quoting In Re Long Island Lighting Co., 71 P.U.R. 4th 262, 1985 WL 258217 (N.Y. Pub. Serv. Comm’n 1985)) (“If a competitive enterprise tried to impose on its customers costs from imprudent actions, the customers could take their business to a more efficient provider. A utility’s ratepayers have no such choice. A utility’s motivation to act prudently arises from the prospect that imprudent costs may be disallowed.”).


\textsuperscript{50} Id.

\textsuperscript{51} Press Release, FCC, Commission Orders Comcast to End Discriminatory Network Management Practices, FCC (Aug. 1, 2008), https://www.fcc.gov/document/commission-orders-comcast-end-discriminatory-network-management [https://perma.cc/WC7Y-FUWA] (“[T]he Commission concluded that Comcast has unduly interfered with Internet users’ right to access the lawful Internet content and to use the applications of their choice.”). While more recent examples of ISP’s discriminatory behavior has occurred, this pre-2010 Open Internet Order example demonstrates an ISPs ability and incentive to act in a manner contrary to the public interest. While an ISP’s private interest to discriminate does not change with new regulations, their incentive to discriminate may be curtailed by an appropriate regulation that holds them accountable for such discriminatory acts.


have expressed their intent to promote pay-to-play prioritization and promote data limits on users.\(^\text{54}\)

This conduct by ISPs runs counter to the identified public interest identified above. For example, when information online becomes more or less accessible due to throttling or is not accessible at all due to blocking, the quality of the user’s experiences is impacted. Additionally, the prohibition against undue discrimination\(^\text{55}\) was violated in the BitTorrent example when ISPs, without reasonable justification, throttled data arbitrarily favoring some Internet traffic over others.

In a competitive market, engaging in these activities may offend customers, and customers may leave behind the services that they are unsatisfied with. But because broadband is not a competitive market and ISPs’ unregulated conduct conflicts with the public interest, a regulation is “necessary to align private behavior with the public interest.”\(^\text{56}\)

B. Regulations Directed at ISPs Fail to Curb Anti-Competitive Conduct.

The Telecommunications Act of 1996 attempted to address technological advances in the telecommunications industry,\(^\text{57}\) and subsequent regulations have attempted to appropriately regulate ISP behavior in accordance with the public interest. However, the FCC’s interpretation of this statute has proven problematic. Instead of one consistent position, the FCC has routinely flip-flopped its categorization of Internet service between an “information service” and a “telecommunication service”—services that have completely different statutory obligations and different statutory limitations. By continually redefining its stance across various regulations in such a stark way, the FCC’s regulation of ISPs has become inconsistent and unpredictable. Furthermore, the current regulation is ineffective because it does not promote behavior consistent with the public interest. Thus, the current


\(^{55}\) HEMPLING, supra note 9, at 288 (“Discrimination can be lawful or unlawful, depending on whether it is ‘due’ or ‘undue.’”).

\(^{56}\) Id. at 3.

\(^{57}\) See ECONOMIDES, supra note 13, at 48. The “dot-com boom” represented a time in the mid 1990s to early 2000s, which saw a dramatic increase in the use of the Internet, bringing the Internet into an era where Internet access is both vital to the U.S. economy and to individuals in order to participate in the economy. This dependence is the reason universal access is necessary to the public interest.
regulation is both administratively improper, in that it is arbitrary, and practically unsuccessful, in that it fails to properly support the public interest.

1. The FCC’s Statutory Authority for Regulating Broadband Is Impermissibly Vague.

The statutory grant of authority to regulate ISPs grew out of the authority to regulate telecommunications services. The Telecommunications Act of 1996 hoped “to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.” To carry out this goal, the 1996 Act created two categories of services: telecommunication services and information services. The classification of broadband as either an information or telecommunication service has now become a central question as to what regulatory authority the FCC has over ISPs because it determines what and how much authority the FCC has to impose obligations on broadband providers.

Telecommunication services, but not information services, may be subject to Title II common carrier requirements. Title II grants the FCC authority to impose, among other things, obligations on common carriers “to interconnect with other carriers and to establish through-routes,” to charge “just and reasonable” prices for all services and products in

---

59 Id.; see also U.S. H. COMM. ON ENERGY AND COMMERCE, MODERNIZING THE COMMUNICATIONS ACT 1 (2014), http://www.npsti.org/download.jsp?tableId=37&column=217&id=2917&file=Communications_ActorWhite_Paper_140108.pdf [https://perma.cc/G4U3-QRDH] [hereinafter MODERNIZING THE COMMUNICATIONS ACT WHITE PAPER] (stating that the Act was intended to increase competition, reduce regulatory barriers, and advance information services technologies).
60 A common carrier is “any person engaged as a common carrier for hire, in interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this Act; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier.” 47 U.S.C. § 153(11) (2012).
connection with communication services,\textsuperscript{62} to avoid “unjust and unreasonable” discrimination,\textsuperscript{63} and to “keep itself informed as to the manner and method” of business management and the “technical developments and improvements.”\textsuperscript{64}

Conversely, the FCC has substantially less authority to impose obligations on providers of information services.\textsuperscript{65} According to the D.C. Circuit, the FCC has only “ancillary” jurisdiction to regulate information services under the broad language of the 1996 Act, which states “[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this Act, as may be necessary in the execution of its function.”\textsuperscript{66} But this authority does not permit the FCC to subject information services to common carrier obligations. Instead, § 706(a) and (b) of the Telecommunications Act “grant[s] the Commission affirmative authority to promulgate rules governing broadband providers.”\textsuperscript{67} Such rules must be tailored to the “specific statutory goal of accelerating broadband deployment”\textsuperscript{68} and should “encourage the deployment . . . of advanced telecommunications capability to all Americans . . . by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market or other regulating methods that remove barriers to infrastructure investment.”\textsuperscript{69}

Thus, the determination of whether broadband is an “information service” or a “telecommunications service” is central to crafting a regulation directing the conduct of ISPs. Given that this first assessment controls what the regulation may permissibly authorize and dictate, it is impractical to design a regulation without first establishing what type of service broadband constitutes. Yet, the FCC has repeatedly switched\textsuperscript{70} its

\textsuperscript{62} 47 U.S.C. § 201(b).
\textsuperscript{63} Id. § 202(a).
\textsuperscript{64} Id. § 218.
\textsuperscript{65} See MODERNIZING THE COMMUNICATIONS ACT WHITE PAPER, supra note 59, at 2.
\textsuperscript{66} Verizon v. FCC, 740 F.3d 623, 632 (D.C. Cir. 2014) (citing 47 U.S.C. § 154(i)).
\textsuperscript{67} Id. at 642.
\textsuperscript{68} Id. at 641.
\textsuperscript{69} 47 U.S.C. § 1302(a) (also referred to as § 706(a)). Section 706(d) defines “advanced telecommunication capabilities” as “high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.” Id. § 1302(d)(1) (also referred to as § 706(d)).
\textsuperscript{70} Under the Computer II regime, the FCC classified Internet, delivered over telephone lines, as a basic service subject to Title II common carrier requirements. The passing of
answer to this threshold question, causing dramatically different policy and regulatory results.

a. The Classification of Broadband Is Ambiguous and Unpredictable

The FCC’s inability to decide on how to classify broadband service has created a legal fiction as to what type of service broadband actually is, highlighting the ambiguous nature of the statute. With each reclassification, the FCC’s authority to regulate ISPs changes overnight. Many judges and scholars have discussed ambiguous statutes as fundamentally flawed. That is, the ambiguous nature of a statute—paired with Chevron deference—grants an agency like the FCC an incredible

the Telecommunication Act of 1996 replaced the basic and enhanced service distinction with information service and telecommunication service distinction. Just like basic services were subject to Title II requirements, so too are telecommunications services under the new statute. After its enactment, the FCC classified DSL as a telecommunication service. But a “DSL provider could exempt its Internet access services . . . from Title II,” if, and only if, the provider operated the service in “a separate affiliate.” Verizon, 740 F.3d at 629–32. A few years later the FCC determined that cable broadband providers were entirely exempt from Title II. Then, in 2015, the FCC reclassified ISPs as telecommunications services, subject to Title II. Finally, in 2018, the FCC repealed this determination and re-categorized ISPs as an information service.

In the early years of broadband regulation, the FCC concluded that a “DSL provider could exempt its Internet access services . . . from Title II,” but only if the provider operated the service in “a separate affiliate.” Verizon, 740 F.3d at 631. A few years later the FCC determined that cable broadband providers were entirely exempt from Title II. Id. Then, in 2015 the FCC re-classified broadband as a telecommunication service subject to Title II. Finally, in 2018, the FCC repealed this determination and re-categorized ISPs as an information service.

See James Tuthill, FCC Throws in Towel, But Public Has Right to Know Why, BERKELEY L. (Feb. 25, 2014), https://www.law.berkeley.edu/article/fcc-throws-in-towel-but-public-has-right-to-know-why/ [https://perma.cc/Y8LR-MXX7] (stating that the FCC’s refusal to appeal a judgment by the court left the authority of the FCC to police the internet with the court or providers).


See generally Christopher J. Walker, Attacking Auer and Chevron Deference: A Literature Review, 16 GEO. J.L. & PUB. POL’y 103, 112–13 (2018); BRANNON & COLE, supra note 73.
amount of discretionary authority. Some judges have voiced concern with the amount of deference afforded to agencies when interpreting ambiguous statutory text. For example, Supreme Court Justice Neil Gorsuch explained, “[p]ermitting an agency to issue and reverse regulations affecting large aspects of the economy, including its own jurisdiction to regulate at all, may not satisfy the ‘intelligible principle’ test set forth by the Supreme Court in delegation cases.”\textsuperscript{75} Supreme Court Justice Clarence Thomas has similarly warned of the of “extremely permissive” deference:

Perhaps there is some unique historical justification for deferring to federal agencies . . . but these cases reveal how paltry an effort we have made to understand it or to confine ourselves to its boundaries. Although we hold today that [the agency] exceeded even the extremely permissive limits on agency power set by our precedents, we should be alarmed that it felt sufficiently emboldened by those precedents to make the bid for deference that it did here. As in other areas of our jurisprudence concerning administrative agencies . . . we seem to be straying further and further from the Constitution without so much as pausing to ask why.\textsuperscript{76}

In other words, a statute that permits this much discretion to an agency is problematic because it allows the political agenda of a given administration to produce entirely different regulations.

Additionally, the ability to re-classify broadband so easily creates confusion among the public as to what, if any, rights they have. And it leads to confusion among ISPs as to their obligations. Furthermore, this wavering is a waste of the judicial and executive resources needed with each overhaul of the broadband regulation and the subsequent litigation. It is unreasonable and inefficient for a statute to be so malleable that ISPs and consumers must adjust their expectations based on political expectations. “Simply calling a rose by another name will not change what it is.”\textsuperscript{77}

\textsuperscript{75} BRANNON & COLE, supra note 73.
\textsuperscript{77} Tuthill, supra note 72.
b. Chevron Deference Should Not Be Granted

At the heart of this inquiry also lies the application of *Chevron* deference. *Chevron* deference requires courts to defer to an agency's reasonable interpretation of an ambiguous statute.78 A statutory interpretation is unreasonable when the agency's interpretation is "arbitrary, capricious, or manifestly contrary to the statute" in question.79 Normally, an agency rule would be arbitrary and capricious "if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise."80 In other words, "if th[e] choice represents a reasonable accommodation of conflicting policies that were committed to the agency's care by the statute, we should not disturb it unless it appears from the statute or its legislative history that the accommodation is not one that Congress would have sanctioned."81

While the Supreme Court has stated, "*Chevron* allows agencies to choose among competing reasonable interpretations of a statute,"82 a reasonable interpretation should not result in diametrically different authority based on who does the interpretation. Proponents of applying *Chevron* deference to the FCC interpretation of the Telecommunications Act of 1996 will likely classify the dispute of how to classify broadband as a policy choice. "When a challenge to an agency construction of a statutory provision, fairly conceptualized, really centers on the wisdom of the agency's policy, rather than whether it is a reasonable choice within a gap left open by Congress, the challenge must fail."83 But even if the classification of broadband as an information or telecommunication service is a policy choice, and while multiple interpretations may be

---

79 *Chevron*, 467 U.S. at 844.
81 *Chevron*, 467 U.S. at 845.
83 *Chevron*, 467 U.S. at 866.
reasonable, to find reasonableness the statute must support the agency’s interpretation. But, how can a statute reasonably be read to redefine the scope of the FCC’s own authority? When the choice for interpretation is binary—e.g., an information service or a telecommunications service—and the resulting choice alters the agency’s scope of authority to nearly opposite conclusions, both interpretations should not be reasonable. Justice Kennedy notes these concerns regarding reflexive judicial deference in *Pereira v. Sessions*, stating “when deference is applied to . . . questions of statutory interpretation, such as an agency's interpretation of the statutory provisions that concern the scope of its own authority . . . is more troubling still.”

*Chevron* requires judicial deference to an agency’s interpretation of a statute when Congress has not “directly addressed the precise question at issue” and “the statute is silent or ambiguous with respect to the specific issue.” However, in *King v. Burwell*, Chief Justice Roberts articulated an exception to *Chevron* deference for questions of deep “economic and political significance.” As more than one source has suspected, “[c]ertainly there is a good argument, a la *King*, that a case involving utility-like regulation of Internet providers is one of deep economic and political significance that should be decided without resort to *Chevron* deference . . . .” In other words, because ISP regulation has become a partisan issue and because the Internet supports large parts of the economy through online commerce, the ISP regulation is a question of deep economic and political significance. Thus, *Chevron* deference should not apply to the FCC’s interpretation of the Act. In this circumstance, the determination of how to interpret the 1996 Telecommunications Act—

---

85 *Chevron*, 467 U.S. at 843.
88 Petitioner Brief for Writ of Certiorari at i, Berninger v. FCC, 139 S. Ct. 453, (Nov. 5, 2018) (No. 17–498) (cert. denied) (listing question #2 for the court as “[i]s the radical reinterpretation of the Act by the Commission entitled to deference under *Chevron* . . . .”).
specifically, whether broadband is a telecommunications service or an information service—should be left to Congress because in this unique set of circumstances, not only has the FCC flip-flopped in its classification of broadband, the court has as well. In *Verizon*, the court stated, albeit in dicta, “[w]e think it obvious that the Commission would violate the Communications Act were it to regulate broadband providers as common carriers.” Yet, less than a year later, the FCC did exactly that in the 2015 *Open Internet Order*, demonstrating a clear disregard for the court’s interpretation of the statute. More confusing still, the D.C. Circuit later upheld the FCC’s classification of broadband as a telecommunication service subject to common carrier rules—contrary to their prior assertion. Given that the FCC’s interpretation of the statute has been inconsistent, that the court’s view of a reasonable interpretation has been inconsistent, and that the D.C. Circuit has both sometimes overruled and sometimes upheld the FCC’s interpretation—all in the last five years—these political branches have demonstrated an inability to agree on the appropriate scope of FCC authority to regulate broadband providers. “When the political branches disagree with a judicial interpretation of existing law, the Constitution prescribes the appropriate remedial process. It's called legislation.”

2. The FCC’s Recent Attempts at Regulating Broadband Service Have Not Provided Adequate Rules to Discourage Improper ISP Conduct Counter to the Public Interest.

The two most recent FCC regulations are exemplary of the FCC’s inconsistent position on broadband classification. These regulations, the

---

90 The D.C. Circuit did, however, later accept the FCC re-classification of broadband as a telecommunication services, subject to common carrier rules in *U.S. Telecom Ass’n v. FCC*, 825 F.3d 674, 710–11 (D.C. Cir. 2016), demonstrating the court’s own inconsistency.
91 *Id.* at 689.
92 Compare *Open Internet Order of 2015* with *Restoring Internet Freedom Order* (declaring that broadband is a telecommunications service under the 2015 Order but then re-defining it as an information service under the Restoring Internet Freedom Order).
93 Compare *Verizon*, 740 F.3d at 650 with *U.S. Telecom Ass’n*, 825 F.3d at 689 (deferring to the FCC’s interpretation of broadband as an information service in *Verizon*, while conversely, deferring to the FCC’s interpretation of broadband as a telecommunications service under *U.S. Telecom Ass’n*).
94 *Gutierrez-Brizuela v. Lynch*, 834 F.3d 1142, 1151 (10th Cir. 2016) (Gorsuch, J., concurring).
2015 Open Internet Order and the Restoring Internet Freedom Order, take opposing views on which type of service broadband is. This difference in classification has resulted in vastly different obligations on ISPs under each Order.

a. Open Internet Orders

The Open Internet Orders provide a case study on the limits of regulating broadband both as an information and telecommunication service because two different versions of the Order, with substantially similar rules, were adopted, each treating broadband as a different type of service. The 2010 Open Internet Order first classified broadband as an information service. The FCC then re-classified broadband as a telecommunication service in the 2015 Open Internet Order, permitting ISPs to be treated as Title II common carriers.

The 2010 Open Internet Order consists of four main requirements for ISPs: transparency, no unreasonable discrimination, no blocking, and reasonable network management. Transparency requires ISPs to clearly “disclose accurate information regarding the network management practices, performance, and commercial terms of [their] broadband Internet access services.” The anti-discrimination provision states that ISPs “shall not unreasonably discriminate in transmitting lawful network traffic.” The anti-blocking requirement prohibits the “block[ing] of lawful content, applications, services, or non-harmful devices, subject to reasonable network management.”

Verizon v. FCC vacated the anti-blocking and anti-discrimination rules of the 2010 Open Internet Order because the Order “subject[ed] broadband providers to common carrier treatment,” while broadband was still classified as an information service. In response, the FCC re-

---

97 Evolution of the FCC’s Open Internet, supra note 71.
99 Id. at 17944 ¶ 68.
100 Id. at 17942 ¶ 63. “A network management practice is reasonable if it is appropriate and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service.” Id. at 17952 ¶ 82.
classified broadband as a telecommunication service subject to Title II in the 2015 Open Internet Order and re-draft the rules prohibiting blocking and throttling. The 2015 Order also added a new prohibition against paid prioritization. The new paid prioritization rule meant that edge providers could not pay for a “fast lane” allowing an ISP to favor some traffic from some sources over others. The transparency and reasonable network management practices remained intact. Thus, merely by re-classifying broadband as a telecommunication service, the FCC was able to re-instate the conduct-focused rules of the 2010 Order that had been previously vacated as beyond the statutory authority of the FCC when broadband was classified as an information service.

Relying on Chevron deference, the D.C. Circuit upheld the FCC’s interpretation of the Telecommunications Act as allowing broadband to be classified as a telecommunication services. The Supreme Court denied the petition for certiorari in 2018 because the promulgation of the 2018 Restoring Internet Freedom Order rendered the case moot. Thus, whether the FCC’s interpretation of the Telecommunications Act of 1996 in light of Chevron deference was proper may still be in question.

Regardless of the service classification, both versions of the Open Internet Order are problematic because they appear facially over-broad, while at the same time, they are actually under-inclusive, allowing loopholes for behavior that should be curtailed and making it difficult for ISPs to achieve conduct consistent with the rules. The rules for blocking and throttling purport to create sweeping prohibitions against ISPs, while including within each rule an escape hatch—an exception for reasonable network management. The no paid prioritization rule from the 2015 Open Internet Order is not subject to this exception and may actually be overbroad.

This exception allows ISPs to excuse harmful behavior through the reasonable network management loophole. A network management practice is a practice that has a primarily technical network management justification but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into

---

102 Evolution of the FCC’s Open Internet, supra note 71.
103 U.S. Telecom Ass’n v. FCC, 825 F. 3d 674, 710–11 (D.C. Cir. 2016).
104 U.S. Telecom Ass’n v. FCC, 139 S. Ct. 475 (2018) (Mem.).
106 See infra Section IV.B.3.b.
account the particular network architecture and technology of the broadband Internet access service.\textsuperscript{107}

One example of the reasonable network management loophole is zero-rating. Zero-rating is the idea that ISPs can select which applications and/or websites count towards data-caps.\textsuperscript{108} While ISPs likely select applications and websites for zero-rating to enhance user experience, other applications of zero-rating may be harmful or anticompetitive, such as when Comcast included their own “Stream TV” service in the zero-rating but excluded Netflix and Youtube.\textsuperscript{109} In both cases, the selection of what is zero-rated and what is not is arbitrary from a technical perspective because how the packets of data are delivered between users does not change based on whether a particular packet counts towards the data cap or not. However, it is not arbitrary from an economic perspective for the ISP that chooses to promote their own services. Yet, an ISP may, and has, argued that both practices are permissible, presumably as a reasonable network management practice.\textsuperscript{110}

Another example demonstrates that the reasonable network management exception to treat data differently in order “to protect [ISP] networks from malicious content and to relieve congestion”\textsuperscript{111} may impose degradations of security. The Broadband Internet Technical Advisory Group reported, “Security of traffic has at times been downgraded to facilitate differentiation techniques.”\textsuperscript{112} But when security

\begin{thebibliography}{9}
\bibitem{108} Devin Coldewey, \textit{WTF Is Zero-Rating}, TECH CRUNCH (Apr. 16, 2017), https://techcrunch.com/2017/04/16/wtf-is-zero-rating/ \[https://perma.cc/K7RF-T8PL\] (Zero rating works by allowing ISPs to choose which packets of data count towards data caps, then when these packets of data are sent/received, the packet of data is either entered onto a ledger towards the user’s data cap or not.).
\bibitem{109} \textit{Id.}
\bibitem{110} Comcast’s argument appears to be “other services came over the cable-powered internet, while Stream TV came over the internet-powered cable.” \textit{Id.} An argument that is skeptical at best.
\bibitem{111} FCC Protecting and Promoting the Open Internet, 80 Fed. Reg. 19738, 19833 (Apr. 13, 2015).
\bibitem{112} TECHNICAL WORKING GROUP, BROADBAND INTERNET TECHNICAL ADVISORY GROUP, \textit{DIFFERENTIATED TREATMENT OF INTERNET TRAFFIC} 29 (October 2015), https://www.bitag.org/documents/BITAG_Differentiated_Treatment_of_Internet_Traffic.pdf \[https://perma.cc/YU6Z-ADJJ\]; see also \textit{id.} at 8-9 (Differentiated treatment of network traffic is a two-part process: (1) traffic is classified into traffic streams, and (2) a prescribed set of actions is applied to each stream. . . . Traffic classification can be performed in most layers of the network model, though the available classification elements differ at each layer.).
\end{thebibliography}
conflicts with efficiency, a person’s, or an ISP’s, interpretation on which reasonable network management practice should prevail—efficiency or security—may and likely will differ.

Admittedly, it is not practical to draw out every exception for “reasonable networking management” practices in a regulation—especially, given the rapidly-changing nature of the Internet and the possibility that articulating a very specific set of rules would allow ISPs to sidestep regulations in another manner by crafting and performing other discriminatory behavior not articulated in what would become a compliance checklist. Yet, drafting more precise language will allow ISPs to have more control over their network management practices and will provide more clarity on what types of network management practices are “unreasonable.”

b. Restoring Internet Freedom Order

In June 2018, not long after the Trump Administration took Office, the FCC once again classified broadband as an information service in the Restoring Internet Freedom Order. This order removed all of the conduct-focused rules of the Open Internet Order except for the transparency requirement. The FCC promoted the Restoring Internet Freedom Order as a “framework for an open Internet, while paving the way for better, faster, and cheaper Internet access for consumers” and determined these goals can be achieved by focusing on consumer protection, transparency, and the removal of unnecessary regulations. Each of these three mechanisms is problematic to achieving conduct consistent with the public interest.

113 For example, ViaSat decrypted data to optimize performance and Gogo InFlight Internet “forged TLS certificates in order to shape traffic or block high-bandwidth uses.” Id. at 27.
115 In fact, the conduct-focused rules are not permissible under the Restoring Internet Order because, as Verizon v. FCC explained, while broadband is classified as an information service, the “specific rules imposed by the Open Internet Order fall outside the scope [of the ancillary authority of § 706(a) and (b).” Verizon v. FCC, 740 F.3d 623, 642 (D.C. Cir. 2014). In other words, while classified as an information service, the FCC may not impose the conduct-specific rules of the 2010 and 2015 orders; it is first necessary to classify broadband as a telecommunication to re-impose the conduct-specific rules. This demonstrates the difference between the scope of authority under Title II and under § 706.
117 Id.
First, to achieve consumer protection, the FCC abdicated its authority and purported to return oversight over broadband providers to the Federal Trade Commission (FTC) authority to “police and take action against Internet Service Providers for anticompetitive acts or unfair and deceptive practices.”\textsuperscript{118} This grant of authority is problematic because “FTC enforcement processes are by nature reactive and can take years.”\textsuperscript{119} Further, enforcement of § 5 of the FTCA,\textsuperscript{120} from which the FTC derives its authority to police unfair and deceptive acts, is rare.\textsuperscript{121} The likely result of repealing the proactive preemptive rules of the \textit{Open Internet Orders}, in exchange for the reactive enforcement authority granted to the FTC, is less consumer protection.\textsuperscript{122}

Second, the removal of “heavy-handed regulations,”\textsuperscript{123} including the removal of the anti-blocking, anti-throttling, and no paid prioritization rules, is problematic because it returns the regulation of ISPs to the status quo discussed in Section III.A above. The return to the status quo would lead to ISP conduct inconsistent with the public interest, given the anti-competitive nature of ISP conduct in the broadband market. The FCC premises the need for de-regulation on a desire to promote investment in high-speed networks.\textsuperscript{124} Increased investment has the potential to increase access to broadband, supporting the universality element of the public interest, and innovation, which furthers the quality and cost-effectiveness elements of public interest. The FCC argues that investment decreased by 5.6\% under the \textit{Open Internet Order},\textsuperscript{125} but this data is actually inconclusive. The FCC relies on a report for this finding that actually determines that investment may have increased by up to 5.3\% or decreased by as much as 5.6\%, depending on how the underlying data is

\textsuperscript{118} Id.
\textsuperscript{121} William E. Kovacic & Marc Winerman, \textit{Competition Policy and the Application of Section 5 of the Federal Trade Commission Act}, 76 ANTITRUST L.J. 929, 933–34 (2010) (“One would be hard-pressed to come up with a list of ten adjudicated decisions that involved the FTC’s application of § 5 in which the FTC prevailed and the case can be said to have had a notable impact, either in terms of doctrine or economic effects.”).
\textsuperscript{122} Kim, supra note 119.
\textsuperscript{123} FCC Restoring Internet Freedom Initiative, supra note 10.
\textsuperscript{124} Id.
\textsuperscript{125} Id.
interpreted and analyzed.\textsuperscript{126} Further, the report correctly reminds readers of the difference between correlation and causation:

Whether investment is up or down after Title II classification doesn’t necessarily tell us much about to what extent . . . Federal Communication Commission (FCC) policy is to thank (or blame) for those changes. Not only is the time period far too short, investment overall could very well be up, but not up as much as it otherwise would be without Title II (same if there was a decline).\textsuperscript{127}

Even with these cautions of statistical analysis, another report affirmatively concludes that “'[p]ublicly-traded broadband internet access service providers' own investment data shows an aggregate increase of 5.3 percent when we compare the two years preceding the Commission’s February 2015 vote to adopt open internet rules and Title II classification with the two years following that vote.”\textsuperscript{128} Thus, at best, the FCC’s current statement that investment decreased during the Open Internet Order is inconclusive. At worst, it is flat out incorrect.

Finally, as discussed previously, transparency is an ineffective tool when consumers have no meaningful choice to shop between ISPs, even though the FCC “anticipates that the . . . disclosures will empower consumers and businesses with information about their broadband internet access service.”\textsuperscript{129} Transparency without additional action is an insufficient means to foster meaningful choice in the market; thus, the Restoring Internet Freedom Order falls short by simply mandating that ISPs report this conduct without pairing it with other requirements.

In sum, the Restoring Internet Freedom Order, which eliminated conduct-focused rules, failed to address concerns about monopolization of the broadband market. Instead, this rule merely returned the ISP market to the pre-2010 status quo.


\textsuperscript{127} Id.


IV. **Proactive Legislation and Regulation Are Necessary to Promote the Public Interest and to Balance the Efficiencies Inherent to the Broadband Industry with Concerns of Undue Discrimination.**

A. An Amendment to the Telecommunications Act of 1996 Is Required to Finally Determine the Classification of Broadband Service and the FCC’s Scope of Authority in Regulating ISPs.

Congress should amend the 1996 Telecommunications Act to: (1) prohibit the political flip-flopping of broadband classification based on political agendas and (2) address technological differences that distinguish broadband from other areas of the telecommunications market. Congress, rather than the FCC or courts, remains best suited to resolve the policy issues raised in recent years by addressing the ambiguities and concerns through the legislative process. In amending the Telecommunications Act, Congress should provide more direction to the FCC, to ISPs, and to the public, particularly with regards to how to classify ISPs—thus determining the FCC’s scope of authority to regulate ISPs.

Additionally, this newly amended statute should include specific instruction on the FCC’s scope of authority to craft new regulatory rules for ISPs. This new category for “smart services” must take into account the unique characteristics of the Internet and the technological capabilities of ISPs that typify broadband service. When the 1996 Telecommunications Act was enacted, the prevailing means of communication in the general public were “dumb”\(^{130}\) services, capable of “little more than . . . [connecting] an electrical circuit between a calling party and a called party. . . . If the system was overloaded, the caller got a busy signal and came back later.”\(^{131}\) However, “smart services” require more than a binary connect or do not connect decision. Instead, they require decisions concerning how to connect. This new “smart services” category must grant more authority than § 706 of the Telecommunication Act of 1996 in order to avoid the same vacating judgment of Verizon v. FCC, which found that the FCC lacked statutory authority to create anti-blocking and anti-discrimination rules when broadband is classified as an information service.\(^{132}\) In addition, Congress could consider granting less authority to the FCC than that of common carriers under Title II, if, for

---

\(^{130}\) EHRlich, supra note 26.

\(^{131}\) Id.

example, the legislature determined it was inappropriate for the FCC to require ISPs to file rate schedules or submit contracts to the FCC for review.  

B. A Regulation Is Needed to Draft the Specific Conduct-Focused Rules that Incentivize ISPs to Behave in Congruence with the Public Interest

Regardless of whether Congress chooses to amend the current telecommunications statute, a new regulation is required to address concerns with the broadband market structure and anticompetitive conduct of ISPs. Mere re-adoption of the 2015 Open Internet Order remains insufficient. Instead, a new regulation should aim to facilitate market conditions that align business conduct with the public interest. While the intent of the 2015 rules is essential to the furtherance of the public interest, more specific rules should be adopted to reduce the problem of over and under-inclusiveness of the rules. The FCC could also attempt to address the lack of competition by limiting the market power of ISPs by breaking up the market participants or by forcing ISPs to share access to the underlying Internet infrastructure. However, such market-based responses are beyond the scope of this paper.

Conduct-focused regulations are appropriate to achieve the public interest of ensuring that reliable Internet access is provided to all Americans in a manner that is not unduly discriminatory at a reasonable cost. In addition to addressing the statutory public interest, clarity of

---

133 Loeb, supra note 61, at 20-21.
134 “Effective competition is, in contrast, some combination of market structure, seller and buyer conduct, and performance outcomes that achieves the goals sought by the policymaker.” Hempling, supra note 9, at 122.
135 Where unbalanced market power creates anticompetitive behavior, at least two types of remedies can address these deficiencies: conduct-based regulations and market-based remedies (e.g., limiting market power by forcing the market participants to break up). The FCC has used both approaches to create competition in the telephone market. For example, in 1984, after the Department of Justice initiated an antitrust lawsuit against AT&T, AT&T split off and relinquished control over the Bell Operating Companies. This paper proposes conduct-focused rules, which when paired with ongoing oversight by the FCC and consumer rights of action, are likely sufficient to keep ISP behavior consistent with the public interest. A different approach to introducing competition to the broadband market may include limiting the market power of ISPs by addressing flaws in the market structure; for example, forcing ISPs to share access to the underlying Internet infrastructure. This paper does not purport to explore these solution comparisons in full; instead, it offers analysis on one possible approach to the issue through rules that are discussed below.
136 See discussion supra Section II.
rules also benefits consumers. First, transparency provides consumers with the tools to identify practices that are and are not allowed, which empowers individuals to hold ISPs and the FCC accountable for reliable Internet access. Second, regulations that craft clearer lines between permissible and impermissible practices advance the public interest by facilitating confidence and trust between market participants. Thus, at a minimum, new rules should reinstate the transparency and anti-blocking rule of the 2015 Order. Additionally, the FCC should provide more specific guidance under the anti-throttling and no paid prioritization rules, especially in defining what constitutes reasonable network management practices and what does not. In other words, the FCC should define what constitutes duly and unduly discriminatory treatment of data.

1. Transparency Is Necessary but Not Sufficient Without an Enforcement Mechanism for Improper Conduct

Transparency is necessary. This is something both the Open Internet Orders and the Restoring Internet Freedom Order agree on. Transparency provides both individuals and the FCC with a means by which to evaluate unduly discriminatory behavior, a key aspect in promoting public interests.

Even though transparency provides some inherent scrutiny of ISP practices, consequences for improper conduct are also necessary. While there are many possible means of building in a check on ISP behavior, one possible means may be to provide a formal complaint mechanism through the FCC with which individuals could report unduly discriminatory behavior.

Transparency is not a sufficient enforcement mechanism absent additional regulatory tools. While transparency provides users with more information to make choices, it does not generate effective competition that would give them meaningful options. For example, if only one broadband service provider exists in the area, the end user can be perfectly informed of the ISPs’ choices but still lack an alternative to their service. As noted previously, approximately 129 million Americans only have one option for broadband in their area. Because of this market structure

---

137 See discussion supra Section III.A.1.
problem, the transparency requirement must be supplemented with other conduct-focused rules to direct the conduct of ISPs that they otherwise would not adhere to in order to promote the public interest.

2. Blocking Legal Content Is Per Se Unreasonable

Allowing ISPs to block lawful content would exclude ideas from the marketplace of ideas, a prevailing paradigm in First Amendment theory and jurisprudence. Although the First Amendment is only implicated by government action, new anti-blocking rule for ISPs should embrace the values that the First Amendment protects for three reasons.

First, while the “marketplace of ideas” was initially a metaphor, today ISPs provide the actual infrastructure to construct a real marketplace of ideas online. “While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the ‘vast democratic forums of the Internet’ . . . .” Second, the FCC, by promulgating rules, is effectively allowing or disallowing entry of ideas into the marketplace depending on whether they permit or prohibit blocking under a new broadband order. In other words, although ISPs are the actors in blocking legal content, the government sanctions this censorship by not crafting a rule prohibiting blocking. Additionally, this government-sanctioned censorship has significant effects on the press, which is generally granted

---

139 U.S. v. Rumley, 345 U.S. 41, 56 (1953) (Douglas, J., concurring); cf. Brandenburg v. Ohio, 395 U.S. 444, 456 (1969) (“The line between what is permissible and not subject to control and what may be made impermissible and subject to regulation is the line between ideas and overt acts.”).


142 Petitioner Brief for Writ of Certiorari at i, Berninger v. FCC, 825 F.3d 674 (D.C. Cir. 2016) (No. 17-498) (cert. denied) (listing question #1 for the court as “Does the Commission’s assumption of gatekeeper power over new methods of communication, in the most important place . . . . for the exchange of views . . . . the vast democratic forums of the Internet . . . . violate the First Amendment?”) (internal citations omitted).
strong First Amendment protections against censorship,\footnote{Willingham, supra note 140; see also Red Lion Broad. v. FCC, 395 U.S. 367 (1969) (holding that the FCC could require radio stations to provide equal airtime to opposing points of view by the press under the Fairness Doctrine, allowing the government to mandate access to the press even though radio stations were privately owned). \textit{But see} Miami Herald v. Tornillo, 418 U.S. 241 (1974) (holding that a government’s mandate to access to the press was unconstitutional when the publication only has finite resources).} given that online news outlets are the primary form of news communications today.\footnote{Christine Schmidt, \textit{Americans Expect to Get Their News from Social Media, But They Don’t Expect It to Be Accurate}, NIEMANLAB (Sept. 10, 2018, 11:35 AM), \url{http://www.niemanlab.org/2018/09/americans-expect-to-get-their-news-from-social-media-but-they-dont-expect-it-to-be-accurate/} (citing a PEW Institute report) [https://perma.cc/3YP4-WANJ].} Third, as a policy matter, Censorship curtails speech and debate, fundamental to the democratic process.\footnote{Eric Fish, \textit{Is Internet Censorship Compatible with Democracy? Legal Restrictions of Online Speech in South Korea}, 10.2 ASIA-PACIFIC J. HUM. RTS. & L. 43 (2009) (“The possibility of government control over the Internet cuts out the very heart of its democratic ambitions.”).} For these policy reasons, the FCC should prohibit ISPs from blocking legal content.

3. “\textit{Reasonable Discrimination}” Does Not Mean No Discrimination

“[D]iscrimination can be lawful or unlawful, depending on whether it is ‘due’ or ‘undue.’”\footnote{\textit{Id.}} Due discrimination means “treat[ing] similar customers similarly; dissimilar customers dissimilarly.”\footnote{\textit{Id.}} This same rule should be applied to data: treat similar data similarly, dissimilar data dissimilarly. In the context of broadband, this line is a helpful distinction in determining what is “unreasonable discrimination” under 47 C.F.R. § 8.7 of the 2010 \textit{Open Internet Order}, prior to its repeal.\footnote{\textit{Id.}} Even with this definition, conduct-specific rules that define undue discrimination should be included for common concepts of potentially discriminatory behavior, including, at a minimum, throttling and paid prioritization practices.

a. Not All Throttling Is Unduly Discriminatory

As mentioned previously, throttling means degrading or impairing access to lawful Internet traffic based on the content, application, service, users, or use of a non-harmful device. To supporters of the *Open Internet Orders*, throttling means that all traffic should be treated equally. But, changes in technology require changes in regulation. “The idea that all traffic must be treated equally sounds democratic, but can be costly and inefficient in practice, and ignores the reality that different Internet traffic can have different needs for speed and reliability.”149 Throttling, in certain circumstances, may actually allow ISPs to optimize performance of the network.150 This optimization is especially important for essential services, such as “autonomous vehicles, remote surgeries, and public safety communications.”151 For example, distinguishing between different types of traffic across the Internet allows ISPs to keep certain “packets” of data together, thereby reducing lag time and buffering.152 In addition, treating data differently could allow for ISPs to create service packages based not on download and upload speeds generally but on the types of services a user requires. While this rule could be implied by the 2015 Order’s requirement for “reasonable network management” exceptions,153 crafting an explicit rule may force both sides of the net neutrality debate to grapple with the issue directly, setting aside political rhetoric and grounding the conduct-driven rules in the foundation of how the Internet operates.

Relying on the analogy that due discrimination (as opposed to undue discrimination), as related to customers, means treating all similar customers similarly, these types of throttling should treat similar classes of data similarly. For example, in the power industry it was not unduly discriminatory to treat municipalities and rural cooperatives differently.

---

149 EHRlich, supra note 26, at 12.
150 See id.
152 EHRlich, supra note 26, at 12.
153 Reasonable network management. A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service. 47 C.F.R. § 8.2.
where “the different load profiles meant different costs to serve.”

Analogously, this general rule could also be used in distinguishing between different types of data. For example, “a packet containing the next frame of your streaming movie or online game needs to be delivered in very timely fashion, while email or a Facebook post can take its time (relatively speaking).”

In fact, discrimination in this manner may increase quality by increasing speed for the services delivered and increase cost effectiveness because end users are paying only for the services they need, giving buyers the opportunity to choose a service that meets their needs. These types of throttling should be permissible and are not unduly discriminatory.

b. Some Edge Provider Paid Prioritization Is Unduly Discriminatory

Paid prioritization embodies the idea that ISPs can promote some data over others based on an edge provider’s payments to increase speed, and thus traffic, on their websites. Throttling by paid prioritization may be unduly discriminatory, although the reasonable network management exception under the Open Internet Orders and the Restoring Internet Freedom Order provide an escape hatch with which ISPs may justify charging large sums of money to edge providers for prioritization. For example, “Netflix already pays huge amounts of money to get their data to consumers quickly,” but this is permissible as a reasonable network management practice because it helps “the Internet run properly.”

---

154 HEMPLING, supra note 9, at 291.
155 Devin Coldewey, These Are the Arguments Against Net Neutrality and Why They’re Wrong, TECH CRUNCH (May 19, 2017), https://techcrunch.com/2017/05/19/these-are-the-arguments-against-net-neutrality-and-why-theyre-wrong/ [https://perma.cc/2TJX-FGBK].
156 See Open Internet Order, 25 FCC Rcd 17905, 17945 ¶ 72 (2010) (“However, prohibiting tiered or usage-based pricing and requiring all subscribers to pay the same amount for broadband service, regardless of the performance or usage of the service, would force lighter end users of the network to subsidize heavier end users. . . . The framework we adopt today does not prevent broadband providers from asking subscribers who use the network less to pay less, and subscribers who use the network more to pay more.”).
157 Note that paid prioritization is a type of throttling that allows “ISPs [to] double-dip by letting them charge consumers for access to Internet services and then turn[ing] around and charg[ing] Internet services for better access to consumers.” Trendacosta, supra note 151.
158 See id.
159 Coldewey, supra note 155.
“Critics of net neutrality believe bandwidth-hogging media giants like Netflix should have to pay extra for the heavy burden they place on broadband networks” while proponents typically argue that “a fast lane for one site would necessarily slow down other, potentially competing sites.” But, these two viewpoints can be reconciled by treating similar edge providers similarly and different edge providers differently. Rather, the prohibition should be against ISPs “rig[ging] sweetheart deals giving fat pipe access to services of their choosing, while charging the competition higher rates.” For example, critics of the recent AT&T-Time Warner merger explain how AT&T may “weaponize” the media content it acquired in the acquisition. With the elimination of the prohibition against paid prioritization, AT&T could zero-rate all data they owned, while leaving unaffiliated media companies under customer data caps. AT&T can also legally charge other media companies for the same zero-rated prioritization.

The rule to treat all similar edge providers similarly and different edge providers differently should take into consideration the following factors: (1) whether the edge providers are competitors with each other, (2) the type(s) of data the edge providers primarily transmit, (3) the number of customers, readers, or viewers of the edge providers’ content, (4) the bandwidth required for an ISP to provide users with adequate service, and (5) potentially additional metrics. Congress should grant the FCC authority to classify edge providers based on these factors and/or other factors deemed appropriate. For example, ISPs should not give preferential treatment to Netflix at a lower paid prioritization rate and discourage Hulu access by charging them a higher rate because they are competitors, transmit similar types of data, and likely have a similar number of customers. Thus, for example, assuming the FCC finds the five factors above are equivalent for Netflix and Hulu, the rate an ISP charges to Netflix for prioritization should be approximately equal to the amount that Hulu is charged. It is inequitable to simply treat all video services equally, for example, because this may prove detrimental to small

161 Coldewey, supra note 155.
163 See id.
businesses that likely cannot afford to pay for the faster pipeline at the same rate as Netflix and Hulu. In other words, ISPs should create reasonable rate tiers, allowing smaller costs for new entrants to the market. One possible means for structuring these rate tiers would be to charge edge providers based on the bandwidth required to transmit their services.

While other industries also charge different rates for prioritization without undue discrimination, paid prioritization in the broadband market is different because of the public interest discussed in Section II and because of the failures in the market structure discussed in Section III. For example, an individual may pay for a toll lane or toll road for faster access to a destination. The rule articulated for paid prioritization here is similar. In other words, if Netflix wants a “fast lane,” they can pay for it; so can a start-up video service. The argument rather is that the “first class seat” price should be different for Netflix versus a start-up because of the number of cars they will be sending across the toll road. Thus, a lower rate for smaller edge providers minimizes the economic burden required to compete with a larger, more established edge provider. Additionally, a higher toll for a larger edge provider does not discourage growth or innovation, even if they have to pay a higher rate because this is only one of many factors a multi-million dollar company would consider in determining growth strategies. Thus, this rule balances the economic interests in allowing ISPs to charge for more bandwidth with the economic interest of promoting new edge providers in the market and may remove barriers to entry where newcomers cannot pay to play. Accordingly, paid prioritization may be permissible if crafted in such a way that treats similar data similarly but impermissible where it does not.

Specific rules that give clarity to ISPs on what practices are unduly discriminatory protect these providers from litigation based on application of broad, ambiguous rules—or no rules at all under the Restoring Internet Freedom Order—and protect end users from practices that may detract from a free and open Internet. The previous rules failed to address the ISP market structure, but removing the textual ambiguities surrounding the classification of broadband and providing clearer, more explicit regulations (and attached consequences for violations) leads to a more consumer-friendly market and seeks to limit anticompetitive behavior. These conduct-driven rules will result in ISP performance consistent with the public interest, helping to ensure reliable Internet access is available to all Americans in a non-unduly discriminatory manner at a reasonable cost. The sheer importance of these services to the American economy and
individual development mean they demand a closer watch. This paper provides one way to do this—put the public interest first.
CASE COMMENT
**Berninger v. Federal Communications Commission: The Outer Limits of Judicial Deference**

Daniel Carlen*

**Cite as:** 3 Geo. L. Tech. Rev. 461 (2019)

## I. Introduction

Broadband Internet is the most common Internet service used in the United States. Broadband includes all services that provide high speed Internet, although not all Internet services are broadband. Government regulation of broadband is highly controversial, in part due to broadband’s rapid development and expansion. Congress has avoided drafting legislation governing broadband and instead granted regulatory authority to the Federal Communications Commission (FCC) under the theory that the FCC is in a better position to promulgate rules related to telecommunications and information services. In turn, the FCC has generally limited its regulation of broadband, with the goal of encouraging online innovation such as the development of video streaming, online commerce, and social networks.4

In pursuit of this goal, the FCC developed net neutrality principles in the 2010 and 2015 Open Internet Orders. Net neutrality is “the principle that [Internet Service Providers (ISPs)] treat all data on the...
Internet equally, and not discriminate or charge differently by user, content, website, platform, application, type of attached equipment, or method of communication. The recent case of Berninger v. FCC addressed the issue of whether the FCC can promulgate net neutrality rules in the future without express congressional authorization. While the Supreme Court ultimately denied certiorari, the question presented by Berninger is still relevant given the continuing public debate on net neutrality and the possibility of a future administration sympathetic to stronger broadband regulation.

In Berninger, petitioner argued that the FCC should be denied judicial deference when implementing net neutrality rules without clear congressional authority because doing so would raise questions of deep political and economic significance. A federal agency that demonstrates that its rules are entitled to deference has much greater flexibility in creating and enforcing rules. Therefore, if the FCC created an order similar to the Open Internet Order of 2015, and the new order were challenged in court, the FCC would likely argue that it is entitled to judicial deference. Petitioner, in turn, asserted that regulations raising questions of deep political and economic significance, such as more robust regulation of broadband, should be exempt from ordinary Chevron deference analysis.

This case comment argues that the Court should not defer to the FCC’s interpretation of the Telecommunications Act of 1996 as to whether broadband is an information or telecommunications service because regulation of broadband raises a question of deep political and economic significance. In the last ten years, the FCC has on several occasions changed its classification of broadband providers, creating ambiguity as to the scope of authority with which the FCC may govern

---

9 Petition for Writ of Certiorari, supra note 7, at 22.
10 Brief of Respondent Free Press at 32, Berninger v. FCC, 139 S. Ct. 453 (2018) (arguing that the Chevron deference framework should apply in the present case).
11 See King v. Burwell, 135 S. Ct. 2480, 2489 (2015). In Mozilla Corp. v. FCC, No. 18-1051 (D.C. Cir. 2018), which had oral arguments on February 1st, petitioner challenged FCC’s repeal of the 2015 Open Internet Order. If the U.S. Court of Appeals for the D.C. Circuit overturns parts of the repeal, then FCC may have to implement further regulation of broadband.
ISPs. Fully removing the ambiguity would require Congressional legislation clarifying whether broadband is a telecommunications service and whether the FCC has the authority to implement net neutrality regulations such as restrictions on blocking, throttling, and paid prioritization.

Furthermore, the Supreme Court has previously declined to grant Chevron deference in circumstances where an agency’s regulation raises questions of “economic and political significance,” which the FCC would raise in implementing restrictions on blocking, throttling, and paid prioritization because these restrictions have the capacity to impact millions of Americans and involve billions of dollars.\(^\text{12}\) Given that the Court has found that Chevron deference does not apply to an IRS interpretation of health insurance tax credits\(^\text{13}\) and the FDA’s regulation of tobacco products,\(^\text{14}\) so too should the Court find that Chevron deference does not apply to regulation of broadband providers.

II. BACKGROUND

Congress passed the Telecommunications Act of 1996 (1996 Act)\(^\text{15}\) to amend the 1934 Act establishing the FCC.\(^\text{16}\) The 1996 Act expanded the FCC’s regulatory jurisdiction\(^\text{17}\) to include Internet-based services—while Congress authorized the FCC to regulate information as well as telecommunication services, Congress did not explicitly pass legislation allowing the FCC to prohibit service providers from blocking or throttling lawful content or engaging in paid prioritization.\(^\text{18}\) In 2010, the FCC initially attempted to implement net neutrality principles under the Open Internet Order of 2010 (2010 Order).\(^\text{19}\) The 2010 Order required ISPs to neither unreasonably discriminate in transferring network traffic

\(^\text{12}\) See King, 135 S. Ct. at 2489.
\(^\text{13}\) See id.
\(^\text{16}\) 47 U.S.C. § 609.
\(^\text{17}\) See 47 U.S.C. § 1302.
\(^\text{19}\) See generally 2010 Open Internet Order, 25 FCC Red. 17905 (2010).
nor throttle or block legitimate websites, applications, services, or non-harmful devices.\footnote{Id.}

The United States Court of Appeals for the District of Columbia (D.C. Circuit) held in 2014 that the FCC had limited authority under the 1996 Act to regulate ISPs because the 2010 Order classified ISPs as providers of information services rather than telecommunications services.\footnote{Verizon v. FCC, 740 F.3d 623, 650 (D.C. Cir. 2014).} Telecommunications services and information services are each regulated by their own statutory provisions, the former by Title II of the 1934 Act and the latter by \$ 706 of the 1996 Act.\footnote{Id.; see also 2010 Open Internet Order, 25 FCC Rcd. 17905 (2010).} Title II grants the FCC authority to impose obligations on common carriers, which includes telecommunications services.\footnote{47 U.S.C. \$ 201(b).} Under this authority, the FCC can, for example, require the prevention of “unjust and unreasonable discrimination” and require the “[interconnection] with other carriers and to establish through-routes.”\footnote{G. Hamilton Loeb, The Communications Act Policy Toward Competition: A Failure to Communicate, 1978 DUKE L.J. 1, 20 (paraphrasing 47 U.S.C. \$ 201(a)).} Additionally, under Title II, the FCC has the authority to impose obligations on common carriers to charge “just and reasonable” prices among all products and services connected to telecommunications services.\footnote{47 U.S.C. \$ 201(b).}

Conversely, because information services are not considered common carriers, the FCC exercises substantially less authority over providers of information services.\footnote{Verizon, 740 F.3d at 655.} The FCC interpreted \$ 706 of the 1996 Act in a way that “grant[ed] the Commission affirmative authority to promulgate rules governing broadband providers”\footnote{Id. at 642.} in order to meet the “specific statutory goal of accelerating broadband deployment.”\footnote{Id. at 641.} In \textit{Verizon v. FCC}, the D.C. Circuit held that because the FCC did not classify broadband as a telecommunications service under the 2010 Order, the FCC did not have authority to regulate ISPs as common carriers and therefore did not have the authority to promulgate the anti-blocking and anti-discrimination rules.\footnote{Id.}

In response to \textit{Verizon}, the FCC reclassified broadband as a telecommunications service in the \textit{2015 Open Internet Order} (2015 Order).\footnote{2015 Open Internet Order, FCC 15–24, \S 363 (2015).} The reclassification allowed the FCC to reintroduce rules
vacated in Verizon, including rules prohibiting providers from blocking or throttling lawful content. Additionally, the FCC crafted a new rule prohibiting paid prioritization. As mentioned, the FCC has broader authority to regulate telecommunications services under Title II, thereby permitting the FCC to regulate ISPs as common carriers and subject them to more extensive regulation. The 2015 Order therefore allows the FCC to circumvent the barrier to regulation set up by the D.C. Circuit in Verizon.

As mentioned, the 2015 Order implements net neutrality principles by banning paid prioritization for Internet access. It also significantly restricts ISPs from blocking or interfering with access provided to specific parties, subject to “reasonable network management practices.” The FCC’s restrictions prevent ISPs from controlling a user’s bandwidth and prevent “edge providers” from receiving exemptions to net neutrality rules that are denied to startups and new market participants. While the FCC explicitly stated that it retains the right to waive the restrictions on paid prioritization at any time, requests for waivers are subject to a notice-and-comment procedure, which sets a high bar for applicants to demonstrate that a waiver (1) would not undermine open Internet access and (2) would provide a significant benefit to the public. Hence, the FCC’s right to waive restrictions grants the agency significant authority over online activity.

In response to the 2015 Order, the U.S. Telecom Association brought suit on the grounds that the order was “arbitrary, capricious, and an abuse of discretion.” The D.C. Circuit in U.S. Telecom Association v. FCC deferred to the FCC’s interpretation of the 1996 Act, rather than

---

31 Verizon, 740 F.3d at 629; see also Amendment of Section 64.702 of the Comm’n’s Rules & Regulations, 77 F.C.C.2d 384, 387 ¶¶ 5–7 (1980).
33 2015 Open Internet Order, FCC 15–24, ¶ 218.
34 Id. ¶ II.A.1.
35 An edge provider is an established company that provides online content and services.
37 Id. at 58 ¶ 130; see also 47 C.F.R. § 1.3 (the Commission may waive any rule “in whole or in part, for good cause shown”).
38 2015 Open Internet Order, FCC 15–24, ¶ 130; An “open Internet” here means one where all functions of the Internet and means to operate on it are easily accessible to all individuals, companies, and organizations. Tom Wheeler, What Is the Open Internet Rule, BROOKINGS INSTIT. (Sept. 15, 2017), https://www.brookings.edu/blog/unpacked/2017/09/15/what-is-the-open-internet-rule/ [https://perma.cc/4JZ5-SY4S].
40 U.S. Telecom Ass’n v. FTC (U.S. Telecom I), 825 F.3d 674, 689 (D.C. Cir. 2016).
independently interpreting the statute. The court based its decision on *Chevron v. NRDC*, which established the judicial practice of granting administrative agencies deference when interpreting a body of law that grants a federal agency legal authority. The D.C. Circuit held that it must defer to the FCC’s interpretation of the statute because the 1996 Act was ambiguous with respect to the classification of broadband and because the FCC’s interpretation of the Act was reasonable. In other words, because the FCC argued that the 2015 Order was necessary to ensure net neutrality, the court determined that the agency’s decision to reclassify broadband as a telecommunications service was reasonable and deferred to the agency’s judgment as a standard judicial practice. *U.S. Telecom* was consolidated with other pending net neutrality cases challenging the FTC’s authority into *Berninger v. FCC*.

III. SUMMARY OF ARGUMENTS

In *Berninger v. FCC*, the petitioner argues that federal courts should not grant *Chevron* deference to the FCC when it attempts to vastly expand its authority to regulate broadband providers by reinterpreting the FCC’s enabling statute (the 1996 Act). In the petitioner’s view, the FCC’s restrictions on paid prioritization are an interpretation that contradicts prior agency interpretations: this treats the statute as a mere blank slate on which the agency would be empowered to issue law. Thus, the petitioner asserts that granting *Chevron* deference would violate the nondelegation doctrine by vesting the agency with the power to “make law” unmoored from any congressionally enacted policy or law. Since only Congress can exercise legislative power, the petitioner argues that the Court should exercise judicial review to determine whether the 1996 Act granted the FCC the authority to adopt the 2015 Order.

---

41 Id. at 711.
43 *U.S. Telecom I*, 825 F.3d. at 689.
44 Petition for Writ of Certiorari, *supra* note 7, at 22.
45 Id.
46 Id.
47 Id. at 22–24.
IV. Analysis

Although the Supreme Court denied certiorari to Berninger, the issue of whether the FCC is entitled to judicial deference for classifying broadband providers as an information or telecommunications service is still relevant. For example, in Mozilla v. FCC, which held oral arguments on February 1, 2019, the petitioner challenged the FCC’s repeal of the 2015 Order—as opposed to U.S. Telecom, which challenged the FCC’s creation of the 2015 Order. According to the petitioner, the broadband regulation is ambiguous, and the FCC’s interpretation of the 1996 Act is reasonable, thus passing the two-step Chevron deference standard. However, King v. Burwell crafted an exception to Chevron deference for questions of deep political and economic significance. This exception should also apply to broadband regulation because imposing net neutrality rules on ISPs implicates a substantial level of online economic activity and constitutes an issue of political and national importance. Therefore, the FCC should not be entitled to judicial deference, and Congress must resolve the ambiguity as to whether broadband is an information or telecommunications service via legislation.

A. The Application of Chevron Deference

Chevron deference applies when an agency acts under a congressional delegation of lawmaking authority. Such delegation may be made by Congress explicitly or implicitly. Implicit delegations of authority arise in cases where the statute in question grants broad authority to an agency or when the wording of the statute is ambiguous.

Chevron deference requires an agency to first demonstrate that (1) Congress has either not addressed the issue directly or addressed the issue ambiguously and that (2) the agency’s decisions are a reasonable interpretation of the statute. If Congress has directly spoken to the

---

48 Brief for Petitioner Mozilla at 6, Mozilla Corp. v. FCC, No. 18-1051 (D.C. Cir. Apr. 23, 2018).
52 In determining whether a particular construction of a statute by the agency is a “reasonable interpretation,” the Court will look to whether the interpretation is “rationally related to the goals of the statute.” See AT&T Corp. v. Iowa Utils. Bd., 525 U.S. 366, 388 (1999).
precise question at issue, then its direction is controlling over the agency’s interpretation.  

For the two-step analysis under *Chevron* to be applicable, the court must first determine whether Congress intended to delegate administrative authority for interpretations by agencies to carry the force of law. The analysis must look for evidence of implicit congressional delegation. A good indicator of implicit delegation is the use of formal procedures. When Congress provides “for a relatively formal administrative procedure,” which encourages “fairness and deliberation,” this indicates that “Congress contemplates administrative action with the [force] of law.” By contrast, agency interpretations that are not the result of formal adjudication or notice-and-comment rulemaking—e.g., interpretations stated in opinion letters, technical releases, policy statements, agency manuals, and enforcement guidelines—are less likely to receive *Chevron* deference.

Turning to *Berninger*, the question of whether the FCC should receive *Chevron* deference depends to a large extent on whether a decision to classify broadband as a telecommunications service was the result of a formal administrative procedure. This condition is met; the FCC used the notice-and-comment rulemaking process, which, as laid out by the Administrative Procedure Act, is required for “legislative rules,” which have the “force and effect of law.” In the 2015 Order, the FCC used the notice-and-comment rulemaking procedure to form the rule in question, receiving over four million comments.

**B. The Major Questions Doctrine**

When a question of deep “economic and political significance” arises, the delegation of authority to an agency must be more than an implied authorization from the underlying statute; instead, it must be explicit. In these cases, courts should interpret the statute *de novo* rather than applying *Chevron* deference.

---

53 Id. at 377–78.
54 *Mead Corp.*, 533 U.S. at 229.
55 Id. at 237.
56 Id. at 243.
59 See 5 U.S.C. § 553(b)–(c).
than defer to the agency’s interpretation. While the 2015 Order carries the force of law, Congress did not delegate authority to the FCC under the 1996 Act to resolve the significant questions related to net neutrality. Ordinarily, an agency claiming to discover in a “long-extant statute an unheralded power to regulate a significant portion of the economy” meets a great deal of judicial skepticism. The Supreme Court followed such skepticism in carving out an exception to Chevron deference in King v. Burwell for questions of economic and political significance, holding that the IRS’s enforcement of tax credits under the Affordable Care Act was exempt from Chevron analysis. For such a question of deep political and economic significance, the Court reasoned, Congress would have expressly delegated enforcement authority to the IRS if Congress intended the IRS to have such authority.

Requiring explicit delegations from Congress to justify regulations that significantly impact the economy, though a rare occurrence, has precedent. The Court has held that it will closely scrutinize agency actions when the agency is attempting to use existing law to exercise new authority. In other words, courts should, in “extraordinary cases,” hesitate before concluding that Congress intended an implicit delegation that would allow for Chevron deference. In FDA v. Brown & Williamson, the Supreme Court held that although agencies are ordinarily entitled to deference in the interpretation of statutes they administer, both the courts and the agency in question “must give effect to the unambiguously expressed intent of Congress.” The Court found Congress had not delegated authority to the Food and Drug Administration (FDA) to regulate tobacco products. In particular, the Court pointed out that in the six separate statutes passed by Congress since 1965 regarding tobacco regulation, the FDA was not granted jurisdiction to regulate tobacco products. Therefore, the Court concluded that Congress did not intend to delegate regulation of tobacco products to the FDA.

Likewise, in Berninger, regulation over broadband by the FCC was not explicitly intended in the 1996 Act nor was authority to regulate broadband expressly delegated. The 1996 Act created the distinction between telecommunications services and information services but did not address whether broadband was a telecommunications or an information

---

63 Petition for Writ of Certiorari, supra note 7, at 20.
65 King, 135 S. Ct. at 2489.
67 Id. at 125.
68 Id. at 122.
service.\textsuperscript{71} By regulating broadband providers like providers of telecommunications services, the FCC’s 2015 Order attempted to address this ambiguity in the 1996 Act.

1. Economic Significance

While the Supreme Court never developed a method to determine the “economic significance” of a regulation, the Court has held that an agency interpretation of its authorizing statute that authorizes the agency to regulate tobacco is economically significant.\textsuperscript{72} Additionally, the Court held that administering tax credits for the Patient Protection and Affordable Care Act (ACA) was similarly economically significant.\textsuperscript{73} In both cases, the Court assessed the economic magnitude of the regulatory decision, which can be quantified as either the number of American citizens or the amount of dollars impacted by the agency’s policy. In 2000, cigarette sales were valued at approximately $62 billion, while other tobacco product sales were valued at approximately $7.5 billion. Total cigarette consumption annually was approximately 435 billion packs, while other tobacco products were estimated at approximately 15.15 billion units during the same period.\textsuperscript{74} These attempted tobacco regulations would have brought a multi-billion-dollar industry under the FDA’s regulatory domain.\textsuperscript{75}

The ACA tax credits had a comparable economic impact. Under Section 36B of the ACA, the IRS allowed any household with an income between 100 percent and 400 percent of the poverty line to receive a subsidy in the form of a tax credit.\textsuperscript{76} The intent of this subsidy was to assist low-income Americans with purchasing health care insurance.\textsuperscript{77} After \textit{King v. Burwell}, the government released data indicating that in 2015 approximately 6.4 million Americans were enrolled in a federal exchange and received a tax credit.\textsuperscript{78} According to other estimates, 8.2

\begin{itemize}
\item \textsuperscript{71} See 47 U.S.C. §§ 153 (24), (53) (providing definitions for “information service” and “telecommunications service”).
\item \textsuperscript{72} FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000).
\item \textsuperscript{73} See King v. Burwell, 135 S. Ct. 2480, 2489 (2015).
\item \textsuperscript{75} Id.
\item \textsuperscript{76} 25 U.S.C. § 36B.
\item \textsuperscript{77} See King, 135 S. Ct. at 2495–96.
\item \textsuperscript{78} Lena H. Sun, 6.4 Million Americans Could Lose Obamacare Subsidies, Federal Data Show, WASH. POST (June 2, 2015), https://www.washingtonpost.com/national/health-science/64-million-americans-could-lose-obamacare-subsidies-federal-data-
million Americans relied on these subsidies to pay for healthcare. Therefore, the tax credits administered by the IRS had an economic impact that affected millions of Americans and a healthcare industry valued at $3.5 trillion. The Supreme Court held that this kind of impact was economically significant, and thus judicial deference should not be extended.

The FCC’s net neutrality rules have at least the same level of economic impact as the tax credits’ impact on the healthcare industry in King v. Burwell and the FDA tobacco regulations’ impact on consumers and the economy in FDA v. Brown & Williamson. In 2017, online retail sales totaled approximately $450 billion, with roughly 230 million Americans making an online purchase during that year. On the business-to-business side of the online commerce industry, transactions in 2018 were about $900 billion and are on track to be valued at around $1.1 trillion by 2021. Even economic activity that is not conducted entirely online is still supported by online infrastructure. The amount of online economic activity is thus comparable to the economic activity involved in the health insurance and tobacco industries.

The 2015 Order had the potential to impact the level of prioritization in latency and bandwidth that sites can purchase, and hence, the FCC potentially could have impacts on all online economic activity—every Internet user, every industry operating through an online medium, and every product sold online. Therefore, the FCC’s authority over net neutrality regulation implicates an interest at least as economically significant as the interests in Burwell and Brown & Williamson.


[81] See King, 135 S. Ct. at 2489.


Consequently, the Court should exercise the same level of scrutiny in the present case.

Furthermore, the Court’s deference to the FCC in *Brand X* should not apply to the 2015 Order. In *Brand X*, the FCC was granted deference in its decision not to classify broadband as a common carrier, but the 2015 Order does not merely reverse a statutory interpretation. Instead, the 2015 Order imposes an even greater degree of regulation on broadband, resulting in a significant economic impact. The major questions doctrine concerns the 2015 Order’s economic impact as opposed to the FCC’s decision to change how it interprets an ambiguity in the statute. The Court’s application of the major questions doctrine is not affected by its grant of deference to the FCC in *Brand X*, where the possible economic impact was not a cited concern. The argument against granting the FCC *Chevron* deference in the present case is therefore distinguished from *Brand X*, which was concerned with statutory construction.

2. Political Significance

The Supreme Court has not elaborated on what factors are relevant when assessing “political significance.” Indeed, the Court discusses questions of “deep economic and political significance” together, which suggests that the factors used to assess economic significance may be relevant to political significance as well. To the extent that political significance constitutes a separate category, the Court likely intended it to be utilized so that judicial deference would preclude agencies from deciding major questions even when the economic impacts of the agency’s decisions are relatively minor. The Court has emphasized the importance of preventing the delegation of congressional policymaking authority to an agency without providing an “intelligible principle” to guide and constrain the exercise of that authority.

---

85 See *King*, 135 S. Ct. at 2488–89.
86 See generally Nat’l Cable & Telecomms. Ass’n, 545 U.S. at 975.
87 *King*, 135 S. Ct. at 2489.
88 For example, the Fifth Circuit found that the Department of Homeland Security’s (DHS) Deferred Action for Parents of Americans and Lawful Permanent Residents (DACA) program was likely unlawful, in part, because it “undoubtedly implicates question[s] of ‘deep economic and political significance.’” *Texas v. United States*, 809 F.3d. 134, 181 (5th Cir. 2015).
89 The Supreme Court interprets “intelligible principles” quite broadly and refers to any standard set by Congress for the agency in question to base their regulations. *See Hampton v. United States*, 276 U.S. 394, 409 (1928).
Additionally, the Supreme Court has emphasized the importance of ensuring democratic legitimacy by presuming Congress is more likely to have focused upon major questions, while leaving the responsibility of the implementation to federal agencies.\(^90\) Justice Breyer, for example, has argued that the Court should take the viewpoint of the “reasonable member of Congress” when determining the scope of the administrative discretion delegated to federal agencies.\(^91\) Breyer then goes on to assert that such a reasonable member would not have wanted courts to defer to agencies on questions of “national importance.”\(^92\)

Those questions that are deemed to be of national importance by the Court are usually questions that are the subject of substantial discussion and over which an agency asserts previously unclaimed regulatory authority.\(^93\) Prior to 1996, tobacco products were controlled through a combination of state and congressional regulations, and the FDA played no role in the regulation of tobacco products.\(^94\) When the FDA proposed its first rule to regulate tobacco products, it received over 700,000 submissions, more than “any other time in its history on any other subject.”\(^95\) These factors suggest that regulation of tobacco products would have been a subject of national importance during the time that the FDA implemented its first regulation of the industry.

Similarly, Congress has not explicitly passed a law delegating authority to the FCC to regulate broadband to the same extent as common carriers. Also, the FCC had not regulated or banned paid prioritization of Internet bandwidth or latency prior to the 2015 Order.\(^96\) The Internet has been called “one of the most significant technological advancements of the 20th century”\(^97\) and is therefore arguably a topic of national importance. Additionally, net neutrality has been the topic of frequent political debate.\(^98\) Thus, in asserting previously unclaimed regulatory authority over


\(^{91}\) STEPHEN BREYER, ACTIVE LIBERTY: INTERPRETING OUR DEMOCRATIC CONSTITUTION 103 (Alfred A. Knopf et al., 2005).

\(^{92}\) Id. at 107.

\(^{93}\) Id. at 267.

\(^{94}\) Brown & Williamson Tobacco Corp., 529 U.S. at 125.

\(^{95}\) Id. at 126–27; see also Regulations Restricting the Sale and Distribution of Cigarettes and Smokeless Tobacco to Protect Children and Adolescents, 61 Fed. Reg. 44418 (1996).

\(^{96}\) Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5629 (2015).


ISPs, the 2015 Order placed the FCC in the same position as the FDA in its initial attempts to regulate tobacco products.

V. CONCLUSION

The Court should not grant judicial deference to the FCC’s interpretation of the 1996 Act because the 2015 Order raises questions of “deep economic and political significance.” The Court has, in the past, declined to grant deference to agencies when they attempted to craft rules with the force of law that impact millions of Americans and involve billions of dollars. 99 Therefore, the FCC’s 2015 Order, which impacts millions of Internet users and implicates billions of dollars in online economic activity, should not be granted deference. Even though the 2015 Order would ordinarily meet the two-part test for judicial deference under Chevron, this issue should be addressed by Congress prior to the FCC’s intervention.

TECHNOLOGY EXPLAINERS
“STUDY DRUGS”: THE MECHANISMS OF ADHD MEDICATIONS AND THEIR ABUSE ON COLLEGE CAMPUSES

Peter Pyatigorsky*

CITE AS: 3 GEO. L. TECH. REV. 476 (2019)

I. INTRODUCTION

The term “study drugs” refers to a sub-class of prescription stimulants, approved by the FDA for the treatment of Attention Deficit/Hyperactivity Disorder (ADHD), that students routinely abuse to enhance academic performance. This sub-class, categorized as substituted phenethylamines, includes methylphenidate (Ritalin, Concerta), dexamphetamine (Focalin), dextroamphetamine (Dexedrine), lisdexamfetamine (Vyvanse), and a mixture of amphetamine salts (Adderall). In the past decade, illicit abuse (i.e., without a prescription) of study drugs on college campuses has skyrocketed, with studies estimating that up to thirty-five percent of college students abuse such stimulant medications.¹

Remarkably, study-drug abuse, unlike the abuse of alcohol and other recreational drugs, fails to elicit condemnation among parents and medical professionals,² who frequently dismiss this behavior as benign and of meager concern. For example, when asked about stimulant abuse

* Georgetown University Law Center, J.D. Candidate 2020; Long Island University, Brooklyn Campus, B.S. Biology. My sincerest gratitude goes out to the sublime GLTR editors, without whom this piece would not have been possible.

¹ Jason Besser, Do We Have an Amphetamine Problem on College Campuses, CTR. ON ADDICTION (Oct. 3, 2017), https://www.centeronaddiction.org/the-buzz-blog/do-we-have-amphetamine-problem-college-campuses [https://perma.cc/ZR5F-BY28].

among college students, Dr. Brian Doyle, a clinical professor of psychiatry at Georgetown University Medical Center, gave the following response:

It's like the psychological equivalent of using steroids to enhance physical performance. These students seem to be doing it with relative impunity, and it doesn't seem to be causing too much trouble since most use the drugs not to get high but to function better. So when exams are over, they go back to normal and stop abusing the drugs.³

Unconcerned views like Dr. Doyle’s underscore the extent to which study drugs have become a normalized part of college life. This explainer will first discuss the underlying biochemistry and physiological effects of study drugs. Thereafter, the evolution of study drug abuse will be examined.

II. HOW STUDY DRUGS AFFECT THE BODY AND BRAIN

A. Neurotransmitters: The Brain’s Biochemical Messengers

Neurotransmitters are chemical messengers, which transmit signals between neurons (specialized cells in the brain and nervous system) and from neurons to muscle cells.⁴ Neurons are connected to other neurons by synapses, which include the extremities on either side of the neuron, and the microscopic gap between the cells through which chemical signals pass, known as the synaptic cleft.⁵ Generally, an electric stimulus, called an action potential, travels down the length of a neuron on one side of the synapse (the pre-synaptic neuron), triggering the release of neurotransmitters from the synaptic vesicles (neurotransmitter storage sacs in the neuron) into the synapse.⁶ On the other end of the synapse, the discharged neurotransmitters will interact with specific receptors on the receiving (post-synaptic) neuron.⁷ Each neurotransmitter has a designated

---

⁵ Id.
⁷ Id.
receptor into which it fits, like a “lock and key,” with only chemically compatible neurotransmitters attaching to a given receptor.

Once a neurotransmitter binds to a receptor, it causes the receiving neuron to respond by either firing an action potential (an excitatory response, which further propagates the signal) or by not firing an action potential (an inhibitory response, which stops the propagation of the signal). After binding to receptors, neurotransmitters may (1) degrade or be deactivated by enzymes in the synapse, (2) drift away from the receptor into the synapse, and/or (3) undergo re-uptake, a process by which neurotransmitters return to the pre-synaptic neuron.

Study drugs interfere in the neurotransmission process, changing how effectively neurotransmitters are able to signal between cells. These interferences enable study drugs to influence the major physiological activities the nervous system regulates, including: heart rate, sleep, appetite, mood, breathing, and alertness. Study drugs predominantly exert their influence by interacting with a specific subclass of neurotransmitter—monoamines—which includes dopamine, norepinephrine, and serotonin.

Monoamine neurotransmitters are classified based on their molecular composition, exhibiting a single amino group (NH₂) linked by a two-carbon chain (CH₂-CH₂) to a benzene ring. The structure of study drug molecules closely resembles monoamine neurotransmitters, meaning that they can bind to receptors, which would have otherwise been reserved for specific neurotransmitters.

Study drugs chiefly interfere in the neurotransmission of the monoamine, dopamine, and norepinephrine. Dopamine plays an essential role in motor control, information processing, motivation, reward, sexual gratification, reinforcement, alertness, attention, and endurance. Norepinephrine is the brain’s central mechanism for regulating the body’s fight-or-flight response, alertness, memory formation and retrieval,

---

8 Id.
9 Figure 1 displays the pertinent chemical groups of these compounds in red. See John R. Richards et al., Methamphetamine, "Bath Salts," and Other Amphetamine-Related Derivatives: Progressive Treatment Update, ENLIVEN ARCHIVE (Aug. 26, 2014), http://www.enlivenarchive.org/articles/methamphetamine-bath-salts-and-other-amphetamine-related-derivatives-progressive-treatment-update.pdf [https://perma.cc/S2S4-FMD5] (source of Fig. 1).
restlessness, and anxiety.\(^{11}\) Figure 1\(^{12}\) below displays the chemical structure of these two neurotransmitters, with their common chemical group outlined in red. Moreover, Figure 1 also presents a side-by-side comparison of dopamine and norepinephrine to several chemical agents which act upon their effectiveness, including the study drugs Adderall (amphetamine) and Ritalin (methylphenidate).

![Chemical structures of neurotransmitters](image_url)

Figure 1. Chemical structure of dopamine, norepinephrine, methylphenidate, cocaine, amphetamine and related derivatives. The common \(\beta\)-phenylethylamine core structure is highlighted. Despite this structural similarity, amphetamines act as competitive substrates at plasma membrane and vesicular membrane transporters of dopamine, norepinephrine, and serotonin, inhibiting reuptake and inducing reverse transport of these endogenous monoamines.

B. The Dopamine Deficit Hypothesis of ADHD

The precise causes of ADHD are unknown, but scientists theorize that the impaired functioning of certain neurotransmitter systems in the brain is at the crux of the disorder.\(^{13}\) Evidence suggests that individuals with ADHD have an overly efficient dopamine-removal mechanism in the

---


\(^{12}\) Richards et al., supra note 9.

area of the brain controlling motivation and reinforcement learning. Excessive concentrations of dopamine reuptake inhibitors, the cellular transporters that return dopamine from the synapse back to the neuron which secreted it, remove dopamine from the synapse too quickly, before the neurotransmitter can bind to receptors and transmit its signal. The result of the low dopamine signaling in the brain’s reward and motivation centers is a diminished ability to concentrate and retain information—the major symptoms of ADHD.

Despite the soundness of this model as an explanation for ADHD, scientists have not yet found direct evidence of overactive dopamine reuptake in patients with ADHD. Ironically, the model is primarily premised on the effectiveness drugs, like Ritalin, have on relieving ADHD related symptoms. During the 1950s and 1960s, clinicians began administering these stimulants to patients who reported attention and motivation deficits symptoms, and observed improvements in patients prescribed the medication. Subsequent experiments on model organisms determined that these stimulants produce increased dopamine activity in the brain’s reward centers. Accordingly, the effectiveness of the treatment combined with the physiological effects demonstrated in model organisms led scientists to infer that dopamine deficiency was the underlying culprit behind ADHD pathology.

This uncertainty in ADHD’s underlying mechanism creates a diagnostic quandary: what is the threshold of overactive dopamine reuptake at which an individual has ADHD categorically? ADHD cannot be revealed by blood test or brain scan. Instead, psychiatrists evaluate the manifestation of symptoms empirically, by watching patients, interviewing parents, and conducting questionnaires and psychoanalytical tests. Furthermore, those who do not have ADHD report the same stimulant benefits—of increased concentration and motivation—as ADHD patients do. Indeed, a compelling body of research suggests that the stimulants prescribed to treat ADHD produce heightened attentiveness, working memory, and task saliency in normal adult subjects without ADHD. Hence, the absence of quantitative testing methods for ADHD produces uncertainty arising from subjective testing.

14 Id.
15 Id.
16 Id.
C. Pharmacology of Common Study Drugs

Study drugs generally operate by increasing the activity of the neurotransmitters, primarily dopamine, in the brain. Study drugs exploit their similarity in molecular structure to natural neurotransmitters (Figure 1) and compete with them for the binding sites of enzymes and receptors involved in their biochemical activity. Exploring the mechanism of action of three major classes of study drugs, amphetamines (Adderall), lisdexamfetamine (Vyvanse), and methylphenidate (Ritalin, Concerta) provides ample insight into how they produce the physiological sensations that make them so attractive to college students.

1. Amphetamine (Adderall)

Amphetamine’s mechanism of action is the product of its structural similarity to the monoamine neurotransmitters, dopamine and norepinephrine. These similarities allow amphetamine to compete to bind with monoamine reuptake transporters, NET (noradrenaline transporter) and DAT (dopamine transporter). NET and DAT are protein structures embedded in the cell membrane of presynaptic neurons, responsible for the reuptake of their respective neurotransmitters from the synapse back into the neuron. These transporters bind to their respective monoamine neurotransmitters and facilitate their return to the inside of the neuron. Amphetamine molecules in the synapse compete with the endogenous monoamines for binding spots on the reuptake transporter. When an amphetamine molecule steals a spot on the reuptake transporter, it reduces the number of neurotransmitters transported back into the neuron. Ultimately, the result is in an increased concentration of dopamine and norepinephrine in the synapse, allowing the neurotransmitters increased time and opportunity to bind to receptors and exert their activity on the receiving neuron and cause a transmission.

In addition to inhibiting reuptake, amphetamine also inhibits the action of synaptic monoamine oxidase (MAO), an enzyme (biological

---

19 See Austin, supra note 13.
21 Id.
22 Id.
23 Id.
24 Id.
catalyst) that deactivates monoamine neurotransmitters in the synapse by “clipping off” their amine (NH$_2$) group. Without an amine group, monoamine neurotransmitters are unable to bind to receptors and transmit signals to the receiving neuron. Similarly to how amphetamine competes with natural neurotransmitters for spots in reuptake transporters, amphetamine will also bind to MAOs in place of the natural neurotransmitter, reducing the quantity of free MAOs remaining in the synapse. Therefore, more neurotransmitters remain active in the synapse and have a higher likelihood of transmitting a signal to the receiving neuron.

Amphetamine also exerts activity inside the pre-synaptic neuron itself. The vesicular monoamine transporter 2 (VMAT2) transports newly synthesized monoamine neurotransmitters, located in the cytosolic pool (the fluid inside a cell), into synaptic storage vesicles within the neuron. Amphetamine competes to bind to VMAT2 in place of the neurotransmitters. This initiates a process known as reverse transport, during which newly synthesized cytosolic monoamine neurotransmitters are pumped out of the cell and into the synapse, instead of, into the cell’s intracellular storage vesicle. The result of amphetamine’s intracellular activity is a heightened potency in comparison to other study drugs.

2. *Lisdexamfetamine (Vyvanse)*

Vyvanse is another common ADHD medication and common study drug. Vyvanse is a pro-drug of dextroamphetamine, meaning it is a biologically inactive compound that is metabolized in the body to produce the actual drug. Once the pro-drug is metabolized into its active

26 Heal et al., supra note 20.
27 Id.
28 Id.
29 Id.
amphetamine form, its mechanism of action is identical to other amphetamines such as Adderall.\textsuperscript{31}

Vyvanse, though it produces the same effects as amphetamines, has a more complex structure than amphetamine drugs and is more expensive. The intended benefit accompanying its cost is that it is less susceptible to abuse than the pure amphetamine drug\textsuperscript{32} (though it may still be abused as a study drug). Unlike pure amphetamines, Vyvanse exerts its effects gradually throughout the day, requiring only a single dose.\textsuperscript{33} This is due to the pro-drug also producing the amino acid L-lysine as it metabolizes, which delays the progression of amphetamine through the blood stream and nervous system.\textsuperscript{34} Additionally, Vyvanse will produce minuscule effects if ingested inappropriately via methods such as ingestion through the nostrils because the pro-drug requires gastrointestinal enzymes to metabolize into amphetamine.\textsuperscript{35} Because snorting the drug will bypass this metabolic process, snorting will not transform the drug into amphetamine, making it less likely to be abused as a stimulant.

3. Methylphenidate (Ritalin and Concerta)

Methylphenidate was the first stimulant approved by the FDA in 1955.\textsuperscript{36} Like amphetamines, it increases dopamine and norepinephrine activity by competing with the neurotransmitters for the binding sites on monoamine reuptake transporters. However, Methylphenidate is purely a reuptake inhibitor; unlike amphetamines, it does not inhibit the deactivation of neurotransmitters through MAO or block the storage of neurotransmitters through VMAT2.\textsuperscript{37} The consequence of methylphenidate’s narrower biochemical functionality is a reduced potency compared to amphetamines. More precisely, ten milligrams of the

\textsuperscript{31} See Lisdexamfetamine, supra note 30.
\textsuperscript{32} Id.
\textsuperscript{33} Id.
\textsuperscript{34} Id.
\textsuperscript{35} See id.
brand name methylphenidate, Ritalin, is functionally equivalent to five milligrams of Adderall, the market-leading brand name amphetamine.\(^3^8\)

D. Physiological Effects of Study-Drugs

Irrespective of the difference in mechanisms of action between sub-types, the net result of study drug consumption is increased dopamine and norepinephrine activity in the brain. Due to the colossal range of physiological activities the nervous system regulates through these neurotransmitters, stimulants can generate complex and myriad effects on users.

The immediate effects of study drugs are desirable to students and ADHD patients alike: increased motivation attached to relevant activities, heightened concentration, an amplified pleasure response, and mild euphoria.\(^3^9\) While perhaps an undesirable side effect for ADHD patients, the energy and insomnia associated with these stimulants appeals to students as they prepare to work long hours or stay awake through the night.\(^4^0\)

Study drugs also have additional adverse cardiovascular, neurological, and gastrointestinal effects associated with elevated activity in the nervous system. Cardiovascular effects include hypertension (high blood pressure), increased heart rate, and irregular heartbeat.\(^4^1\) Neurological side-effects may include anxiety, headaches, decreased sexual arousal, dizziness, aggressive behavior, appetite loss, hallucination, and mild tics.\(^4^2\) Gastrointestinal effects include stomach aches, constipation, diarrhea, and weight loss.\(^4^3\) Additionally, users commonly report dry mouth and teeth-grinding.\(^4^4\) Nonetheless, stimulants are relatively safe at recommended medical dosages, with most users reporting only mild undesirable effects from the drugs.\(^4^5\)

---

\(^3^8\) For a detailed comparison of the relative potencies of various ADHD medications, see generally Matt Swenson, *Stimulant Equivalency Table*, UACAP, http://www.uacap.org/uploads/3/2/5/0/3250432/stimulant_equivalency.pdf [https://perma.cc/Z923-EW38].


\(^4^0\) See id.

\(^4^1\) Id.

\(^4^2\) Id.


\(^4^4\) Id.: *The Effects of Amphetamine Use*, supra note 39.

\(^4^5\) See Henry A. Spiller et al., *Overdose of Drugs for Attention-Deficit Hyperactivity Disorder: Clinical Presentation, Mechanisms of Toxicity, and Management*, 27 CNS
At high dosages, study drugs carry a risk of overdose. An overdose is typically associated with extremely high or abnormal heart rate, hypertension, confusion, difficulty breathing, and muscular tremors. A collective manifestation of these side-effects may be deadly if not treated promptly. Nevertheless, national stimulant overdose fatalities are rare, especially in comparison to other drugs.

Study drug abuse may lead to addiction. As users develop a tolerance for these drugs, they may increase their dosage to the point where the likelihood of devolving addiction increases substantially. Also, as study-drug abusers become accustomed to the cognitive boosts that study-drugs deliver, they may become increasingly unable or unwilling to engage in many activities without the aid of study drugs. As research explains, relying on study-drugs may discourage students from developing sustainable study habits, analogously to how reliance on dieting pills often leads consumers to avoid developing long-term weight-loss habits like regular exercise and healthy eating.

III. THE ABUSE OF STUDY DRUGS ON COLLEGE CAMPUSSES

Study drugs have become ubiquitous with college life, with as many as thirty-five percent of college students claiming to have used study drugs for non-medical objectives. The widespread and normalized use of study drugs among college students raises questions as to how students gain access to these drugs and why they engage in their use.

A. Diagnostic Uncertainty and the Diversion of Legitimately Prescribed ADHD Medications Ensures a Steady Supply of Study Drugs

ADHD is the most commonly diagnosed mental health disorder in the U.S., with over ten percent of the entire U.S. population between the

46 See Spiller et al., supra note 45.
47 See id.
48 See id.
49 See id.
50 See id.
51 The Effects of Amphetamine Use, supra note 39.
52 See Arria & DuPont, supra note 2 (describing how dependence can lead to the development of poor self-discipline).
53 This statistic excludes the millions of ADHD diagnosed students who use stimulant medications legally. Besser, supra note 1.
ages of seven and twenty-five currently afflicted.\textsuperscript{54} This diagnosis rate represents a five-fold increase in national ADHD cases since 1990. From 1993 to 2001, Adderall production alone has increased 5,767 percent, and world-wide revenue from all ADHD stimulants has exploded from $1.7 billion in 2002 to $9 billion in 2012.\textsuperscript{55} Up to twenty-nine percent of students with legitimate stimulant prescriptions report that their peers have solicited them to give, sell, or trade their medication, and as many as sixty-two percent of college students with prescriptions divert at least part of their supply to non-prescribed students.\textsuperscript{56} Thus, rising ADHD medication prescription rates ensure that study drugs are readily available on campus.

The dramatic rise of ADHD patients in the U.S. can be attributed to the subjective clinical diagnostic methodology used when testing for the disorder.\textsuperscript{57} There is no objective “normal” amount of dopamine activity from which a negative deviation can be conclusively characterized as ADHD. Instead, ADHD is diagnosed in accordance with the Diagnostic and Statistical Manual, Fifth Edition guidelines (DSM-V).\textsuperscript{58} The guidelines consist of two sets of criteria: (1) inattention and (2) hyperactivity and impulsivity. Each of these categories provides a list of symptoms which are indicative, but not alone definitive, of ADHD.\textsuperscript{59} When a mental health professional concludes that the requisite number of these symptoms are found, she is authorized to categorize the patient as having ADHD and to prescribe stimulants as treatment.

The test for ADHD relies on vague criteria, such as an inability to focus on tasks, fidgeting, or interrupting others that are also common

\textsuperscript{54} See generally Data & Statistics, CDC (Sept. 21, 2018), https://www.cdc.gov/ncbddd/adhd/data.html [https://perma.cc/H8J6-T6NV]. This page contains all the most recent ADHD related statistics as gathered by the Center for Disease Control and Prevention.

\textsuperscript{55} Besser, supra note 1.

\textsuperscript{56} Arria & DuPont, supra note 2; Shaheen E. Lakhan & Annette Kirchgessner, Prescription Stimulants in Individuals with and without Attention Deficit Hyperactivity Disorder: Misuse, Cognitive Impact, and Adverse Effects, 2 BRAIN & BEHAVIOR 661, 665 (2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3489818/pdf/brb30002-0661.pdf [https://perma.cc/ASF7-9HQ4].


\textsuperscript{58} For an in-depth look at the DSM-V guidelines for ADHD diagnosis, see Symptoms and Diagnosis, CDC (Dec. 20, 2018), https://www.cdc.gov/ncbddd/adhd/diagnosis.html [https://perma.cc/K7QL-GAWC].

\textsuperscript{59} This list includes enumerations such as “often has trouble holding attention on tasks or play activities,” “is often easily distracted,” and “often avoids, dislikes, or is reluctant to do tasks that require mental.” Id.
among adults and children who are not affected by ADHD.\textsuperscript{60} Moreover, clinicians, in conjunction with parents who value academic performance,\textsuperscript{61} have adopted a liberal approach to ambiguous ADHD diagnostics, erring on the side of stimulant-based treatment.\textsuperscript{62} Indeed, studies have found that the average time it takes a patient to obtain a positive ADHD diagnosis can be as little as fifteen minutes and that up to twenty percent of ADHD patients may be misdiagnosed.\textsuperscript{63}

The murky nature of ADHD diagnostics enables people without ADHD to receive medication by simulating the symptoms.\textsuperscript{64} Dedicated adults can quite easily deceive a medical professional into believing they have ADHD. As many as ninety-three percent of people succeed in fooling their psychiatrists into prescribing them amphetamine medications.\textsuperscript{65} Cassie Schwartz, a renowned author in the field of developmental neuroscience and psychoanalysis, shared her account of how she obtained an Adderall prescription while a student at Brown:

I went to the nearest campus computer and searched for ‘cognitive behavioral psychiatrist’ . . . . The very next day, I was . . . describing to the young psychiatrist how I had always had to develop elaborate compensatory strategies for getting through my school work, how staying with any one thing was a challenge for me, how I was best at jobs that required elaborate multitasking, like waitressing. Untrue, all of it. I was a focused student and a terrible waitress. And yet these were the answers that I discovered from the briefest online research were characteristic of the A.D.H.D. diagnostic criteria. These were the answers they were looking for in order to pick up their pens and write down ‘Adderall, 20 mg, once a day’ on their prescription pads. So these were the answers I gave. Fifty minutes later, I was standing . . . prescription slip in hand.\textsuperscript{66}

\textsuperscript{61} Arria & DuPont, \textit{supra} note 2.
\textsuperscript{62} See Newmark, \textit{supra} note 60.
\textsuperscript{63} Id.
\textsuperscript{65} Id.
Schwarz easily obtained an Adderall prescription by deliberately feigning the pertinent ADHD symptoms specified in the DSM-V. The conclusions of researchers corroborate Schwarz’s account, finding that for an adult who is determined to gain legal access to ADHD medications, success is very likely.67

Not only can healthy patients feign ADHD, but they can also receive prescriptions from multiple doctors simultaneously.68 While HIPAA laws require physicians to maintain centralized patient records documenting the medications they prescribe, many neglect to reexamine these records when prescribing new medications.69 Bad actors can legally procure a steady supply of study drugs as long as they can find doctors who will prescribe them medication.

Some psychiatrists voluntarily adopt more vigorous diagnostic safeguards to reduce the frequency of ADHD misdiagnosis. These safeguards include extending the length of the sessions and requiring patients to meet with them multiple times before rendering a diagnostic decision.70 Additionally, the psychiatrist will closely monitor the patient after prescribing a stimulant prescription and periodically reassess whether the patient is benefiting from the prescribed medication and using it as intended.71 However, these amplified procedures are not universally followed, and patients are free to “shop” for clinicians with a reputation for quick and liberal stimulant prescription practices.72

ADHD is a chronic mental health condition that can be unduly burdensome if left untreated.73 To many suffering from ADHD, treatment with stimulants is critical to the enjoyment of their daily lives and normal functioning.74 Nevertheless, current ADHD diagnostic methods are vague and easily exploited, ensuring that a legal supply of study drugs is unlikely to subside.

---

67 See Lord, supra note 64.
68 Id.
69 See id.
70 Id.
71 Id.
72 A simple Google search of “how to get an Adderall prescription” reveals forums filled with people recommending doctors with a reputation for stimulant prescriptions.
73 See Lord, supra note 64.
74 Id.
B. Study Drugs Are in Demand Among Students Because of their Perceived Benefit During Studying

Study-drugs are perceived by many students as educational doping, permitting students to prolong study sessions by enhancing concentration, attention, motivation, and wakefulness. Moreover, study drugs induce euphoria and help students relieve stress factors inherent to the educational environment. Abuse rates of study drugs tend to peak during exam periods when students stay up to “cram” for tests and meet impending deadlines on assignments. In general, the majority of students report that abusing study drugs has been helpful to their academic progress. Notwithstanding, a growing body of research suggests that study drugs do not provide a pure boost to a healthy student’s cognitive performance.

Even though study drugs improve studying stamina by keeping students awake, concentrated, and euphoric, these heightened feelings do not necessarily translate into an increased intellectual capacity. A study that examined student performance on reading comprehension and short-term memory tests, found no benefit from study drug ingestion. Another study found that working memory enhancement from study drugs was correlated with an individual’s baseline academic performance, with students who tend to perform well on intellectual tasks benefiting the least from study drugs. Furthermore, studies have found that study drugs do not increase IQ. Thus, study drugs, despite their boost to attentiveness and motivation, are not likely impacting baseline cognitive performance.

75 See Lakhan & Kirchgessner, supra note 56.
77 Id; Lakhan & Kirchgessner, supra note 56.
78 Lakhan & Kirchgessner, supra note 56.
79 See id.
80 See id.
82 Lakhan & Kirchgessner, supra note 56.
83 Id.
The demand for study drug consumption by students is powered by their desire to increase productivity, motivation, and concentration. The universal efficacy of study drugs means that they are advantageous to both students who are struggling to get good grades and to those who are determined to outshine their fellow classmates. Despite data suggesting that study drugs do not increase pure intellectual performance, i.e. they do not make students smarter, the euphoria, sleeplessness, and increased attention they stimulate will likely continue to fuel the demand among students.

C. Study Drug Abuse Avoids Public Scrutiny and Is Perceived as Low-Risk by Students

The prevalence of study drug abuse can be further attributed to the neutral stance taken by society towards illicit study drug consumption and to the low risk many associate with study drug-abuse. A study on media coverage of study drug abuse revealed that ninety-five percent of articles mentioned at least one benefit of study drug abuse, but only fifty-eight percent disclosed the risks or side-effects. Academics say that parents use academic success to justify the abuse of these stimulants:

[Parents appear] to be enabling the problem by turning a blind eye or even encouraging the behavior. Fueled by their concerns about maximizing their child’s academic performance, these parents are highly susceptible to [believing] that, at best, nonmedical use of prescription stimulants might help their child earn better grades, and that, at worst, it is harmless.

Many clinicians share a similar sentiment, seeing study drug abuse as a minor concern, since it is used for a positive aim—studying—and because abuse will likely recede after exams are complete. Many students

---

84 “A web-based survey administered to medical and health profession students found that the most common reason for nonprescription stimulant use was to focus and concentrate during studying.” See Lakhan & Kirchgessner, supra note 56.
85 Id.
86 Id.
87 Arria & DuPont, supra note 2.
88 Id.
perceive study drugs as posing only a mild health risk, especially those who have previously experimented with the drugs.\textsuperscript{89}

Study drugs have managed to circumvent active public disapproval and have failed to incite fear of any serious health risks from users, parents, or clinicians. In fact, the data suggests that the prevailing sentiment is one of passive acceptance.

\textbf{IV. CONCLUSION}

Study drug abuse is a prodigious phenomenon on college campuses across the nation. The ease of accessibility of study drugs coupled with the euphoric and motivational boost they provide users leads scores of students to reach for the “magic” pills in their pursuit of academic excellence.

\footnote{\textsuperscript{89} Indeed, students who have experimented with study-drugs consider the risk negligible. \textit{See} Besser, \textit{supra} note 1.}
Automated Defense Technology

Shelby Smith*

CITE AS: 3 GEO. L. TECH. REV. 492 (2019)

Automated defense technology (ADT) refers to weaponry designed to fend off incoming threats that is typically employed in international combat and utilizes automation in some part of its operation. Because of this automation, ADT removes some human error from warfare, and more recent automation technology allows machines to make certain decisions about engagement without any human input. The goal of this piece is to provide a rudimentary introduction to the concept of, and implications for, automation in defense technology. This paper first explores a brief history of automated weaponry, then it supplies operational definitions for modern ADT, and finally it considers some ethical implications for the future of ADT use and development.

I. The History of Automated Weaponry

As early as the 15th century, Leonardo da Vinci contemplated non-human soldiers. Sketches from his notebooks show designs for a humanless knight capable of human-like movement, designed to be controlled by a system of pulleys.1 However, autonomous weapons were not invented until after the industrial revolution, when functioning blueprints came to exist alongside the development of effective and sustainable power sources.2

The First World War saw enormous growth in automated weapon technology. For example, machine guns, which utilized energy from initial combustion in order to supply the energy to load the next bullet into the

---

* Georgetown Law, J.D. expected 2020; University of Missouri, B.A. 2016.
2 See generally Jimmy Stamp, Unmanned Drones Have Been Around Since World War I, SMITHSONIAN.COM (Feb. 12, 2013), https://www.smithsonianmag.com/arts-culture/unmanned-drones-have-been-around-since-world-war-i-16055939/ [https://perma.cc/9H8Z-R4JJ].
chamber, eliminated the need for soldiers to load and lock each individual bullet, cutting down on wasted time tremendously. Also during this period, engineers in the United States began designing the first unmanned aircraft, a type of technology better known today as drones. In 1918, Charles F. Kettering and Orville Wright developed a quarter-ton unmanned aircraft that could drop a bomb at a pre-calculated point in its flight path. Kettering and Wright calculated how many engine revolutions would occur before the aircraft was over the target location, at which point a camshaft would prompt the expulsion of the bomb. This Kettering “Bug,” however, was never deployed in combat. Furthermore, despite how innovative this type of automation was for its time, automated weaponry remained only mechanical—not digital or software-based. Humans still predetermined any ‘decisions’ that had to be made by the weapons; the technology was simply an extension of a human act.

World War II saw the introduction of much more intelligent and lethal weaponry. Notably, the United States and Britain began utilizing radar in weaponry during WWII. For example, proximity fuses utilized radar to trigger an explosion when the weapon was still twenty to fifty feet in the air. Shrapnel would erupt into the space above the ground, causing much more damage than a typical shell. This was an effective weapon for aircraft flying over the battlefield. Arguably, these weapons were among the first truly automated weapon systems used in warfare because the system inside the shell itself was making the operational decision. The internal radar system triggered the ‘decision’ to explode, rather than a human operator.

The latter half of the twentieth century saw a dramatic expansion in the development of guided missiles. Most modern automated defense technology utilizes features first implemented by guided missile

---

4. Stamp, supra note 2.
5. Id.
9. Id.
10. Id.
11. The next section will discuss more about what constitutes automation in weapons.
technology during the 1950s. Guidance systems found in these missiles perform three crucial functions: navigation, guidance, and control. Navigation technology allows a missile to track its location in space, while guidance and control capabilities allow the missile to continue its course toward the final location and make directional adjustments accordingly. In the mid-1950s, the United States began using the Talos system; this system was a ship-mounted weapons system, deploying missiles capable of course-correcting mid-flight using a homing device. The missiles were directed towards a target by a human actor, but once launched, the missiles themselves corrected for height and distance automatically. Although more sophisticated versions of these missiles are still in use today, the decision-making functions aboard such weapons are not designed to select targets.

The advent of software, the ability of computers to account for microscopic variations in atmosphere, and the discovery of machine learning led to the development of modern automated defense technology. These advances allow weaponry that previously utilized automation in parts of its deployment to become fully automated. Three types of automated weapons, discussed below, are used primarily for defending vehicles, aircraft, buildings (or camps), and ships during wartime: semi-autonomous weapons, human-supervised autonomous weapons, and fully autonomous weapons.

II. OPERATIONAL TAXONOMY FOR MODERN AUTOMATED DEFENSE TECHNOLOGY

“Autonomy” can involve several different machine functions, and the terms autonomous and automated are not particularly helpful in categorizing modern weapons, of which many perform at least some functions automatically. Leading national security scholars suggest that there are multiple dimensions to the concept of “autonomy” insofar as it relates to defense technology. In order to more clearly delineate the

15 Id.
16 This distinction will become important in the next section.
categories of these weapons, this paper adopts definitions set forth by Paul Scharre and Michael C. Horowitz. Scharre and Horowitz describe three theoretical categories of weapons designed to select and engage targets based on the level of human input at different stages of their deployment:

- **Autonomous weapon systems** are those that “once activated, [are] intended to select and engage targets where a human has not decided those specific targets are to be engaged.”

- **Human-supervised autonomous weapon systems** are those that share the characteristics of autonomous weapons, but a human is able to monitor their operations and intervene if necessary.

- **Semi-autonomous weapon systems** “incorporate[] autonomy into one or more targeting functions and, once activated, [are] intended to only engage individual targets or specific group[s] of targets that a human has decided are to be engaged.”

Scharre and Horowitz’s definitions are critical because they clearly delineate levels of human input and culpability. For many, these systems’ significance comes from their capacity to cause injury and destruction to human life and real property to a magnitude not anticipated by the party deploying them. Specifically, a machine that falsely identifies a target, and subsequently makes the decision to eliminate that target, could cause millions of dollars of property damage and inflict needless casualties. When a human plays a decision-making or auditing role in a weapon’s operation, a liable actor can be readily identified in the event of a misfire. Grouping these machines according to their level of decision-making capability is particularly useful for anyone examining the legal and ethical implications of their deployment. For regulators, these categorizations are important tools that focus on who may be held responsible for outcomes, instead of a highly technical categorization system focused only on the functions of the weaponry.

---

18 Id. at 16.  
19 These definitions very closely resemble categorical definitions set out by the United States Department of Defense in a 2012 Directive. Id. at 19.  
20 Id.  
21 Id.  
22 Id.  
A. Semi-Autonomous Weapon Systems\textsuperscript{24}

In the deployment of a semi-autonomous weapon, a human actor selects the target or group of targets. This human decision is the defining feature of this system. The classic example of a semi-autonomous weapons system is guided munition.\textsuperscript{25} These weapons were introduced during World War II and include “projectiles, bombs, torpedoes, and other weapons” that can correct for human error after a human has deployed the technology to locate a specific target or location.\textsuperscript{26} In pre-modern munitions, errors involved in the target acquisition could not be corrected until after the projectile left the control of the human actor.\textsuperscript{27} In modern semi-autonomous weapons, the significant autonomous features of the weapon allow for corrections in flight path after the weapon has left direct human control. In this way, guided munitions are more accurate and generally more cost-efficient than previous projectile weapons.\textsuperscript{28}

In modern warfare, most semi-autonomous weapons include missiles, although their tracking and guidance systems vary greatly between manufacturer and model.\textsuperscript{29} These missiles are classified by the type of termination point they are designed to hit: go-onto-target (GOT) weapons or go-onto-location-in-space (GOLIS) weapons.\textsuperscript{30}

1. Go-Onto-Target Missiles

Go-Onto-Target missiles are fired at a specific target, such as an enemy plane or ship. In this class of missiles, guidance technology varies greatly. Many of these weapons use a radar detection system, housed onboard the weapon, to correct for movement of the target after deployment.\textsuperscript{31} Radar detection functions by sending out radio waves and processing the signals that return after bouncing off of objects in the space around the weapon.\textsuperscript{32} GOT weapons may also use heat-seeking or noise detection technology, which employ sophisticated sensors to measure the

\textsuperscript{24} Some drones, or UAVs, may fall under this category. For the purposes of this paper, I will not be covering the autonomous features of drones.

\textsuperscript{25} Scharre & Horowitz, \textit{supra} note 17, at 8.

\textsuperscript{26} Id.


\textsuperscript{28} Id. at 6.

\textsuperscript{29} See Scharre & Horowitz, \textit{supra} note 17, at 21–23.

\textsuperscript{30} Id. at 9.

\textsuperscript{31} Id.

types of disturbances in the atmosphere.33 Generally, these weapons are aimed in the direction of the target by the human decision-maker and, after deployment, the weapon utilizes the onboard technology to correct for location. This guidance may happen throughout flight or begin as the missile approaches the target.34 This type of weapon may be used to attack both moving and stationary targets, but GOLIS missiles are often alternatively preferred for their accuracy in targeting stationary objects.

2. Go-Onto-Location-in-Space Missiles

For targeting stationary objects, a GOLIS missile is a more accurate weapon because it fixes in on a geographical location. These weapons use a guidance device outside of the missile itself in order to ensure that the designated target is precisely hit.35 Many GOLIS systems communicate with satellite-based global positioning systems during flight in order to arrive at a pre-programmed point on the Earth.36 This technology functions by continuously communicating information to the satellite about wind speed, direction, and height—receiving real time corrections. One significant limitation of these weapons is their dependence on location communications with separate technology. If a satellite were to lose a communication signal for even a fraction of a second, the warhead could diverge from the flight path.

B. Human-Supervised Autonomous Weapon Systems

Human-supervised autonomous weapons are those which select and seek out targets without human command, usually with a human monitoring very closely and able to intervene if necessary.37 This category of weapons makes up what is colloquially called “autonomous weapons” because the weapon makes the ultimate decision about what to target and when to fire, within a set of programmed parameters. These human-supervised autonomous weapons are currently used by the United States and several other military powers.38 All of these systems currently in use are employed to defend a moving object (such as a vehicle or ship) or a non-moving base and are manned by an on-site human monitor.39 Below

33 Scharre and Horowitz, supra note 17, at 8–10.
34 Id.
35 Id.
36 Id.
37 Id. at 12–13.
38 Id. at 12.
39 Id. at 12–13.
are some examples of human-supervised autonomous weapons currently in use.

**US Patriot System**

The Patriot system is a vehicle-mounted missile defense system currently employed by the US Army. The defense system contains an onboard radar system that continually monitors the space around the vehicle, up to 100 kilometers, for potential threats. Once the Patriot system detects a threat, it deploys a missile automatically. The missile is equipped with a target acquisition system that collects real-time data about the target and communicates with the control center for corrections based on the data before collision.

**Goalkeeper System**

The Goalkeeper is a Close-In Weapons System (CIWS) that is mounted aboard ships to destroy incoming projectiles or aircraft. The Goalkeeper detects threats at the surface level by employing advanced radar technology to collect information about the surrounding area, filtering out noise and other impediments, and searching the data continuously. Once the radar detects a threat based on a set of characteristics found in the data, it employs a machine gun able to fire more than 4,000 rounds per minute. The Goalkeeper is also monitored by a human decision-maker, but because the programmed response to a perceived threat is artillery, errors can be costly.

**Iron Curtain**

The Iron Curtain is a CIWS currently in production by Artis LLC, an American developer. While the Iron Curtain’s specific functionality is not yet well-known to the public, it is designed to be portable, attaching to

---

40 Id. at 21.
42 Id.
44 Id.
most vehicles or buildings. The Iron Curtain system continuously monitors its surrounding area for threats and can engage them at extremely high speeds. One of the system’s array of countermeasures utilizes radar and on-site calculations to intercept an incoming threat, causing it to quickly burn up instead of detonating completely and disabling the threat with minimal collateral damage.

C. Autonomous Weapon Systems

Autonomous weapon systems select and engage targets without any direct human oversight. Fully autonomous weapons systems in use or being publicly developed today are scarce. Presumably due to uncertainty about non-human error, many countries are hesitant to add fully autonomous weapons to their arsenals. One example of an autonomous weapon system is the loitering munition. Loitering munitions, which hover over a human-designated area and strike at targets that match specific parameters, are currently only employed in Israel. The Harpy NG, the most commonly used and advanced model manufactured by Israel Aerospace Industries, is designed to attack enemy radar systems. These loitering munitions resemble drones, or UAVs, and can stay in the air for up to nine hours. Because loitering munitions are set up with specific limits to their range, they may offer a model for future development of autonomous weapons that afford an element of control without the need for human monitoring.

III. ETHICAL IMPLICATIONS

On July 3, 1988, a semi-autonomous weapons system mounted to the U.S.S. Vincennes, a United States guided missile cruiser in the Persian Gulf, misidentified an Iranian commercial flight for a fighter jet. The system, which was overseen by a human operator, fired two missiles at the airplane, killing 290 people. At the time, the ship was engaged in a

---

46 Id.
47 Id.
49 Scharre & Horowitz, supra note 17, at 13.
50 Id.
skirmish with an Iranian ship. The misidentification of a large commercial airliner as a small military jet might be attributable to the state of the technology nearly three decades ago, but it raises concerns about how much capability should be given to autonomous weapons systems, even if humans are supervising them.

Many lawmakers’ concerns about automated defense technology can be attributed to unease about a machine making the decision to end a life. In April 2018, military experts traveled to Geneva in order to discuss the future of “killer robots,” in part because many non-governmental organizations (NGOs) fear regulations are not keeping up with the rapid pace of “killer robots” developments. One such NGO, the Campaign to Stop Killer Robots, is lobbying to codify an international statute banning autonomy in target selection and applying violent force among defense technology. Technologically advanced countries like Russia and the United States are reluctant to support the organization.

The Pentagon has dismissed concerns of this type by claiming that any artificial-intelligence-employing weapons system will always have a “man in the loop.” However, thousands of AI and computer scientists including Elon Musk and the late Stephen Hawking anticipate these developments as military resources are being diverted to the study of machine learning. In 2015, those scientists signed an open letter, calling for a “ban on offensive autonomous weapons beyond meaningful human control.” On the other hand, many scholars argue that flat bans are dangerous. Critics assert that autonomy in weapons allows for much less...
human error and collateral damage—which could actually save lives—and a ban would stifle the development of such machines.\textsuperscript{60}

IV. CONCLUSION

Few of the world’s autonomous weapons systems make command decisions, but the potential does pose a question for the future of the intersection of autonomous weapons and artificial intelligence systems. Any fully integrated autonomous weapons technology will need a legal framework for liability and culpability when error inevitably occurs. Logistical safeguards need to be implemented, and humans must always be kept in the loop. The international community has made strides towards a consensus about the acceptability of fully automated weapons in interstate conflict. For now, nations and corporations continue to develop and deploy autonomous weapons across the globe, further delegating decision-making power to these systems.

\textsuperscript{60} Id.
Drones: How They Work, Applications, and Legal Issues

Joseph Suh

CITE AS: 3 GEO. L. TECH. REV. 502 (2019)

I. INTRODUCTION

In 2001, a U.S. military drone, Predator, became the first weapon to stalk and kill an individual on the other side of the planet.1 Controlled from the Central Intelligence Agency (CIA) campus in Virginia, the Predator hovered over a compound in Afghanistan, which housed Mullah Mohammed Omar, an ally of Osama Bin Laden.2 The Predator drone then followed a convoy and fired missiles at the target.3 While not all drones are designed with deadly force in mind, the Predator drone demonstrates the striking extent of drone capabilities.

Drones have become increasingly prevalent throughout the twenty-first century, with their utility spanning from defense applications to recreational filmography. At its core, a drone is an aerial vehicle that flies without a physical person aboard.4 In 1946, the name “drone” was first

---


3 Id.

applied to a radio-controlled aircraft—taking its lineage from the term for a male bee.\(^5\)

This paper discusses how drones work, their applications, and legal issues. Further history of drones is presented in Section II. Section III discusses the functionality and operations of drones, while Section IV delineates the different types of drones. Drone applications are discussed in Section V followed by legal issues in Section VI. Section VII concludes.

II. HISTORY OF DRONES

Although drones have gained attention recently, their origins stretch back over a century. One hundred and twenty years ago, Nikola Tesla controlled an unmanned boat using a remote and radio frequency signals.\(^6\) Drones first became airborne in 1940 when remote-controlled target aircrafts were used to train anti-aircraft gunners for World War II.\(^7\) In 1995, the U.S. military began using the lethal Predator—just six years before it was used to kill Al Qaeda forces at Mullah Mohammed Omar’s compound.\(^9\)

While most of drone history is rooted in military applications, commercial use is now becoming popularized. The French company Parrot released their “AR.Drone” in 2010 as the “first commercially successful ready-to-fly consumer drone.”\(^10\) Just eight years later, in 2018, the Federal Aviation Administration (FAA) announced that the number of commercially registered drones topped one million.\(^11\) In 2017, it was estimated that about three hundred companies were investing in drones, and the market could reach $46 billion by 2026.\(^12\)

---


\(^7\) Id.

\(^8\) See Id.

\(^9\) See Terdiman, supra note 1.


\(^12\) Richard Levick, Drone Industry Just Beginning to Take Off, FORBES (May 15, 2018, 12:44 PM), https://www.forbes.com/sites/richardlevick/2018/05/15/drone-industry-just-beginning-to-take-off/#1f05e3a172bc [https://perma.cc/77SK-UW5E].
III. FUNCTIONALITY AND OPERATIONS OF DRONES

The most common forms of drones contain a set core of components. These include a flight controller, sensors, and an energy source.

The flight controller is the drone’s brain and is central to the control of the drone. The flight controller receives inputs from radio frequency signals from a user as well as signals from various onboard sensors. Accelerometer sensors can be used to determine the position and orientation of the drone in flight, while inertial measurement units sense changes in the drone’s direction. Other sensors may be used to track GPS location or may indicate battery level. All of these sensors feed into the flight controller which uses the sensor signals to determine the speed of the motors in order to control the drone.

The energy sources for drones can vary based on the type of drone in use. In commercial drones, lithium polymer (LiPo) batteries are typically used to power drones because they have high capacities and can deliver the high discharge rate necessary for the drone propellers. LiPo batteries are safe if properly handled; however, they can present a dangerous risk of explosion if a battery is punctured. Alternatively, industrial or military drones may draw power from solar panels or

---

14 See Id.
16 Id.
18 See Corrigan, supra note 13.
19 Id.
21 Id.
gasoline. The military Predator drone contains fuel tanks capable of storing 600 pounds of high-octane fuel—enabling 24-hour flights.

Drones can be fairly autonomous by programming flight paths in advance in place of real-time control. The preprogrammed flight path can be determined by specifying waypoints to travel through, as well as the location and hover duration at each point. For example, if a user wants a drone to fly over a golf course, the user can specify eighteen waypoints for eighteen golf holes. The first waypoint corresponds to the location of the first hole with a height value and hover time duration, while the second waypoint would correspond to the second hole, and so on. The programmed flight path information is stored in the drone controller. Then, once launched, the drone would fly to the first hole using the location data and follow the programmed path. In addition to the autonomous movement, certain drones enable a user to control flights manually by sending the flight control information in real time. This control information is typically sent to drones via radio signal.

IV. TYPES OF DRONES

Most drones take the form of two popular designs: multi-rotor and fixed-wing. Multi-rotor designs function like helicopters, and fixed-wing designs operate like airplanes. These two designs provide different benefits due to the way they maintain flight.

A multi-rotor drone, like the name implies, uses multiple rotors where each rotor consists of two or more rotor blades. The drone contains a motor which rotates the attached rotor blades. In a multi-rotor drone, the rotors are commonly grouped in pairs with two, four, six, or

more rotors. The drone generates the force required to lift the drone upward by the rotating blades. The faster the blades rotate, the more force generated. The absolute and relative speeds among the blades determine the movement of the drone, where a mismatch in the speeds allows the drone to turn. As the rotors have sharp edges and rotate at very high speeds, they can be very dangerous. Therefore, some drones are manufactured with guards around their rotors for safety.

Fixed-wing drones operate like airplanes and, unlike the multi-rotor drone, rely on wings in addition to one or more propellers. The fixed-wing drone’s upward lift is provided by the fixed wings mimicking a regular airplane. Spatial control comes from mechanisms on the wing and body, which “traditionally consist of ailerons, an elevator, and a rudder.” The advantages of the fixed-wing drone include faster speed and longer flying time, but they require runways to take off to reach enough speed to become airborne. While some fixed-wing drones can fly up to twenty-five hours at a time, like an airplane, they cannot stay at a set position in the air. If monitoring a fixed point is needed, a fixed-wing drone must circle around that point. Therefore, these drones are generally used for applications that take advantage of their distance and flight-time, such as the environmental monitoring of a forest and agriculture.

Compared to the fixed-wing drones, multi-rotor drones have shorter flights and range. However, the advantages of the multi-rotor drone come from its low cost, easy control, and runway-free takeoff.


30 Id.


32 See id.

33 Id.


36 Johnson, supra note 34.

37 Id.

38 Module 1 Introduction and Applications, supra note 31.
The traveling speed is slower for a multi-rotor drone, and the distance it can travel is shorter because it needs to use energy to push air down to stay afloat. Therefore, these drones excel in applications that require precise control over a small coverage area such as wedding videography, food delivery, or the delivering of a lifesaver to someone drowning.

V. APPLICATIONS

Drones have become more popular recently, with many individuals and organizations utilizing the technology. Drone utility includes a broad spectrum of applications, from military and police use, to recreational, commercial, and even criminal uses.

One of the most publicized areas is the use of drones by governmental entities such as military and police law enforcement. The military has utilized drones in the past to find and assassinate Al Qaeda forces abroad. Domestically, the United States Customs and Border Protection is currently using drones to monitor borders and intercept trafficked drugs. On a more localized level, police and fire departments are using drones for various purposes, including rescue operations.

39 Johnson, supra note 34.
45 See Terdiman, supra note 1.
46 Id.
traffic management, crime-scene photography, and aerial surveillance of fires.

Outside of the realm of governmental use, the most popular personal uses focus on recreational photography and videography. Drone photos are appealing because the aerial shots from the sky provide new perspectives to familiar landscapes. Outside of photography, drone racing, where drones fly at up to eighty miles per hour, is a new sport that attracts thousands of fans at racing events.

Commercial uses include photography, video, agriculture, delivery, and environmental monitoring. Full operation of Amazon Prime Air is still in the future. Amazon Prime Air is a quick package delivery service that delivers packages in thirty minutes or less.

---

48 Bachman, supra note 44.
49 Id.
50 Id.
using drones. Amazon plans to deploy the service when they obtain regulatory support.

Drone taxis are currently under development. A drone taxi is a regular drone, except that it carries one or more people. After a passenger chooses a destination, the drone would fly to the destination automatically. A Chinese company, Ehang, developed a drone taxi after over a thousand test flights as a new form of aerial transport. Ehang’s drone taxi allows passengers to select any destination within ten miles of its launch point.

Volocopter, a German drone taxi company, also demonstrated a five-minute flight in Dubai—a city which hopes to be the first to provide drone taxi service. Boeing, known as the world’s largest aerospace company, also joined the drone taxi race by completing a short flight of under one minute. The advantages of the drone taxi include a short travel time and no need for a taxi driver. However, the disadvantages include higher risk due to the drone’s airborne nature and the infancy of the technology, the relatively short travel distance, and the need for a landing space.

While there are many legitimate uses for drone technology, drones are now also assisting perpetrators of drug crimes. For example, drone delivery capabilities have been used to transport illicit drugs into prisons. In November 2017, border patrol agents spotted thirteen drones suspected

---

57 Id.
59 Id.
60 Id.
of carrying drugs across one section of the U.S.-Mexico border during just one, four-day period. U.S. agents believe the cartels are aware that the U.S. lacks the ability to detect and intercept in-flight drones. While there are several methods to detect drones, the methods are only effective in short ranges. U.S. Customs and Border Protection has tried a few of these detection systems before and is currently trying another system in Arizona. Even in instances where drones can be detected, the technology to stop them mid-flight are mostly ineffective.

Weapons have been developed and designed to shoot down drones, but they are limited to a range of about one hundred meters. Specially trained eagles have been used to capture drones by Dutch Police, but the program was cancelled due to high costs, small demand, the danger to the eagles, and the potential danger of eagles to the public.

VI. LEGAL ISSUES

Drones can crash from the sky and cause unintended damage as a result of failure or operational errors. When there is harm to individuals or to property, lawsuits and legal issues frequently follow. As a result

65 Id.
69 Id.
of this new and uncharted territory, attorneys specializing in drone issues are in high demand.\textsuperscript{74} The FAA has experience promulgating and enforcing rules and regulations for the sky, but there have also been several private tort cases that involved damages,\textsuperscript{75} injuries,\textsuperscript{76} or class action suits.\textsuperscript{77} Because of the limited case law in this area and complex government regulations, “drone attorneys” have forged a new area of legal specialization.\textsuperscript{78} The questions these attorneys seek to answer involve “permissible operation, civil and criminal liability, misuse, and the like.”\textsuperscript{79}

While the regulatory framework is new and growing, the FAA has stepped in to create rules for drones and drone operators under Part 107 of the Code of Federal Regulations.\textsuperscript{80} Part 107 requires a drone user to register and pay a small fee if the drone weighs more than 0.55 lb.\textsuperscript{81} The requirement is waived for certain circumstances following application and approval by the FAA; such waiver can allow drones to operate outside of

\begin{flushright}
\footnotesize
\footnotesize
\footnotesize
\footnotesize
\footnotesize
77\hspace{1em}Kathryn Rattigan, DJI Drone Manufacturer Hit with Class Action Lawsuit over Firmware Update, DATA PRIVACY & SECURITY INSIDER (Feb. 23, 2017), https://www.dataprivacyandsecurityinsider.com/2017/02/dji-drone-manufacturer-hit-with-class-action-lawsuit-over-firmware-update/ [https://perma.cc/C5K7-YKX7].
\footnotesize
78\hspace{1em}Ricker, supra note 74.
\footnotesize
79\hspace{1em}Id.
\footnotesize
\footnotesize
81\hspace{1em}If I’m Flying My UAS or Drone in My Own Yard, Do I Have to Register It?, FAA, https://faa.custhelp.com/app/answers/detail/a_id/765/kw/General%20UAS%20or%20Drone%20Questions/related/1 [https://perma.cc/U8CD-JAAB]; Welcome to the FAA Drone Zone, FAA, https://faadronezone.faa.gov/#/ [https://perma.cc/HWM2-X9RG].
\end{flushright}
the limits of regulations. Failure to register may result in regulatory and criminal penalties: civil penalties of up to $27,500, criminal penalties of up to $250,000, and imprisonment for up to three years.

In addition to the registration requirements, Part 107 contains further restrictions on the operations of drones. These include limitations on flying drones near airports and stadiums, as well as national parks. To help drone operators navigate the complexities of the regulations, the FAA provides a mobile app called B4UFLY which shows the restricted fly areas based on the operator’s current location. Additionally, other operation restrictions exist, including the requirement to fly at or under 400 feet and to keep the drone within the operator’s line of eye sight.

Unsurprisingly, the FAA drone regulations have been challenged in courts. In 2015, for example, a model aircraft hobbyist named John Taylor challenged the FAA’s registration rule. Taylor argued—among other things—that the rule exceeded the agency’s statutory authority and was arbitrary and capricious. The U.S. Court of Appeals for the D.C. Circuit upheld the regulations in Taylor v. FAA.

The following cases demonstrate regulations on the use of drone technology represent a new and undeveloped area of the law.

In 2015, the FAA sought to fine a drone-photography company, SkyPan International, $1.9 million. The FAA alleged that SkyPan flew

---

88 Taylor v. FAA, 895 F.3d 56, 56 (D.C. Cir. 2018) (upholding the FAA rule).
89 Id at 60.
90 Id at 58.
91 Id.
sixty-five unauthorized flights and lacked the proper certificate and registration for the flights. The parties ultimately settled for a $200,000 civil penalty.

In 2015, a video of a handgun being fired from a flying drone was released by 18-year-old Austin Haughwout. The FAA subpoenaed Haughwout to submit to questioning under oath in a deposition and to produce a wide range of documents related to the video, although Haughwout was not charged with any criminal offenses, since no state law was violated. Haughwout sued the FAA to resist the agency’s subpoena. But he was unsuccessful, and the district court ultimately decided for the FAA.

In the same year, Shawn Usman lost control of a drone, which crashed on the grounds of the White House. Because the drone was so small, only about two feet in diameter, the White House radar system did not detect the drone, exemplifying the difficulty in identifying and deterring errant drone use. The White House initiated a security lockdown, and a Secret Service investigation followed. Usman had to pay a $5,500 fine to the FAA even though federal prosecutors declined to pursue criminal charges against him.

94 Id.
97 Kennedy, supra note 96.
99 Id. at *5.
102 Swarts, supra note 100.
103 Ricker, supra note 74.
104 Swarts, supra note 100.
Federal or state law enforcement agencies can also charge civilians who attack or otherwise damage drones. As of 2016, at least a dozen shootings of drones have been reported, which could constitute a federal crime as aircraft sabotage under 18 U.S.C. § 32. However, the government has yet to pursue a federal charge for damaging drones as aircrafts.\(^\text{105}\) At the state level, however, Russell Percenti was indicted on charges of possession of a firearm after he was tracked down and arrested by police in 2015.\(^\text{106}\) He pled guilty to the charges and admitted that he had fired a shotgun at a drone, claiming he was trying to protect family privacy.\(^\text{107}\) In Kentucky, a similar charge for shooting down a drone was dismissed by a district judge who stated, “[h]e had a right to shoot at this drone.”\(^\text{108}\) In 2019, a man was charged with third-degree criminal mischief after shooting at a drone that was being used to find a lost dog in New York.\(^\text{109}\)

Outside the criminal realm, private suits such as tort cases,\(^\text{111}\) and even a civil class action suit, have been filed against a drone


manufacturer.\textsuperscript{112} The potential for other private law suits with varying causes of action is high. For example, while experts say that “a standard homeowner's policy or optional comprehensive insurance on the car would cover any damages” if a drone damages a house or car,\textsuperscript{113} a lawsuit may still be necessary to resolve liability issues. Further, causes of action, such as a claim for intrusion upon seclusion\textsuperscript{114} may provide victims a private means for enforcement of their privacy rights. Overall, while drones add a new layer of complexity to the law, often the existing set of civil laws can be applied to the new technology.

VII. CONCLUSION

Recently, drones’ adoption, usage across industries, and global awareness have significantly expanded.\textsuperscript{115} The main reasons for this spike in popularity, especially in the consumer market, are low costs and easy controls for the drones. Further, the technology of drones continues to improve due to advances in sensor and stabilizing controller technology.\textsuperscript{116}

Drones are now utilized by a broad spectrum of users from photographers to law enforcement and even drug traffickers. Legal battles have begun to shape the outer limits of drone usage, and the FAA has stepped in with regulations to guide hobbyists and businesses alike. The pace of adoption is not expected to slow, and the use of drones is expected to increase significantly.\textsuperscript{117} Legal issues and cases are likely to increase as well, and, as with any technology, finding the right balance between the legal and technical issues will ultimately impact the future utilization of the drone technology.

\textsuperscript{112} Rattigan, supra note 77.
\textsuperscript{113} Kennedy, supra note 96.