GEORGETOWN LAW TECHNOLOGY REVIEW

VOLUME 1, ISSUE 1

FALL 2016

VOLUME I 2016-2017 ISSUE I

Table of Contents

FOREWORD

A NEW JOURNAL AT THE INTERSECTION OF LAW AND TECHNOLOGY

Marc Rotenberg*

Few issues are of greater need for careful attention today than the intersection of law and technology. And there is no better place to launch such an effort than at the Georgetown Law Center in the nation's capital. Technology is now central to many of the cases before the U.S. Supreme Court, the hearings in Congress, and the workshops at federal agencies. Legal education is itself transformed by technology, creating new paradigms for learning, new sources of information, and new policy issues.

The *Georgetown Law Technology Review* marks the beginning of a journal dedicated to providing Georgetown students and faculty—as well as students, scholars, and practitioners across the country—with the opportunity to explore the intersection of law and technology, to understand the remarkable dialectic that exists at this nexus, and to contribute to the ongoing dialogue that helps makes possible the evolution of our laws and our legal system.

The start of the *Georgetown Law Technology Review* has special significance for me. My first job out of law school was with the Senate Judiciary Committee on a newly formed subcommittee on Technology and Law. Those were the early days of Internet policy, but many of the issues from that era–privacy, IP, consumer security, transparency–seem even more relevant today. With a law degree and a little background in computer science, I found myself at the center of many of the most interesting legal and policy issues of the day. What constitutes a computer crime? Should encryption be regulated by the government? What laws protect innovation? How are privacy laws best designed for a digital world? How can technology promote the transparency of government? A legal education was important to understand the significance of court cases, the drafting of statutes, and the roles of the various branches of governments, but so too was some understanding of technology and, more often, the ability to find the right expert to help assess a complex problem.

* President and Executive Director of the Electronic Privacy Information Center. He joined the Georgetown faculty as an Adjunct Professor in 1990, and teaches the Law of Information Privacy and Litigation Under the Freedom of Information Act. He is coauthor (with Anita L. Allen) of Privacy Law and Society, and maintains the website privacylawandsociety.org.

Translating between the legal world and the world of technology thus became a central task. And once the connection is made between these two domains, our democratic institutions are strengthened as our courts and legislatures make better, more well-informed decisions. We have seen over the last several years the growing interest in promoting this dialogue. From the White House to the FTC, technologists and lawyers work closely together to assess emerging issues and develop policy recommendation. Georgetown law school graduates have worked with the Office of Science and Technology Policy to prepare recommendations for the President, informed by the expertise of scientists and engineers.

And we can anticipate that the demand for lawyers who "speak geek" will continue to grow. Technology is creating enormous opportunity but it is also posing many challenges, in areas from privacy and security to employment and competition. Familiar issues will grow more complex and new issues will emerge. Judges, members of Congress, and White House advisors will all need the ability to understand and assess these developments.

Our legal system thrives when smart, thoughtful lawyers engage in constructive debate about new challenges. We may not always agree about the best outcome–look at the number of closely decided cases at the U.S. Supreme Court–but overall the outcomes will be better with evidence-based analysis that integrates legal and technological expertise.

The *Georgetown Law Technology Review* is destined to become a leading resource for policy innovators.

ARTICLE

LAW OF THE FOAL: CAREFUL STEPS TOWARDS DIGITAL COMPETENCE IN PROPOSED RULES 902(13) AND 902(14)

Hon. John M. Facciola[*] & Lindsey Barrett[•]

CITE AS: 1 GEO. L. TECH. REV. 6 (2016)

http://bit.ly/2gQ2HVA

INTRODUCTION

The Federal Rules of Evidence were originally established to create uniformity in evidence law by providing guidance for every evidentiary problem that could be reasonably expected to occur at a trial. The rules are firmly grounded in the tangible, as courts typically deal with the concrete concerns posed by physical evidence or the testimony of witnesses. But, as our tangible world has grown increasingly virtual, so too has the evidence, creating a diametric switch the existing rules are ill-designed to accommodate. The rules of evidence simply do not speak specifically to the admissibility of digital evidence lawyers and judges now confront. Rules that speak to the written word, testimony, or physical evidence must now be construed and applied to electronic evidence, despite the radical differences between how most evidence was once created, and how it is generated now. The question of how and whether to adapt the rules of evidence for the digital era presents two possible approaches: Does disruptive technology compel a rewriting of existing rules, or are technology-specific approaches to evidentiary issues a solution in search of

[*] U.S. Magistrate Judge (ret.); Adjunct Professor of Law, Georgetown Law. J.D. Georgetown Law, B.A. College of the Holy Cross.

[•] Managing Editor, GLTR; Georgetown Law, J.D. expected 2017; Duke University, B.A. 2014.

a problem, and more likely to create new problems as lawyers and judges struggle to craft new rules for digital evidence?

In May 2015, the Advisory Committee on Evidence proposed Rules 902(13) and 902(14) concerning the authenticity of electronically stored information.[1] While the proposed amendments are not overly ambitious and do not tackle the issue of proof needed to establish the authenticity of all digital evidence under Rule 901, they do embrace certain technological realities that can guide courts into an updated understanding of evidence in the digital age. Rule 902(13) would provide for a certification process for digital information produced by a computer system or process, analogous to Rule 902(11)'s provision for certification of business records.[2] Rule 902(14), governing the self-authentication of copies of electronic information, would allow the authentication of a file by using its hash value, a unique identifier frequently referred to as a "digital fingerprint,"[3] obviating the need for further authentication by witness testimony.[4] The proposed Rules will likely reduce litigation costs spent authenticating information, and help foster judicial efficiency and familiarity with technology. Authentication using hash values will allow courts and lawyers to focus on more pressing issues, and will provide courts with the assurance that presented digital evidence is, in fact, what it purports to be.

The proposed new rules represent a modest step toward updating rules that were created to ensure sufficient authentication of physical documents to meet the needs of an increasingly digital evidentiary landscape. The amendments must, however, be implemented carefully, lest lawyers ignore that ascertaining the authenticity of digital evidence is only the first step in

---

[1] There are two crucial reports on these new rules: (1) Memorandum to Honorable Jeffrey S. Sutton, Chair, Standing Committee on Rules of Practice and Procedure from: Honorable William K. Sessions, III, Chair, Advisory Committee on Evidence Rules, May 7, 2015 *in* JUDICIAL CONFERENCE OF THE UNITED STATES COMMITTEE ON RULES OF PRACTICE AND PROCEDURE, STANDING AGENDA BOOK – MAY 2015, 463–473 (2015) (hereinafter May 2015 Report), http://www.uscourts.gov/rules-policies/archives/agenda-books/committee-rules-practice-and-procedure-may-2015, which provides the text of the proposed rules; and (2) Memorandum to Honorable Jeffrey S. Sutton, Chair, Standing Committee on Rules of Practice and Procedure from: Honorable William K. Sessions, III, Chair, Advisory Committee on Evidence Rules, May 7, 2016 (hereinafter May 2016 Report), http://www.uscourts.gov/rules-policies/archives/committee-reports/advisory-committee-rules-evidence-may-2016.

[2] May 2016 Report, *supra* note 1, at 10.

[3] *See* Simon Garfinkel, *Fingerprinting Your Files*, MIT TECH. REV. (Aug. 4, 2004), http://www.technologyreview.com/news/402961/fingerprinting-your-files/.

[4] *See* May 2016 Report, *supra* note 1, at 12.

determining admissibility. Difficult questions under other evidentiary rules, and in articulating the demands of the right to confrontation persist.[5] But the new rules are, at the very least, a significant start.

THE PROBLEM

The question of how to coalesce new technology with older legal frameworks has produced contradictory approaches, summarized in now-classic form by Professor Lawrence Lessig[6] and Judge Frank Easterbrook.[7] The first would take an exceptionalist approach to applying old laws to new facts, recognizing that disruptive technology frequently compels the construction of new rules to preserve the principles and objectives those rules are intended to serve.[8] The second would critique that approach as unduly hasty and apt to create conflicting, erroneous, and patchwork rules for a world changing too quickly for lawmakers to keep apace.[9] As Judge Easterbrook famously described it, "Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses…[a]ny effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles."[10] The fear of creating a well-intentioned but misguided set of new rules continues to nag lawmakers attempting to adapt existing rules to new facts.

The divide between the two approaches is keenly felt in the evolving world of digital evidence. In his book, *Foundations of Digital Evidence*, George Paul argues that the rules of evidence were premised on a philosophy of empiricism, and the rules that this philosophy generated have nothing to do with how the

---

[5] That the report of a blood test, based on analysis of its contents using computer technology, is authentic has nothing to do with whether the result of the test is scientifically accurate, and whether the defendant should be entitled to call a human being who has certified its accuracy. *See* United States v. Washington, 498 F.3d 225, 232-234 (Michael, J., dissenting).

[6] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 546 (1999).

[7] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F., 207, 216 (1996).

[8] *See* Lessig, *supra* note 6, at 546.

[9] Easterbrook, *supra* note 7, at 207 ("[t]he best way to learn the law applicable to specialized endeavors is to study general rules."); *id.* at 215-16 ("Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us instead do what is essential to permit the participants in this evolving world to make their own decisions.").

[10] *Id.*

modern world assesses the accuracy of its communications.[11] Paul, therefore, argues in favor of a radically different approach to the admission of digital evidence.[12] A competing, Easterbrook-sympathizing school would argue that "if it ain't broke, don't fix it," insisting that the old rules of evidence will work very well with the new technology, as they have worked with information generated by telegraph messages and Xerox machines.[13]

The digital era has therefore created a dramatic issue for courts – how to apply rules and doctrine intended for physical evidence to intangible, digital evidence. The Lessig-Easterbrook fault line divides those, like George Paul, who would completely re-conceptualize and reimagine the rules to deal with a changing evidentiary landscape, and those that want to graft the old rules onto new kinds of evidence. While the battle lines have formed, there is a stalemate. There is no perceptible movement towards the wholesale revision of the Federal Rules of Evidence to deal with digital information.[14] Like it or not, the competent lawyer will largely have to grapple with the Rules as they are, no matter how ill-fitting the applicability of the pertinent Rule and the information being offered. Nevertheless, the proposed new rules are a refreshing step towards a more modern and efficient judiciary for the Information Age.

THE PROPOSED NEW RULES

The Advisory Committee on Evidence Rules has proposed to the Committee on Rules of Practice and Procedure that the Federal Rules of Evidence be amended to add two new rules governing the authenticity of electronically stored information.[15] The proposed rules seem to be a

---

[11] GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 3, 16 (2008). In the interest of transparency, it should be noted that Judge Facciola wrote the forward.

[12] *Id.* at xxv ("We are at a crossroads— a change of phase. With our new information infrastructure, the concept of written evidence has reached a critical tipping point, Judges, professors, students, and thinkers must rewrite the rules.").

[13] Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 172 (2006), http://www.law.northwestem.edu/joumals/njtip/v4/n2/3/J.%20Withers.pdf.

[14] *See* Jonathan L. Moore, *Time for An Upgrade: Amending The Federal Rules of Evidence To Address The Challenges of Electronically Stored Information In Civil Litigation*, 50 JURIMETRICS 148 n. 9 (2010) (*citing* PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 492 (2d Ed. 2008) (noting that "new evidentiary problems faced in the internet age have been directly addressed in few, if any, of these evidence codes")); George L. Paul, *The "Authenticity Crisis" In Real Evidence*, L. PRAC. TODAY, (Mar. 2006), http://www.abanet.org/lpm/lpt/articles/tch03065.shtm ("Certainly no action has been taken by Congress to change the federal rules of evidence to address the recent wave of digitization.").

[15] May 2016 Report, *supra* note 1, at 1.

compromise between the Lessig[16] and Easterbrook[17] schools, and recognize the novelty of this new evidence within the context of traditional evidence law. While the amendments do not deal with the substantive issues as to how digital information is authenticated under Rule 901,[18] they do accomplish two laudable goals. First, the proposed rules create a means of authentication that will relieve the proponent of calling a witness to authenticate the information, if the witness provides a certificate that this information is the product of a process or system that produces an accurate result.[19] Second, they permit a copy of electronically stored information to be admitted if a declarant indicates that she has copied that information from a device, storage media, or electronic file if it is authenticated by what the proposed rule call a "process of digital identification."[20] In the latter situation, the person who derived the copy need not testify; written certification that she made the copy will suffice.[21] More specifically, proposed Rule 902(13) provides that "a record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of 902(11) or 902(12)."[22] Proposed Rule 902(14) provides that "data copied from an electronic device, storage media, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or 902(12)."[23]

Rule 902(13)

The Committee began with the proposition that in the vast majority of cases, the authenticity of electronically stored information is never challenged

[16] Lessig, *supra* note 6, at 546.
[17] Easterbrook, *supra* note 7, at 216.
[18] Rule 901 states that a document is not relevant unless it is what it purports to be and a party must, therefore, produce sufficient evidence to support a finding that it is what it purports to be. For digital evidence that is not self-authenticating, lawyers traditionally use three rules of evidence by: (1) providing testimony from a witness with 901(b)(1); (2) demonstrating that the appearance, contents, substance, internal patterns or other distinctive characteristics of the item, taken together with all the circumstances under 901(b)(4); (3) providing evidence describing a process or system and showing that it produces an accurate result under 901(b)(9).
[19] May 2016 Report, *supra* note 1, at 10.
[20] *Id.* at 12.
[21] *Id.*
[22] *Id.* at 10.
[23] *Id.* at 12.

and it is, therefore, wasteful to insist that a witness come to court to state what is obvious and unlikely to be challenged.[24] On a daily basis, the courts admit into evidence paper documents upon the certification of a custodian, complying with the requirements of Rule 803(6) without any need to call the custodian.[25] Accordingly, electronically stored information should be admitted on the same basis. The Committee, therefore, indicated that its purpose is "narrow: to allow authentication of electronic information that would otherwise be established by a witness."[26] The opposing party, who is entitled to notice of the intention to use such a certification, remains free to challenge the representations made in the certification. The certification suffices only to excuse the witness from appearing if her certification is filed with the court and there is no objection to the authenticity of the evidence as asserted by the certification.

The Advisory Committee provides a series of helpful examples of how the new rule would operate to relieve a party from calling a witness and securing instead the necessary certification from a witness.[27] A party could establish how the iPhone software captures the date, time, and GPS coordinates of each picture taken with the iPhone, permitting the court to conclude that whoever took the picture did so at a particular time and from a particular place.[28] It bears noting that Exif data, the automatically generated metadata indicating, among other things, the date, time and place a particular photo was taken,[29] can be altered—but this is highly unlikely to be the case for the vast majority of cases, and is further counteracted by the requirement that the party certify that the metadata is legitimate.[30] A party could explain how a Samsung phone logs the content date, time and communicating phone that called or was called by the

---

[24] *Id.* at 5.
[25] FED. R. EVID. 803(6).
[26] May 2016 Report, *supra* note 1, at 10.
[27] *Id.* at 7-10.
[28] *Id.* at 7-8.
[29] J.D. Biersdorfer, *Erasing GPS Data from* iPhones, PERSONAL TECH, N.Y. TIMES (Nov. 7, 2016), (explaining how to remove exif data from an image file), http://www.nytimes.com/2016/11/08/technology/personaltech/erasing-gps-data-from-photos.html?ref=technology; *see also*, CAMERA & IMAGING PRODUCTS ASS'N, EXCHANGEABLE IMAGE FILE FORMAT FOR DIGITAL STILL CAMERAS: EXIF VERSION 2.3 31, (December 2012), http://www.cipa.jp/std/documents/e/DC-008-2012_E.pdf (explaining the technical standard for the inclusion of GPS tag in Exif data for digital cameras); *Id.* at 44 (explaining the technical standard for the inclusion of date and time a picture is taken in the Exif data).
[30] Jason Cipriani, *How to view, remove, Exif photo data on your iOs device*, CNET (FEB. 20, 2015), https://www.cnet.com/how-to/how-to-view-remove-exif-photo-data-on-your-ios-device/ (explaining how the date and time an iOS photo was taken, and the location the photo was taken, can be removed using an app).

Samsung phone of text messages that were sent to or from the phone.[31] In each of these instances, the certification of how the electronically stored information was created, transmitted, and stored would suffice to establish authenticity even though the witness was not called. Authenticity is further contingent on the court finding that that the electronically stored information being offered into evidence is what it purports to be (under Rule 901(a)), or self-authenticating (under Rule 902(9)) because the certification establishes that it is the product of a process or system that produced an accurate result.[32]

Rule 902(14)

The proposed rule pertaining to copies of electronically stored information, Rule 902(14), is much easier to apply. The Rule is premised on the fact that it is possible to assign a unique numerical identifier called a "hash value" to electronically stored information by performing calculations on the data within the electronically stored information. It is premised on the incontrovertible reality that each piece of electronically stored information has a unique hash value.[33] The hash value has been referred to as a digital fingerprint because it is a functionally unique and random identifier for a given set of data.[34] The hash value of a file is created when a data string (such as an electronic file serving as evidence) is run through a series of mathematical functions, resulting in a seemingly random string of characters of a fixed length, and much shorter than the input data string. [35] That output is the hash value of the input file, which could have been anything from a simple string of characters to all the files on a hard drive.[36]

Three properties of commonly available hash functions—high collision resistance, high preimage resistance, and high second preimage resistance—make their use the ideal for the authentication of digital evidence. A hash function has a high collision resistance when it would be

[31] May 2016 Report, *supra* note 1, at 8.
[32] FED. R. EVID. 902(9).
[33] *Cf.* BARBARA J. ROTHSTEIN ET AL., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 24 (1st ed. 2007) (defining hash value as "a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set" and providing further background information), http://federalevidence.com/pdf/2008/09-Sept/FJC_%20Managing%20Discovery%20of%20Electronic%20Information.pdf.
[34] Garfinkel, *supra* note 3.
[35] Bret Mulvey, *Hash Functions*, THE PLUTO SCARAB, http://papa.bretmulvey.com/post/124027987928/hash-functions (last visited Nov. 23, 2016).
[36] *Id.*

computationally infeasible (computer science-speak for "almost impossible") for two different inputs, computer files for example, to have the same hash value after the hash function is applied to them.[37] A hash function has a high preimage resistance when it is computationally infeasible to determine the input based on the algorithm and the hash value (such that the hash algorithm is "one-way"); and it is second preimage resistant is when it is computationally infeasible for two different inputs to produce the same hash value.[38] If one uses a hashing algorithm with the three properties mentioned above, it is overwhelmingly unlikely that two pieces of evidence will ever produce the same hash value. The odds of hashing two different pieces of evidence and getting the same hash value is on the order of one in 340 undecillion— or 300 trillion trillion—if using the popular MD5 hash algorithm.[39] Because a hash algorithm is designed to give a complex and highly random output, even a slight change in the input will result in a radically different hash value. This change could be as small as a single pixel added to an image.[40] Comparing hash values makes it easy to identify if the file has been even slightly modified.[41]

The uniqueness of a hash value to a file, the fact that the hash value it is a compact microcosm of the larger file, and the feature that the slightest change to the input will be immediately revealed, strengthens the argument for Proposed Rule 902(14). The Committee extrapolated from the primary premise, namely that authentication using hash values is essentially error-proof, that assigning hash values to original files could provide for a more seamless self-certification process. The odds of a false positive, of the system finding a match because a different file and the piece of evidence happened to share the same

---

[37] NAT'L INST. OF STANDARDS & TECH., RECOMMENDATION FOR APPLICATIONS USING APPROVED HASH ALGORITHMS 6, (2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf ("The longer a hash value is, the more collision resistant it is, as the predicted collision resistance is believed to be half the length of the hash value in bits...").

[38] Mike James, *Hashing – The Greatest Idea in Programming*, I PROGRAMMER, http://www.i-programmer.info/babbages-bag/479-hashing.html (last visited Nov. 23, 2016). While collision resistance and second preimage resistance are similar, they are distinct attributes. *See Second Preimage Resistance vs. Collision Resistance*, CRYPTOGRAPHY STACK EXCHANGE, (Dec. 24, 2014), http://crypto.stackexchange.com/questions/20997/second-pre-image-resistance-vs-collision-resistance.

[39] *See* Rothstein, *supra* note 33, at 24.

[40] Stephen Hoffman, *An Illustration of Hashing and Its Effect on Illegal File Content In The Digital* Age, 22 INTELL. PROP. & TECH. L.J. 6, 10-11 (2010).

[41] Glenn Fleischmann, *Faster Computing Will Damage The Web's Integrity*, MIT TECH. REV. (Oct. 8, 2012), http://www.technologyreview.com/view/429531/faster-computation-will-damage-the-internets-integrity/.

hash value, are infinitesimally low.[42] Hashing provides exactly the proof that Rule 902 requires: that the document is what the attorney states that it is.[43]

Thoughtful Implementation

While the new rules eliminate the unnecessary, there is an obvious concern: Lawyers will seek the path of least resistance and will resort to forms that will simply regurgitate the new rules ("I certify that _____was the result of an accurate system or process"), and move on. But, if the once tangible has become virtual, lawyers and judges will make very little progress if they use these new rules as an excuse not to understand how the underlying technology works. They will fail to realize that the technology properly understood can lead to further advances in creating new rules that will deal with the other issues of authenticity that are based on a forensic evaluation of how computers operate, and create vitally useful information. Forensic technology may answer quickly whether a particular computer produced this electronically stored information because data created by the system itself can answer that question indubitably in particular case.[44] Unless an individual uses a privacy-enhancing technique like Tor,[45] user metadata indicating the time and IP address of a particular user activity took place can be stored by the company operating the application, such as Facebook or Google, or the internet service provider, such as Comcast or AT&T.[46] Should we undertake to create new rules

[42] Robyn Burrows, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 GEO. MASON L. REV. 255, 258 (2011).

[43] The Committee's understanding of how hash values was not precisely correct. Describing the use of hash values for Proposed Rule 902(14), the report tells us that "[a] hash value is a unique alpha-numeric sequence of approximately 30 characters that an algorithm determines based upon the digital contents of a drive, media, or file. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates." May 2016 Report, *supra* note 1, at 12. A hash value is not approximately 30 characters, and in fact the longer it is, the smaller the chance of computational collision–in other words, the more closely authentication approximates the kind of certainty the process is designed to secure.

[44] *See e.g.*, CAT3 LLC v. Black Lineage, Civil Action No. 14Civ5511 (AT)(JF), 2016 BL 7342 (S.D.N.Y. Jan. 12, 2016) (forensic evaluation of metadata proved certain crucial facts); GE Netcom v. Plantronics, Civil Action No. 12-1318 (LPS), 2016 WL 3792833 (D. Del. July 12, 2016) (same).

[45] Kyle Swan, *Onion Routing and Tor*, 1 GEO. L. TECH. REV. 110 (2016).

[46] *See* Kim Zetter, *Google Takes on Rare Fight Against National Security Letters*, WIRED (Apr. 4, 2014, 1:02 PM) (explaining that internet service providers and others can store confidential records about their customers, such as subscriber information, e-mail addresses, websites visited and more).

that more precisely define when forensic evidence can permit the court to conclude that a particular piece of digital evidence is authentic? These rules are arguably only the beginning of a process that will use technological certainty as the only true premise of the authenticity of digital evidence.

Counsel also must realize that a certification of the authenticity of a result is not a certification of its correctness. There are two questions presented when, for example, the report of a breathalyzer is offered into evidence and the resolution of the first, is the report authentic, is, at best, an introduction to the second—did it work? If only the first question is asked and answered we run the risk that the new rules will be completely misconstrued. While Rule 901 speaks of authenticity, a malfunctioning machine cannot produce relevant evidence and, despite the certification, counsel still must call the scientist who performed the analysis if there is reason to doubt that result. Knowing that a report is an accurate reproduction of the results of a process or system is one thing; knowing whether that process or system worked correctly is another.

CONCLUSION

The ultimate implications of hashing for self-authenticating evidence is clear, and the steps that the Committee have taken to move towards a pragmatic understanding of how digital evidence works is promising. Hashing has presented lawyers with a strongly practical alternative to requiring certification of evidence that both computer science and basic statistics declare authentic. The other rule, which neatly equates certification of digital records with the certification of paper business records, is equally sensible and, properly used, can save the time and money spared by avoiding calling a witness who will state the obvious.

But the ambition of these rules is humble. They do not deal with an articulation of the proof needed to establish authenticity under Rules 901 or 902, leaving significant questions of substantive proof still up for debate. Courts will, therefore, continue to apply rules truly designed for paper to electronically stored information. Nevertheless, there is reason for optimism—if the certifications are done correctly, they could illuminate for the court the underlying forensic science that will explain why the evidence being offered can be trusted and relied upon. This is, of course, a welcome alternative to lawyers and courts looking everywhere except the technological basis to determine the authenticity of an email or a Facebook entry. Finally, the use of hash values as the means of guaranteeing that one electronically stored file is the same as its copy is particularly welcome. Time spent attempting to establish that two electronically stored files are identical other than by using hash values

at this juncture is inefficient in both time and cost. Rules 902(13) and (14) are an acknowledgment of the need to reform analog rules for a digital age; while a modest and careful beginning, they are at the very least a modest and careful step in the right direction.

STUDENT NOTE

FROZEN, FANFIC, AND A FLEXIBLE APPROACH FOR FAIR USE IN THE DIGITAL AGE

Cassandra Vangellow*

CITE AS: 1 GEO. L. TECH. REV. 17 (2016)

http://bit.ly/2fFTN8j

INTRODUCTION

Conventional copyright doctrine views copyright from a "top down" perspective where copyright holders possess the power and control over their exclusive rights, expecting potential users to seek permission for any and all protected uses.[1] However, this viewpoint does not map onto what is occurring in our "share this" society. Disney, which is one of the largest and most litigious companies in the world, purposely chose not to pursue individuals posting *Frozen* commentary, interpretations, and parodies on YouTube and other social media platforms. Instead of viewing these uses of Disney-owned material as infringement, this powerful copyright owner views these forms of user

* Georgetown Law, J.D. expected 2017; University of Florida, B.S. Journalism 2014. The author would like to thank Professor Julie E. Cohen for her help in developing, editing, and providing commentary on this piece.

[1] Edward Lee, *Warming up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1459 (2007).

expression as a form of advertising and promotion.[2] Disney's commitment to the new opportunities available through Internet interaction may be best illustrated by its purchase of Maker Studios,[3] which provides the largest content network on YouTube.[4] In recent years, media giant Viacom has also loosened its hold on some of its intellectual property by encouraging the creation of parody.[5] What propelled this momentous shift in behavior on the parts of powerful IP holders such as Disney and Viacom?

Part I describes how current copyright law, especially the damages regime, fails to address user-generated content (UGC) that borrows from or bases itself on copyrighted works. Part II explores how copyright owners are tolerating some UGC, which is creating 'soft' law customs and practices. Part III assesses how informal acceptance of certain practices should result in flexible no-action policies while acknowledging the ethical obligations facing courts, intellectual property attorneys, and their clients.

PART I – COPYRIGHT REGIME IS ILL-EQUIPPED TO ADDRESS CURRENT USES

Personal Use Problem

The public-private dichotomy used to be unequivocal on the face of the law and in practice – users would face potential infringement claims for displays and performances in public and avoid such claims for displays and performances occurring in private.[6] Personal use seemed to reach its apex in the Supreme Court's famous "Betamax" case.[7] As Justice Stevens so eloquently expounded:

> One may search the Copyright Act in vain for any sign that the elected representatives of the millions of people who watch television every day have made it unlawful to copy a program

[2] Chris Osterndorf, *How 'Frozen' fandom changed Disney's stance on copyright infringement*, THE DAILY DOT (May 30, 2014, 8:51 AM), http://www.dailydot.com/opinion/disney-frozen-fandom-copyright-infringement/.
[3] Andrew Leonard, *How Disney learned to stop worrying and love copyright infringement*, SALON (May 23, 2014).
[4] MAKER STUDIOS, http://www.makerstudios.com/about (last visited Feb. 17, 2016).
[5] Nate Anderson, *Viacom's top lawyer: suing P2P users "felt like terrorism,"* ARS TECHNICA (Nov. 16, 2009, 3:22 PM), http://arstechnica.com/tech-policy/2009/11/viacoms-top-lawyer-suing-p2p-users-felt-like-terrorism/.
[6] Julie E. Cohen, *Comment: Copyright's Public-Private Distinction*, 55 CASE W. RES. L. REV. 963, 963 (2005).
[7] Jessica Litman, *Lawful Personal Use*, 85 TEX. L. REV. 1871, 1873 (2007).

> for later viewing at home, or have enacted a flat prohibition against the sale of machines that make such copying possible.

Personal use can be defined as use that an individual makes for herself, her family, or her close friends, which can occur in a range of places, such as at home, at work, or on the street.[8] It can be expected that some personal uses will be clearly legal, some uses will be clearly illegal, and some will operate in a gray area that includes uses neither expressly allowed nor explicitly precluded by existing law. An example of a lawful personal use is a private performance of a copyrighted work.[9] A young woman watching a lawfully acquired digital or physical copy of *Titanic* in her apartment for the umpteenth time will certainly not be pursued for copyright infringement. The limitation of the copyright owner's exclusive rights to distribute, perform, and display various works to the public setting eliminates any concern about this private personal use.[10] In addition, other statutory exemptions and privileges protect users' personal uses, including the distribution and display to the public of owned, lawfully created copies associated with the first sale doctrine.[11] and the ability to modify and produce computer program backup copies.[12]

However, the statutory privileges and exemptions only extend so far, especially as technological development and innovation occur at increasingly faster rates. The internet gives users the opportunity to be news providers, publishers, television networks, movie studios, radio stations, or all of the above, often as part of the collaborative UGC network.[13] This peer production phenomenon allows users to select the activities and tasks they are best suited for, which effectively allocates human capital.[14]

That UGC has been allowed to flourish and be shared has facilitated a burst of creativity in the adaptation arena. The internet features fan fiction for everything from *Grey's Anatomy*[15] to *Harry Potter*, where one wizard-dedicated fan-fiction portal claims to house 84,577 stories and 38,570 authors.[16]

---

[8] *Id.* at 1894.
[9] *Id.* at 1895.
[10] *See* 17 U.S.C. § 106 (2012).
[11] 17 U.S.C. § 109 (2012).
[12] 17 U.S.C. § 117 (2012).
[13] Lee, *supra* note 1, at 1501.
[14] Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369, 376-77 (2002).
[15] FANFICTION.NET, https://www.fanfiction.net/tv/Grey-s-Anatomy/ (last visited Mar. 27, 2016).
[16] HARRY POTTER FAN FICTION, http://www.harrypotterfanfiction.com (last visited Mar. 27, 2016).

Instead of causing harm to a given work, these creative uses are making the original work more valuable by serving as a complement rather than a replacement.[17] These complements are in sharp contrast to succeeding works that borrow from the work's original owner without adding a significant contribution, as demonstrated by the *Harry Potter* fan who attempted to publish a guidebook to the series, predominantly appropriating material directly from author J.K. Rowling's books.[18] Some individuals favoring a staunch copyright regime postulate that copyrighted works have no complements because anything based upon the original work would be a derivative work, which the original owner has the exclusive right to exploit.[19] Alternatively, the stronger argument seems to be that instead of a work being "recast, transformed, or adapted" when a complement is created, a new and distinct work results with associated benefits of this separate identity.[20] While *Fifty Shades of Grey* may be an extreme example because of its commercial success, the series began as fan-fiction inspired by Stephenie Meyer's vampire saga, *Twilight*.[21] It is difficult to argue that an erotic novel emblematic of the "mommy porn" genre should be viewed as a substitute for a young adult novel about vampires and werewolves because the intended audiences and impacts are categorically dissimilar.[22]

Incompleteness of Fair Use

As the law is largely static because of its need to exist in perpetuity, this complicates matters when external changes occur that are not addressed by the law. If we were to use a fair use analysis of a given personal use, we would typically proceed through the four factors: (1) the purpose and character of the

---

[17] Tim Wu, *Tolerated Use*, 31 COLUM. J.L. & ARTS 617, 630-31 (2008).

[18] John Eligon, *Rowling Wins Lawsuit Against Potter Lexicon*, N.Y. TIMES (Sept. 8, 2008), http://www.nytimes.com/2008/09/09/nyregion/09potter.html ("I went to court to uphold the right of authors everywhere to protect their own original work. The proposed book took an enormous amount of my work and added virtually no original commentary of its own.").

[19] 17 U.S.C. § 106 (2012) ("Derivative work" is defined in § 101 as "a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted.").

[20] Wu, *supra* note 17, at 631.

[21] Natasha Bertrand, *'Fifty Shades of Grey' started out as 'Twilight' fan fiction before becoming an international phenomenon*, BUS. INSIDER (Feb. 17, 2015), http://www.businessinsider.com/fifty-shades-of-grey-started-out-as-twilight-fan-fiction-2015-2.

[22] *See id.*

use, focusing specifically on whether the use was transformative, (2) the nature of the involved copyrighted work, (3) the amount and substantiality of the segment used in relation to the copyrighted work as a whole, and (4) the effect of the use upon the potential market or value of the copyrighted work.[23] However, the fair use framework is an inadequate tool for protecting activities "at the core of ordinary uses of copyrighted works,"[24] especially because these uses do not tend to have a commercial purpose or impact the market or value of the copyrighted works. It is difficult to see how the nature of the work and the amount used should cut in the personal use context because the goal is for users to enjoy the copyrighted materials. Legislators and courts seem to forget that for these creative works to mean anything, someone needs to "read the book, view the art, hear the music, watch the film, listen to the CD, run the computer program, and build and inhabit the architecture."[25] Related to the consumption is how people interact, celebrate, and critique these creative works.

Instead of looking to fair use to determine a personal use's lawfulness, the use should be evaluated for where it would fall on a continuum between enjoyment and exploitation. While it can be convincingly argued that technology has generated more avenues and forums for dissemination that can detract from copyright owners' ability to maintain control over their works, new technologies have simultaneously provided these owners with greater abilities to control and prevent unlawful uses. If these technological developments are to preserve the equilibrium between enabling fair use and allowing copyright holders to limit fair use, balance is essential because copyright is supposed to serve and protect both the copyright creators and consumers.[26] Clearly, "A Frozen Father," which is a YouTube parody video based on Disney's blockbuster *Frozen*, is on the enjoyment side of the spectrum.[27]

Copyright owners rightfully have a claim to the profits generated by their creative works. While the copyright system should protect copyright owners from those uses that are capturing the financial gain that should be attributed to the copyright owner, it is questionable whether copyright owners should pursue the average YouTube user classified in the entertainment category who is averaging 9,816 views per video.[28] However, copyright owners

---

[23] 17 U.S.C. § 107 (2012).
[24] Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535, 554 (2004).
[25] Litman, *supra* note 7, at 1880.
[26] *Id.* at 1911.
[27] Andrew Leonard, *supra* note 3.
[28] Carla Marshall, *How Many Views Does a YouTube Video Get? Average Views By Category*, REELSEO (Feb. 2, 2015), http://www.reelseo.com/average-youtube-views/

could express concern about whether YouTube uploaders are getting rich by using the owner's content in mash-up creations because users will make about $2,000 for every one million views.[29] "Sesame Street: Share It Maybe," which parodies the Carly Rae Jepsen song "Call Me Maybe" with lyrics including "Hey, me just met you, and this is crazy, but you got cookie so share it maybe," currently has more than 20 million views.[30] It seems highly unlikely that Jepsen would pursue a case against Sesame Workshop's nonprofit Cookie Monster rendition that celebrates Jepsen's song. Various other groups made parodies of "Call Me Maybe," including the Miami Dolphins Cheerleaders and the Harvard baseball team. A YouTube user transformed Adele's "Hello" into a *Star Wars* video called "Hello (from the dark side)," which features images of Darth Vader and other notable characters and lyrics like "Can't say that I'm sorry, for blowing up Alderaan. We could have ruled the galaxy as father and son."[31] More than 8.5 million viewers have watched this video.[32] While this user utilized copyrighted information owned by Adele and Disney, this still seems to be on the enjoyment side of the spectrum. Although from the user perspective these uses appear to be on the enjoyment side, the value of the generated publicity for the holders should not be overlooked.

However, many examples exist of personal use expanding into exploitation. In *Mattel, Inc. v. Pitt*, the Southern District of New York looked at whether a defendant's use of a Barbie head on another doll wearing sadomasochistic clothing and accessories and being featured in a sexually explicit story constituted fair use.[33] In recognizing the viability of the fair use defense, the court noted the Dungeon Dolls' transformative character as demonstrated by the selected apparel, doll figure, and associated context, as

(Revealing that, on average, How-to and Style videos receive about 8,332 views per video, pet/animal videos receive about 6,542 views per video, people/blogs videos receive 2,354 views per video).

[29] Jim Edwards, *Yes, You Can Make Six Figures As a YouTube Star…And Still End Up Poor*, BUS. INSIDER (Feb. 10, 2014), http://www.businessinsider.com/how-much-money-youtube-stars-actually-make-2014-2.

[30] Brian Anthony Hernandez, *Cookie Monster Stars in Sesame Street 'Call Me Maybe' Parody*, MASHABLE (Jul. 10, 2012), http://mashable.com/2012/07/10/cookie-monster-share-it-maybe/#cvWNXP.44Eqr.

[31] Kate Thomas, *'Hello from the Dark Side!': Star Wars parody of Adele's chart-topping ballad takes the internet by storm*, DAILY MAIL (Dec. 9, 2015), http://www.dailymail.co.uk/tvshowbiz/article-3352692/Star-Wars-parody-Adele-s-Hello-takes-internet-storm.html.

[32] ADELE – HELLO (FROM THE DARK SIDE) [PARODY], https://www.youtube.com/watch?v=UAMyh8DjCrQ (last visited May 14, 2016).

[33] Mattel, Inc. v. Pitt, 229 F.Supp.2d 315, 322 (S.D.N.Y. 2002).

well as the considerable improbability that these altered dolls would ever usurp demand for Mattel's dolls in the toy market.[34] Although the defendant's website provided free access, Mattel may have been victorious in its motion for summary judgment if the defendant earned a profit from the altered dolls. Another close case involved T-shirts and tank tops featuring a copyrighted photo used to comment on the local mayor's desire to terminate the annual University of Wisconsin Mifflin Street Block Party.[35] Due to the T-shirts and tank tops not serving as substitutes for the original photo and because what was ultimately used on the products was a stripped down facial outline that could not receive copyright protection, Judge Frank Easterbrook determined this predominantly personal use fell under the fair use umbrella.[36] This case raises the exploitation question because Sconnie Nation earned a small profit on the sold apparel, and the creators had other options, such as taking their own photo of the mayor instead of using the photographer's copyrighted version.[37] The somewhat conflicting and counterintuitive nature of these cases demonstrate why fair use alone cannot address these expanded personal uses.

Damages and Willful Infringement

Much of the consternation associated with copyright law results from the damages regime. The Copyright Act is notable for granting expansive rights to copyright owners, including its principal vehicle, section 106, which grants holders the broad rights of reproduction, distribution, performance, display, and the preparation of derivative works.[38] However, users' rights are much more restricted as the law delineates exactly what users can do as compared to the copyright holders' expansive rights.[39] For example, if libraries and archives want to engage in any sort of copying so as to avoid infringement, they are allowed to make limited copies (one to three depending on the underlying work), but only if the institutions are open to the public, available to scholars who are part of the library, archives, or institution, or available to people pursuing research in a particular field.[40] The internet introduces new avenues

---

[34] *Pitt*, F.Supp.2d at 324.
[35] Kienitz v. Sconnie Nation LLC, 766 F.3d 756, 758-59 (7th Cir. 2014).
[36] *Id.* at 759-60.
[37] *See id.* at 759-60.
[38] Michael Grynberg, *Property is a Two-Way Street: Personal Copyright and Implied Authorization*, 79 FORDHAM L. REV. 435, 443 (2010).
[39] *Id.*
[40] *See* 17 U.S.C. § 108 (2012) (Limitations on exclusive rights: Reproduction by libraries and archives).

for sharing copyrighted material, while simultaneously compounding opportunities for infringement. However, a disparity exists between user expression, possible infringement, and available copyright remedies because the lines separating these phenomena are blurred and ever-changing based on what users are doing with the protected material.

The copyright system is marked by several developments of the damages regime. An 1856 amendment to the Copyright Act marked a shift in statutory damages because it introduced an available range.[41] As could be expected, resulting damages often did not match the infringement's scope, particularly because of the per-sheet infringement approach. The defendants in *Falk v. Heffron* made 2,400 copies of an infringing photograph, but because they put multiple photographs on 115 sheets, the sustained statutory damages were only $115.[42] *Bolles v. Outing Co.*, which involved a defendant making a photogravure of plaintiff's photograph, resulted in statutory damages of $1 because the plaintiff could only prove that one copy of his work—the photograph—was ultimately sold.[43] These two cases indicate how the damages calculation shied away from its intended purposes: providing full compensation to the copyright holder for any incurred damages and deterring subsequent infringement.[44]

The Copyright Act of 1909 aimed to address the penalizing nature of the per-sheet remedy.[45] The Act distinguished between the compensatory, deterrent, and penal functions for damages by fashioning a new criminal provision to punish infringements that were both willful and profitable and by creating a compensatory regime for when actual damages were difficult to prove.[46] In addition to section 101(b) unequivocally stating that statutory damages "shall not be regarded as a penalty," some courts refused to award statutory damages when actual damages or profits could be shown.[47] However, the legislation also featured the arbitrary and cryptic phrase "as the court shall appear to be just."[48] Although in *F.W. Woolworth Co. v. Contemporary Arts*,

---

[41] Joe Donnini, *Downloading, Distributing, and Damages in the Digital Domain: The Need for Copyright Remedy Reform*, 29 SANTA CLARA COMPUT. & HIGH TECH. L.J. 413, 418 (2013).
[42] Falk v. Heffron, 56 F. 299, 300 (C.C.E.D.N.Y. 1893).
[43] Bolles v. Outing Co., 175 U.S. 262, 268 (1899).
[44] Brady v. Daly, 175 U.S. 148, 154-56 (1899) (Rationalizing that in the event actual damages are difficult to prove, the statutory scheme allows for at least minimum recoveries).
[45] Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 447 (2009).
[46] *Id.* at 444.
[47] *Id.* at 449.
[48] Donnini, *supra* note 41, at 424.

Inc. the infringer only made a gross profit of approximately $900 from the infringing cocker spaniel statuettes, the Court awarded $5,000 in statutory damages.[49] This arguably excessive award appears to be in penalty territory, which is outside the stated purposes of statutory damages.

The Copyright Act of 1976 further complicated the damages issue by combining statutory damages' compensatory and penal functions by calling for limited damages in innocent infringement cases, a broad range for ordinary infringement, and heightened damage levels for willful infringement.[50] The 1976 Act continues to struggle with the awarding of actual damages and profits, when to award statutory damages, and how to address willful versus innocent infringers, which is crucial in the UGC context.

Section 504(b) allows the copyright holder to recover his or her actual damages and any of the profits received by the infringer as a result of the infringing act.[51] Congress viewed actual damages as compensating the copyright holder for losses incurred due to the infringement and the recovery of the defendant's profits as a way to preclude the infringer from unfairly benefitting from a wrongful act.[52] While actual damages and profits may be difficult to assess in some situations, this regime seemed to preserve the idea of making the plaintiff whole.

Although the 1976 Act attempted to constrain statutory damages, it actually expanded their power. Section 504(c) indicates that statutory damages are only available in place of actual damages and the defendant's profits.[53] Online infringement cases often involve statutory damages because the infringement's scope may not be discernible.[54] The 1976 Act attempted to limit statutory damages in several ways, including by limiting the statutory damages remedy to those who register their copyright claims within three months of the copyrighted work's publication, and by providing that infringement of a compilation should be treated as a single work for statutory damages purposes.[55] In another attempt to limit statutory damage awards, Congress adopted a "per infringed work" rule to replace the "per infringement" rule.[56]

---

[49] F.W. Woolworth Co. v. Contemporary Arts, Inc., 344 U.S. 228, 235 (1952).
[50] Samuelson & Wheatland, *supra* note 45, at 444-45.
[51] 17 U.S.C. § 504 (2012).
[52] Donnini, *supra* note 41, at 433.
[53] Samuelson & Wheatland, *supra* note 45, at 451.
[54] U.S. DEP'T OF COM., INTERNET POL'Y TASK FORCE, COPYRIGHT POL'Y, CREATIVITY, AND INNOVATION IN THE DIGITAL ECON.: WHITE PAPER ON REMIXES, FIRST SALE, AND STATUTORY DAMAGES, 70 (Jan. 2016).
[55] Samuelson & Wheatland, *supra* note 45, at 452-53.
[56] *Id.* at 453.

However, this rule fails to map onto content sharing through the Internet and other platforms. Other provisions in the 1976 Act functioned to expand the power of statutory damages. In addition to increasing the statutory damage maximum to $30,000, plaintiffs have the right to elect statutory damages at any time during litigation up until the entry of a final judgment.[57] Section 504(c) also does not include section 101(b)'s language that statutory damages are not supposed to serve a penalty function.[58] Finally, the introduction of a new category of "willful infringers" with a higher damages cap is likely the predominant impetus for the broadening of statutory damages.[59]

While the "innocent infringer" and "willful infringer" labels seem like they would be instructive in awarding statutory damages, they are typically misconstrued. Although section 504(c)(2) references both types of infringers, neither classification is defined in the Act.[60] As the Second Circuit complained in *Fitzgerald Pub. Co. v. Baylor Pub. Co.*, "'[w]illfully' infringing and 'innocent intent' are not the converse of one another. Thus it is possible in the same action for a plaintiff not to be able to prove a defendant's willfulness, and, at the same time, for the defendant to be unable to show that it acted innocently."[61] Innocent infringer and willful infringer are not mutually exclusive terms. As sharing and sampling become increasingly commonplace, it appears that the impermissible line between willful and innocent infringement is only becoming more blurred. While a user might consciously be selecting to include part of a Beyoncé or Jay-Z song in a video mash-up, whether this user is willfully infringing a protected right involves another determination that the current framework does not address.

Unfortunately, the innocent infringer provision, which gives courts the discretion to reduce a statutory damages award to a minimum of $200,[62] is effectively useless for defendants.[63] This is primarily because courts are extremely strict about defendants indicating both a good-faith belief that their conduct was non-infringing and that the defendants had a reasonable basis for that belief.[64] Only two cases involve a court awarding statutory damages in an amount lower than the ordinary infringement minimum.[65] The Southern District

[57] 17 U.S.C. § 504 (2012).
[58] Samuelson & Wheatland, *supra* note 45, at 457.
[59] *Id.* at 458.
[60] 17 U.S.C. § 101 (2012).
[61] Fitzgerald Pub. Co., Inc. v. Baylor Pub. Co., Inc., 807 F.2d 1110, 1115 (1986).
[62] 17 U.S.C. § 504(c)(2) (2012).
[63] Samuelson & Wheatland, *supra* note 45, at 452.
[64] *Id.* at 475 n.174.
[65] *Id.* at 474-75.

of New York levied a $100 statutory damages award against a small shop for unknowingly selling infringing toys, but the damages reduction was likely a result of the inappropriate tactics of the plaintiffs' lawyer.[66] In *D.C. Comics, Inc. v. Mini Gift Shop*, the Second Circuit affirmed a $200 statutory damage award against a defendant who did not have the business acumen or notice that the copyrighted works were infringing.[67] Although it would seem that many users, particularly those expressing themselves in a non-commercial way, could qualify as innocent, this is not shown in the case law.

Willful infringer was supposed to apply to "exceptional cases" involving repeat infringers, counterfeiters, and the like, but recent case law indicates that this undefined term is resulting in arbitrary and excessive damages awards.[68] In *Capitol Records, Inc. v. Thomas-Rasset*, the three separate trials yielded statutory damage awards of $222,000 (equates to $9,250 per work), $1.92 million (equates to $80,000 per work), and $1.5 million (equates to $62,500 per work).[69] *Sony BMG Music Entertainment v. Tenenbaum* also resulted in a high damages award; although the district court claimed the $675,000 statutory damages amount was excessive and unconstitutional, the appellate court reinstated the original award.[70] The First Circuit reasoned that if Congress contemplated a commercial/non-commercial user dichotomy, it would have indicated this distinction expressly as it did in the Sound Recording Act of 1971 and the Audio Home Recording Act of 1992.[71] *Maverick Recording Company v. Whitney Harper* involved a high school student who downloaded thirty-seven songs from a file-sharing program, infringing several labels' copyrighted sound recordings.[72] Unfortunately for Harper, she could not invoke the innocent infringer defense. Section 402(d) of the Copyright Act states that if the published phonorecord includes a copyright notice, "then no weight shall be given to such a defendant's interposition of a defense based on innocent infringement in mitigation of actual or statutory damages."[73] The court did not grant much credence to the fact that while the plaintiffs included the requisite copyright notice on their physical CDs and other physical embodiments of the

---

[66] *Id.* at 475 (*citing* Warner Bros., Inc. v. Dae Rim Trading Inc., 677 F. Supp. 740 (S.D.N.Y. 1988)).
[67] *Id.* at 475 n.175.
[68] *Id.* at 459.
[69] WHITE PAPER ON REMIXES, FIRST SALE, AND STATUTORY DAMAGES, *supra* note 54, at 71 n.414.
[70] Sony BMG Music Ent. v. Tenenbaum, 660 F.3d 487, 509 (1st Cir. 2011).
[71] *Id.* at 499.
[72] Maverick Recording Co. v. Harper, 598 F.3d 193, 195 (5th Cir. 2010).
[73] 17 U.S.C. § 402 (2012).

music, they did not include such notice on the downloadable recordings infringed by Harper.[74]

Although ignorance of the law is no excuse, and the public is much more aware of copyright because of the Grokster and Napster litigation, the damages framework treats UGC creators in a draconian manner. While creative expression that is seen as honoring or celebrating a work by contributing something new is likely to be viewed as not harmful, courts are still unlikely to view this behavior as innocent. This is especially true if defendants cannot formulate a reasonable basis for their belief that their activity was not infringing. This harmless conduct is distinct from deliberate infringement that shows an awareness of protection coupled with a blatant attempt to avoid the ramifications, such as uploading an entire copyrighted work to BitTorrent.[75] While the BitTorrent user should be subject to the penalties associated with this willful action, users' actions are unlikely to be either objectively innocent or expressly willful. A mismatch exists between user action and potential damages exposure, and the pre-Internet framework must be changed to account for all involved stakeholders.

PART II – USER-GENERATED CONTENT, TOLERATED USES, AND THE EMERGENCE OF A SOFT LAW FRAMEWORK

UGC opportunities have exploded with the growing interactive capabilities of the Internet, and this content is a major contributor to the development of tolerated uses and the emerging non-enforcement norms. UGC can be separated into two main categories: (1) pure UGC where all content is produced by the user and (2) mashup/remixed UGC, which involves the user's content being mixed with content created by others.[76] This paper does not implicate the first category because the user has not taken material from copyrighted works, thus eliminating the copyright infringement concerns. However, mashups are concerning because they may infringe the copyright holder's exclusive rights protected by the Copyright Act.[77] UGC is rampant in the computer game industry because the gaming community encourages "modding," which is where players alter the original games.[78] Sega, a video

[74] Donnini, *supra* note 41, at 440-41.
[75] Interview with Michelle M. Wu, Law Library Director and Professor or Law, Georgetown University Law Center (Mar. 30, 2016).
[76] Lee, *supra* note 1, at 1506.
[77] *See id*. at 1509.
[78] Rafi Letzter, *Online communities are changing video games to make them better, weirder, and much more wonderful*, BUS. INSIDER (Jul. 20, 2015, 11:49 AM),

game and hardware development company, is now allowing users to modify and redistribute user-augmented versions of classic games.[79] Users also produce movie trailers through a combination of studio-released footage and other creative contributions.[80] Although using copyrighted material, user-created trailers may benefit the movie studios by manifesting what aspects of a movie that fans deem to be particularly salient.[81] Users uploading lip-sync and lip-dubbing versions of popular songs, such as Harvey Danger's "Flagpole Sitta," raises complex copyright questions.[82] Parodies are also complicated because, in order to be successful in making a point, they must use a good amount of the original work. At the same time, parodies tend to be less likely to displace the market for the original material because consumers are much less likely to buy the criticizing version if they actually want the original. Consider the fan who reimagined the dramatic thriller *The Shining* into a romantic comedy.[83] *The Shining* is not likely to receive reduced viewership because of this parody. A fan of the video game *Mass Effect 2* and Donald Trump created a parody called the "Trump Effect" that the presidential candidate endorsed by circulating on social media.[84] Although these mashups implicate copyright, rights holders and the existing framework are struggling with how to address UGC.

The tolerated use moniker, which can be applied to the technically infringing yet nonetheless tolerated uses of protected works, is contributing to the emergence of a soft law framework that attempts to fill in copyright law's gaps. These uses are largely tolerated because of the mass quantity of use combined with low value ascribed to each transaction.[85] In allowing these

---

http://www.businessinsider.com/video-game-modding-2015-7 (Enabling players to fix bugs, update graphics, bring in new elements, and generate new games).

[79] Kyle Orland, *Sega embraces legal console game modding with new Genesis PC emulation hub*, ARS TECHNICA (Apr. 20, 2016, 5:45 PM) http://arstechnica.com/gaming/2016/04/sega-embraces-legal-console-game-modding-with-new-genesis-pc-emulation-hub/.

[80] Grace Chung, *Five Best Fan—Created Movie Trailers on the Web*, ADVERT. AGE (Jul. 24, 2014), http://adage.com/article/digital/fan-made-movie-trailers-web/294268/.

[81] Jacqueline D. Lipton, *Copyright's Twilight Zone: Digital Copyright Lessons from the Vampire Blogosphere*, 70 MD. L. REV. 1, 37-38 (2010).

[82] Marc Hogan, *Mime Crime: Capitol Sues Vimeo Over Lip-Sync Videos*, SPIN (Sept. 20, 2013), http://www.spin.com/2013/09/vimeo-lip-sync-copyright-lawsuit-capitol-records-dmca-safe-harbor-1972/.

[83] neochosen, *The Shining Recut* , https://www.youtube.com/watch?v=KmkVWuP_sO0, YOUTUBE (last visited May 14, 2016).

[84] Tim Hains, *Donald Trump Posts Over-the-Top Cinematic Fan-Made Campaign Ad: "The Trump Effect,"* REAL CLEAR POL. (Apr. 4, 2016),
http://www.realclearpolitics.com/video/2016/04/04/donald_trump_posts_cinematic_the_trump_effec t_parody_campaign_ad.html.

[85] Wu, *supra* note 17, at 617 (2008).

tolerated uses, owners are likely motivated by a variety of incentives and disincentives, such as enforcement costs, the desire to formulate goodwill, and the determination that the use generates an economic complement to the copyrighted work.[86] Just as Carly Rae Jepsen has little incentive to sue Sesame Workshop, bringing an action against Harvard University and the Miami Dolphins would be extremely costly, both in terms of legal fees and negative publicity. Additionally, these videos appeared to highlight and promote Jepsen's work by drawing increased attention to the original song and lyrics.[87]

Although this practice of tolerated use began in science fiction and other niche areas, the strategy expanded to the higher revenue arenas of television, movies, and fictional works because of the Internet.[88] Today, this strategy is often employed by companies that have an entire portion of their legal department dedicated to searching for copyright and trademark infringement, yet these owners often deliberately decide not to sue and may actually "hype" the uses as a way to monetize other branding opportunities.[89] Even Disney, a notoriously litigious company, is viewing viral videos for *Frozen* as free advertising.[90] Disney will likely continue its strategy of non-enforcement with its other works, especially *Star Wars*, because of creator George Lucas' emphasis on open access and sharing throughout his career.[91] Rj Idos, who is the content creator of Idos Media, created "Taylor Swift – Shake It Off Disney Style" and "Disneyfied Star Wars."[92] Although these videos geared toward children and young adults respectively have more than 19.5 million and 57,000 views, no one affiliated with Taylor Swift or Disney contacted Idos Media

---

[86] *Id.* at 619.

[87] Email Interview with Anne Gilson LaLonde, Author, GILSON ON TRADEMARKS (May 6, 2016) (Explaining in the trademark context, the explosion of new domain name extensions is causing trademark owners to reevaluate their priorities because it is impossible to stop all mark uses and variations in all spaces. The trademark owners are also cautious about not offending those who have so much affection for a brand that they create their own fan websites and other creations).

[88] Interview with Michelle M. Wu, Law Library Director and Professor or Law, Georgetown University Law Center (Mar. 30, 2016).

[89] *Id.*

[90] Chris Osterndorf, *How 'Frozen' fandom changed Disney's stance on copyright infringement*, THE DAILY DOT (May 30, 2014, 8:51 AM), http://www.dailydot.com/opinion/disney-frozen-fandom-copyright-infringement/.

[91] Interview with Michelle M. Wu, Law Library Director and Professor or Law, Georgetown University Law Center (Mar. 30, 2016).

[92] Idos Media, YOUTUBE: IDOS MEDIA, https://www.youtube.com/channel/UCuXy7lKIoAVWDU4WI0EzPOw (last visited May 15, 2016).

regarding its UGC.[93] Idos explained that while the Channel generates some income through Google AdSense, whatever is earned is used for song studio fees, costume rentals, and other costs that go toward the creation of more videos.[94] Users' experiences with copyright owners vary greatly. Although Universal Music Group contacted YouTube user John Smith[95] about ownership of the song used in his video, which has more than 24 million views, UMG chose to profit from the video by keeping it available on YouTube.[96] For the same video, Disney reached out to Smith and coordinated a trip toCalifornia, a private studio tour, and a professional audition.[97] While Smith acknowledges that none of his subsequent videos have been as popular as the initial video that caught Disney's attention, the small amount of income he earns goes into the creation of additional impression videos.[98] Although liability likely exists for many of these tolerated uses, a policy of non-enforcement seems to be coalescing.

While some have hypothesized a chilling effect from uncertainty in how owners and the copyright system will ultimately address these uses,[99] it appears that if anything, a 'warming phenomenon' is taking place, where "users make unauthorized uses of copyrighted works based on the belief that it is acceptable because it is a larger-scale practice engaged in by others."[100] This phenomenon can be classified as a bandwagon effect – if users see other people in the marketplace engaging in these practices that are either ignored or encouraged by the copyright owners, they take these indicators as a sign that the behavior is legitimate and proceed accordingly.[101] If users see that the Idos Media and John Smith videos remain on YouTube and continue to receive views and positive feedback, they are likely encouraged to create their own content. This warming is likely a major contributing factor for why blogs, fan-fiction creations, and other mashups have grown at such an expeditious rate.[102]

Gap fillers that serve as "soft law" are addressing gray areas by establishing acceptable practices among the involved parties.[103] In some circumstances, copyright holders like to hedge by adopting a "wait and see"

---

[93] Email Interview with Rj Idos, Content Creator, Idos Media (May 4, 2016).
[94] *Id.*
[95] Name has been changed at the creator's request to remain anonymous.
[96] Email Interview with John Smith, Content Creator (May 3, 2016).
[97] *Id.*
[98] *Id.*
[99] Michael W. Carroll, *Fixing Fair Use*, 85 N.C. L. REV. 1087, 1148 (2007)
[100] Lee, *supra* note 1, at 1544.
[101] *Id.* at 1545.
[102] *Id.*
[103] *Id.* at 1462-63.

approach for how their works will be used.[104] Companies, including Apple, may appreciate and celebrate what users generate, even if what the users do technically infringes and violates the owners' intellectual property rights.[105] Even if a company wants a particular activity or behavior to cease, the UGC can still provide informative case studies for what is occurring in the marketplace.[106]

Five factors that make the development of an informal copyright practice more likely and legitimate include: (1) absence of litigation and settled case law deeming the practice to be an infringement, (2) existence of a novel issue of law, (3) colorable defense or exemption potentially available, (4) high transaction costs in obtaining permission or formal licenses, and (5) no express objection by the rights holder.[107] Before delving into the UGC context, tolerated use developing into informal copyright practice is seen in other areas of the law. Photocopying for personal use is a prime example of how a practice outside of the law's strict confines has developed into an informal practice. First, the case law is unsettled because of the existing Supreme Court split in *Williams & Wilkins Co. v. U.S.* about whether limited photocopying should qualify as fair use; second, although a commonly known practice, the limited library photocopying exemption does not mention individuals; third, fair use seems like it would be an appropriate affirmative defense of this practice; fourth, obtaining permission before making any personal photocopies would be a time consuming and likely unsuccessful endeavor; fifth, copyright holders failed to decry this practice when it first began and have generally ignored it.[108] This is in contrast to the unauthorized sharing of music files, which is an illegitimate practice that copyright holders continue to combat. First, record labels and music industry stakeholders pursue thousands of lawsuits against individuals and other entities related to this practice; second, this practice is widely disfavored and generally recognized as infringement; third, existing law clearly establishes that fair use and other defenses do not apply; fourth, inexpensive music files are available, which eliminates arguments about prohibitive

---

[104] *Id.* at 1486.

[105] *See* Stuart Elliot, *Student's Ad Gets a Remake, and Makes the Big Time*, N.Y. TIMES (Oct. 25, 2007), http://www.nytimes.com/2007/10/25/business/media/26apple-web.html?_r=0 (Revealing how Apple worked with user to professionalize a commercial originally uploaded to YouTube).

[106] *See* Sam Savage, *"SNL" skit puts YouTube on map,* REDORBIT (Mar. 21 2006), http://www.redorbit.com/news/entertainment/436839/snl_skit_puts_youtube_on_map/ (Discussing how NBC introduced YouTube largely because of uploaded "Lazy Sunday" clip, which was a parodic rap about *The Chronicles of Narnia*).

[107] Lee, *supra* note 1, at 1494.

[108] *Id.* at 1496-97.

transaction costs; fifth, the major labels and the Recording Industry Association of America maintain strong public positions against this practice.[109]

Applying these factors to modding, trailers, lip syncs, and parodies indicates how these UGC activities are emerging into generally tolerated informal copyright practices. First, although various jurisdictions have addressed modding, the jurisprudence is largely unsettled because of the wide variation of modding techniques.[110] Partial modding, which includes tweaks to the game's storyline and characters like what was at issue in *Micro Star v. FormGen. Inc.*, is viewed as an infringing derivative work,[111] but total conversions, which focus on the game's functional elements instead of the creative content, unsettle the modding case law.[112] Second, modding began more than thirty years ago when players started manipulating circuit boards,[113] but enhanced technological capabilities now allow players to completely replace a game's artwork, characters, plot, story, and music.[114] Third, as total-conversion modding depends on a game's functional aspects, a strong argument exists for why this practice should be distinguished from the partial mods that are designated as derivative works. Even if courts find that total-conversions are derivative works, fair use would be an appropriate defense to raise as these versions transform the game's content, the emphasis is on the game's functional aspects not the artwork, only the underlying functionalities are being utilized for modding, and the market for the original game is unlikely to be usurped.[115] Fourth, while a licensing regime exists that may provide source code and other networking details,[116] end user licensing agreements tend to include boilerplate language that limits users' modding abilities.[117] Fifth, although some copyright holders expressed their objections through litigation, Sega's Mega Drive

---

[109] *Id.* at 1497-98.

[110] Note, *Spare the Mod: In Support of Total Conversion Modified Video Games*, 125 HARV. L. REV. 789, 802-803 (2012).

[111] *Id.*

[112] *Id.* at 808.

[113] Midway Mfg. Co. v. Artic Intern., Inc., 704 F.2d 1009, 1010-11 (7th Cir. 1983) (Holding defendant's selling of circuit boards that speed up *Galaxian's* sounds and images violated plaintiff's copyrights because boards created a derivative work).

[114] *Spare the Mod*, *supra* note 110, at 789.

[115] *See id*. at 806-10; *see also* Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1523 (9th Cir. 1992) (Emphasizing how video game players generally purchase multiple games).

[116] David B. Nieborg & Shenja van der Graaf, *The mod industries? The industrial logic of non-market game production*, 11 EUR. J. CULTURAL STUD. 177, 183-84 (2008).

[117] Dorisa Shahmirzai, *Why License Video Games?*, HG.ORG LEGAL RESOURCES, http://www.hg.org/article.asp?id=31519 (last visited Oct. 05, 2016).

Classics Hub encouraging the sharing of modified versions demonstrates this informal practice may become more common and supported by other owners.[118]

Fan-created movie trailers follow a similar trajectory to that of modding. First, little to no litigation has addressed this practice likely because of its promotional appeal at no additional cost for the movie studios. Second, this practice is somewhat novel, especially because it can also involve a hybrid creation where fans combine their own contributions with stock images and video, such as the Harry Potter inspired trailer for *Voldemort: Origins of the Heir*.[119] This trailer begins with a banner message: "The following fan film was created with no intention of profit. The character of Voldemort and his likeness are exclusive properties of Warner Brothers Entertainment Inc. and J.K. Rowling."[120] Third, even without a blatant message, it seems like these noncommercial enterprises could raise a fair use defense. A fair use defense is more likely to be successful when the trailer involves a larger ratio of UGC to protected material. Fourth, obtaining permission or formal licenses is a complicated process that is likely to be cost prohibitive for fans and users. For example, users interested in using Walt Disney Studios clips and stills must fill out a detailed form about the requested programming and specifics about how Disney's materials will be used.[121] Separate Disney employees serve as the contacts for different programming, which presumably complicates the process for users wanting to access clips and stills of various types[122] Fifth, while owners, such as *Twilight* author Stephenie Meyer and film company Summit Entertainment, maintain the ability to go after fans who create misleading trailers, overall the fan-created trailers are left alone for public consumption.[123]

---

[118] Daniel Sheridan, *Get Ready to Load the Sega Mega Drive Classics Hub*, SEGA (Apr. 20, 2016), http://www.sega.co.uk/news/sega-mega-drive-classics-hub.

[119] Sam Haysom, *'Harry Potter' fans create epic trailer for film about Voldemort's school days*, MASHABLE (Mar. 15, 2016), http://mashable.com/2016/03/15/voldemort-film-trailer/#MmLzGfIZPmqk.

[120] Brinton Parker, *This Voldemort Origin Story Looks Like the Coolest Harry Potter Film Yet*, POP SUGAR (May 9, 2016), http://www.popsugar.com/tech/Voldemort-Origins-Heir-Fan-Film-40940848 (Complicating the fair use argument is the creator's Kickstarter campaign that has raised more than $15,000).

[121] THE WALT DISNEY STUDIOS, http://disneystudiolicensing.com/ (last visited May 14, 2016).

[122] *Id.* (listing individual contacts for Television content (1955-1984) and motion picture content, Disney/ABC Domestic Television, ABC Library – Pre-1985, ABC Studios (Current Programming – Promotional Footage), ABC Library – Post-1985, ABC Primetime Reality, ABC Daytime, ABC Touchstone (SCHOOLHOUSE ROCKS!), ABC Family, ABC News, ABC News Videosource Stock Footage Library, KABC-TV (Los Angeles), Still Images – Archive, Still Images – Current).

[123] Lipton, *supra* note 81, at 37-38.

Lip syncs and lip dubbing are another area where fans and users are contributing to the creation of an informal practice, particularly because the publishing of this behavior is somewhat novel and appears to qualify for fair use protections. First, lip syncing case law is unsettled, especially because Capitol Records' case against Vimeo is currently being appealed.[124] Capitol Records took issue with the lip-dub videos housed on Vimeo that show fans mouthing the words to various copyrighted songs.[125] Second, the practice is novel and complex largely because it also has ramifications for the Digital Millennium Copyright Act safe harbor provisions that aim to protect the platforms, such as Vimeo, as long as they remove the infringing content.[126] Third, these lip sync videos are prime candidates for a fair use defense because users are often attempting to create a transformative work that lacks a commercial purpose. Fourth, although identifying and negotiating with copyright owners currently imposes high transaction costs, a micro-licensing platform that would create a one-stop licensing shop is currently in development by the recording and music publishing industries.[127] If such a platform were to come to fruition, an informal lip sync practice would presumably be replaced. Fifth, apart from Capitol Records, copyright holders have not vehemently expressed objection to this lip sync practice likely because it is generally harmless to the underlying copyrighted work.

Although the Supreme Court's decision in *Campbell v. Acuff Rose Music* remains the authoritative precedent on parodies, this case is not necessarily instructive in the UGC context because it involved a commercial parody. First, many of the fan-created parodies are made for pure entertainment purposes without a profit motive, such as "Brokeback to the Future," a parody that utilizes the music from *Brokeback Mountain* to tell a love story between Doc Brown and Marty McFly.[128] Second, while fan-created parodies are not a recent development, many of these parodies involve mash-ups that may implicate multiple works and different copyright holders.[129] Third, creators would likely be able to raise a fair use defense, especially if the parody's

[124] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 537, 556 (S.D.N.Y. 2013).
[125] *Id.* at 546.
[126] Al Newstead, *Lip Sync Videos Targeted in Major Copyright Lawsuit*, TONE DEAF (Sept. 13, 2013), http://www.tonedeaf.com.au/347008/lip-sync-videos-targeted-in-major-copyright-lawsuit.htm.
[127] WHITE PAPER ON REMIXES, FIRST SALE, AND STATUTORY DAMAGES, *supra* note 55, at 20.
[128] Pamela Samuelson, *Unbundling Fair Uses*, 77 FORDHAM L. REV. 2537, 2554-55 (2009).
[129] *See* Andrew S. Long, Comment, *Mashed Up Videos and Broken Down Copyright: Changing Copyright to Promote the First Amendment Values of Transformative Video*, 60 OKLA. L. REV. 317, 319 (2007).

emphasis is commenting on or criticizing the underlying work.[130] Fourth, in addition to the costs and burden of licensing copyrighted content, it is extremely unlikely that owners would be interested in providing licenses to those who are going to criticize their work.[131] Fifth, although copyright holders may not encourage parody creation, express objections are unlikely to preclude users from commenting on creative works because of the free speech implications. While tolerated uses and informal practices are benefitting both the copyright owners and creators, the accompanying arbitrariness creates enforcement hurdles for the owners and creation concerns for users.

PART III – FROM WARMING TO FORMALIZATION IN A NO-ACTION POLICY

No-Action Strategy

With the advent of UGC, the discussion typically focuses on whether copyright owners should adopt an opt-in or opt-out approach to protection, but a no-action policy would simultaneously allow owners to protect their works and users to express themselves. An ex-post notice scheme would dictate that uses are not unlawful or illegal until the owner takes some action.[132] For example, under this framework, Disney fanatics' use of the *Frozen* material would be excused unless and until Disney contacted them regarding allegedly infringing behavior. One of the major benefits of placing the onus on the rights holder to act is the notice indicates what uses owners do not think detracts from the actual work's value, as well as uses that are consistent with common practice.[133] Although this approach seems counterintuitive, as copyright owners are presumed to have the rights that protect their expressions and ensuing derivative works, requiring action on the part of the copyright owner has been demonstrated in other contexts. Search engines and other content hosts are shielded from copyright liability until they are sent clear notice of the infringing use, and fail to respond to the removal request in an appropriate manner.[134]

---

[130] ELEC. FRONTIER FOUND., *Fair Use Principles for User Generated Video Content,* https://www.eff.org/pages/fair-use-principles-user-generated-video-content (last visited May 14, 2016).

[131] Rebecca Tushnet, *User-Generated Discontent: Transformation in Practice*, 31 COLUM. J.L. & ARTS 497, 515 (2008) (Explaining "existing licensing options for user-generated content routinely retain the option to censor").

[132] Wu, *supra* note 17, at 621.

[133] *Id.* at 626.

[134] 17 U.S.C. § 512 (2012) (Often referred to as the Digital Millennium Copyright Act "safe harbor").

Additionally, non-profit entities are free to utilize non-dramatic works unless and until they receive notice of an objection.[135] As copyright owners want to maintain as much control as possible while also limiting transaction costs, owners may allow users to create their works but only choose to go after individuals whose use of the work is harmful or damaging.[136] While this non-enforcement is encouraging for users, it likely is not indicative of movement toward an "opt-in" system where owners must provide notice before the work's usage amounts to infringement.

An opt-out regime contains some benefits, but copyright owners are unlikely to relinquish their rights on the front end. While an opt-out regime is laudable for allowing rights holders to determine what rights they want to keep as compared to what rights they are willing to surrender, this approach seems to assume that copyright owners will know a given right's individual worth.[137] This value assessment would be particularly difficult when a work is first created and does not yet have an established following or market. Google Books originally based its project on an "opt out" process where authors could specifically elect to not participate in the full-work scanning or choose to only include snippets.[138] However, from the early stages of the litigation, stakeholders expressed their discontent with the burden being placed on authors to take added steps when Google copied their works without first obtaining consent.[139] While these examples demonstrate the pros and cons of opt-in and opt-out approaches, many copyright holders are unwilling to commit to a hardened method, especially given the ever-changing digital landscape.[140]

Instead of forcing users to infer whether a practice will be permitted, copyright owners should specify or even encourage uses that will be permitted and not pursued for infringement.[141] This "No Action" policy would provide clarity to users who want to use these works without fear of receiving an ominous cease and desist letter or facing litigation, while also serving as an efficient method for the owners in only going after the economically significant infringements. These "No Action" policies will prevent holders from

---

[135] 17 U.S.C. § 110 (2012).
[136] Wu, *supra* note 17, at 628.
[137] Brad A. Greenberg, Comment, *More than Just a Formality: Instant Authorship and Copyright's Opt-Out Future in the Digital Age*, 59 UCLA L. REV. 1028, 1060 (2012).
[138] Ellen Duffer, *Why The Google Books Ruling Is Good For Publishers*, FORBES (Oct. 26, 2015), http://www.forbes.com/sites/ellenduffer/2015/10/26/why-the-google-books-ruling-is-good-for-publishers/#7062b52447a4.
[139] Authors Guild v. Google, Inc., 770 F.Supp.2d 666, 682 (S.D.N.Y. 2011).
[140] Wu, *supra* note 17, at 622.
[141] *See id.* at 633.

establishing precedents that impede their ability to pursue the cases involving more money and more prominent copyrights.[142] Similar to the Securities and Exchange Commission's "No Action Letters" addressing any doubts that might impede investment, Rj Idos, John Smith, and other content creators would be cognizant of what behavior is okay without harming creative expression.[143] SEC No-Action Letters are specifically restricted to the requester's particular facts and situation as indicated in the letter, and SEC staff maintain the ability to deviate from prior no-action letters.[144] If a similar policy were implemented in the copyright context, owners would have flexibility as technologies and uses change. This flexibility would be particularly advantageous if it took the format of a revocable license limited to certain categories of works, such as non-commercial online encyclopedias and noncommercial character artwork.[145]

This "no action" policy must be distinguished from other types of open frameworks, such as end user license agreements and Creative Commons licenses. Creative Commons licenses are premised on the copying and distribution of works, especially when the licensing works are noncommercial.[146] However, no-action policies are more limited than the expansive Creative Commons licenses because the business models for many of these owners are dependent upon maintaining control over reproduction and distribution.[147] Using a Creative Commons license would be unlikely to address the fears of such owners. The Creative Commons framework also includes a firm irrevocability policy, which can make copyright owners anxious about allowing a use that they will later want to exploit or limit because of economic implications or other reasons.[148] By contrast, the no-action policies enable an owner to revoke or adjust a given policy based on changing conditions.[149] Although a creative commons license can be somewhat restricted based on the

---

[142] *Id.*
[143] *See id.*
[144] U.S. SEC. AND EXCH. COMM., NO-ACTION LETTERS, https://www.sec.gov/answers/noaction.htm (last visited Sept. 20, 2016).
[145] *Id.* at 634.
[146] CREATIVE COMMONS – ABOUT THE LICENSES, https://creativecommons.org/licenses/ (last visited Mar. 29, 2016).
[147] Wu, *supra* note 17, at 634.
[148] *See* CREATIVE COMMONS – CONSIDERATIONS FOR LICENSORS AND LICENSEES, https://wiki.creativecommons.org/wiki/Considerations_for_licensors_and_licensees#Irrevocability (last visited Mar. 29, 2016) ("Once you apply a CC license to your material, anyone who receives it may rely on that license for as long as the material is protected by copyright and similar rights, even if you later stop distributing it").
[149] Wu, *supra* note 17, at 634.

work,[150] no-action policies can be limited to specific categories of work joined with additional requirements, such as express disclaimers.[151] This combination of factors is presumably why the Creative Commons framework has been employed by individuals and small firms.[152] The no-action policies can serve a similar function for the larger entities with the more commercially valuable works.[153] As long as this framework does not foreclose the ability of these copyright owners to respond to individual product and market changes, these no-action policies have a possibility of being adopted and becoming institutionalized.[154]

Ethical Implications and Guidelines

Empirical research revealed that "repeat players" who are constantly involved in disputes over copyrights and trademarks assert weak claims because the pursued parties are consumed by the uncertainty surrounding their activities.[155] According to the American Bar Association Model Rules of Professional Conduct, "A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous."[156] Arguably, a powerful licensing company going after a small bobblehead manufacturer with a strong free speech argument seems to indicate a frivolous claim and one that further demonstrates the unequal bargaining power between repeat IP players and ordinary users.[157]

---

[150] *See* CREATIVE COMMONS – CONSIDERATIONS FOR LICENSORS AND LICENSEES, https://wiki.creativecommons.org/wiki/Considerations_for_licensors_and_licensees#Scope_of_the_license (last visited Mar. 29, 2016) ("The licensor should have marked which elements of the work are subject to the license and which are not. For those elements that are not subject to the license, you may need separate permission").

[151] Wu, *supra* note 17, at 634.

[152] *Id.*

[153] Email Interview with Anne Gilson LaLonde, Author, GILSON ON TRADEMARKS (May 6, 2016) (Indicating that while this approach could be adopted for copyright owners, trademark owners may be less amenable to a formal no-action policy because an owner generally has to enforce its mark to maintain its associated rights).

[154] *See* Interview with Michelle M. Wu, Law Library Director and Professor or Law, Georgetown University Law Center (Mar. 30, 2016).

[155] William T. Gallagher, *Trademark and Copyright Enforcement in the Shadow of IP Law*, 28 SANTA CLARA COMPUT. & HIGH TECH. L.J. 453, 459 (2012).

[156] MODEL RULES OF PROF'L CONDUCT r. 3.1 (AM. BAR ASS'N 1983).

[157] Gallagher, *supra* note 155, at 457-58 (Discussing case involving Arnold Schwarzenegger's licensing company and an Ohio retailer producing and selling bobbleheads featuring Schwarzenegger wearing a suit and holding a rifle that culminated in settlement, which left often the question whether the use was protected).

Although norms of professionalism and decorum underlie the legal profession, whether these norms are complied with is an oversight issue. In actuality, most intellectual property rights enforcement occurs in the everyday practices of the rights holders and their lawyers, such as through the sending of cease and desist letters, phone calls, and negotiations, as compared to the court system with its accompanying supervisory functions.[158] In these situations, what is to stop an attorney from asserting rights and claims that may deviate from what the law actually says?

In addition to the ethical concerns involved with aggressive cease and desist and litigation practice, copyright owners must also be concerned with the possibilities of resulting publicity. While the media attention may reveal a compromise that allows a user to continue promoting his or her expression, such as what happened with Amplive permitting purchasers of Radiohead's In Rainbows to receive his remixed "Rainydayz Remixes" for no charge,[159] response from both the copyright owner and the media is not always so favorable. Chilling Effects Clearinghouse, which is now called the Lumen Database,[160] collects and publicizes demands and notices that it considers to be overly aggressive of IP rights.[161]

What is particularly instructive about this concern for ensuing publicity and maintaining positive relationships with current and future fans is Lumen's inclusion of a "No Action" category.[162] Although this category does not seem to have as many notices and helpful guidance as some of the other categories, including DMCA Notices and DMCA Safe Harbor, for how recipients should react to a complaint, the addition of this analysis could mean that copyright owners are sending these demand or cease and desist letters more as a warning. The owners may think it is sufficient to notify users that they are aware of their behavior. However, if these owners create a flexible no-action policy, this approach would allow the rights holder to take further action once a greater consensus is reached, both internally within a given company and externally in a given industry.

While all attorneys generally operate under the constraints of the Federal Rules of Civil Procedure and the ABA Model Rules of Professional Conduct, these formalized structures are not as helpful outside of the courtroom.

---

[158] *Id.* at 456.

[159] Eliot Van Buskirk, *MP3s: Amplive's 'Rainydayz' Remix of Radiohead's 'In Rainbows' Album*, WIRED (Feb. 13, 2008), http://www.wired.com/2008/02/mp3s-amplives-r/.

[160] LUMEN DATABASE, https://lumendatabase.org/ (last visited Mar. 31, 2016).

[161] Gallagher, *supra* note 155, at 495.

[162] LUMEN DATABASE – NO ACTION, https://lumendatabase.org/topics/30 (last visited Mar. 31, 2016).

Although Federal Rules of Civil Procedure Rule 11 provides for sanctions if an attorney submits a pleading, motion, or other paper based on an improper purpose, frivolous reason, or on contentions lacking in evidentiary support, how can attorney conduct be regulated if it is predominantly occurring in private?[163]Attorneys typically defend their aggressive demand letter and associated tactics by pointing to their responsibilities of policing and protecting their clients' intellectual property, which involves zealous representation.[164] Rule 1.3 of the Model Rules of Professional Conduct, which specifies that lawyers "shall act with reasonable diligence and promptness in representing a client" only references a "zeal in advocacy" within the commentary.[165] While it is admirable that an attorney will ferociously protect the client's property, an ethical question remains how attorneys should go about fulfilling this responsibility. If the American Bar Association was concerned with lawyers being driven by zealousness, it can be argued that this would have been included in the actual rule instead of being relegated to the commentary. There is a fine line between behavior that qualifies as zealous advocacy and behavior that can only be characterized as abuse.

While it would clearly be cost prohibitive for work owners to assert every copyright or trademark claim that exists, the general norm is to evaluate a combination of legal and non-legal factors.[166] Although a rights holder is much more likely to pursue a potential infringement if it pertains to the client's "core" protected expression, the owners, and more specifically, their legal teams, will likely be focused on whether the unauthorized use may tarnish or disparage the expression.[167] Generally, enforcement is much less likely when the users are fans who are not attempting to commercialize or to create unflattering portrayals of a work or its characters.[168] Idos Media's experience demonstrates this point. If a YouTube video disparaging *Frozen* began gaining traction in terms of viewership and other buzz, there is a high likelihood that Disney would have pursued the user with all of the intellectual property

[163] FED. R. CIV. P. 11 ("An attorney or unrepresented party certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances: the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law.").
[164] Gallagher, *supra* note 155, at 490.
[165] MODEL RULES OF PRO'L CONDUCT r. 1.3 and cmt. 1 (AM. BAR ASS'N 1983).
[166] Gallagher, *supra* note 155, at 472.
[167] *Id.* at 476, 479.
[168] *Id*. at 481.

protections within its arsenal.[169] Similarly, this is often why trademark owners are more likely to focus their efforts to combat infringement on users creating gripe or ".sucks" websites.[170]

While limited scholarship has been written on the litigation that does occur in the IP context, patent litigators claim that pretrial discovery is one of the prominent areas of ethical concerns within the field.[171] Surveyed patent litigators claim that while they focus on playing by the rules, they do not feel required to surpass this low bar.[172] One indication of this phenomenon was the revelation by interviewed patent lawyers that ethical lawyering is about zealously protecting and preserving a client's interests, and duties to the legal system and commitment to a "just" result are secondary afterthoughts, if they are considered at all.[173] Similar to defendants in criminal cases who are more likely to plead guilty than to go to trial because of information asymmetries, a comparable dynamic exists for defendants in copyright infringement cases.[174] Instead of focusing on the discovery rules, such as Federal Rule of Civil Procedure Rule 26 and ABA Model Rule 3.4(d), ethical duties should be woven into guidelines. An approach to introduce ethical standards addressing pre-plea discovery of exculpatory and impeachment information in the prosecutorial arena could be instructive.[175] Like the suggestion that prosecutorial ethical rules should be construed to require pre-plea discovery, plaintiffs in copyright suits should have to support infringement claims prior to filing motions for summary judgment.[176] While plaintiffs should not have to share their entire theory of the case, this sharing of infringement information may encourage agreement or settlement without wasting court resources and exorbitant amounts on attorney's fees. In the alternative, if parties are unable to come to an agreement, defendants would have access to some material that could be used for their defenses, including fair use. This framework would help ensure that only those defendants who actually infringed an owner's IP rights are punished, not just those who do not have access to evidence or resources.[177]

---

[169] Interview with Michelle M. Wu, Law Library Director and Professor or Law, Georgetown University Law Center (Mar. 30, 2016).
[170] Email Interview with Anne Gilson LaLonde, Author, GILSON ON TRADEMARKS (May 6, 2016).
[171] William T. Gallagher, *IP Legal Ethics in the Everyday Practice of Law: An Empirical Perspective on Patent Litigators*, 10 J. MARSHALL REV. INTELL. PROP. L. 309, 315 (2011).
[172] *Id.* at 320.
[173] *Id.* at 324.
[174] Erica Hashimoto, *Toward Ethical Plea Bargaining*, 30 CARDOZO L. REV. 949, 949 (2008).
[175] *Id.*
[176] *See id.* at 950-51.
[177] *See id.* at 950.

Although the lawyer's role is influential in determining the scope and role of infringement and discovery requests, the level of client deference is high because the clients know their works best and are paying the ever-increasing fees of large law firms and litigators.[178] However, lawyers must be mindful of potential sanctions that courts and ethics bodies can issue for discovery and other sorts of infractions. Fortunately for lawyers, though unfortunately for copyright users more generally, threats of consequences or reprimand are often deemed too abstract to significantly impact how IP lawyers conduct themselves on a regular basis.[179] While *Qualcomm Inc. v. Broadcom Corp.*, which involved a complex patent case in the Southern District of California, may have served as a cautionary tale for lawyers and clients who attempt to subvert the process, its impact was diminished because the individual attorney sanctions were lifted.[180] Clients, their attorney representatives, and the judiciary should take on a more active role in ensuring a just process, especially in the remedies context.

Ethical standard reforms are even more sorely needed in the damages regime. Arbitrariness and excessiveness are rampant as indicated by a judge wanting to award $118 million in statutory damages even without any evidence of actual harm or infringement-related profits.[181] To rein in this abuse, the courts should return to the original premise underlying statutory damages that they should be awarded only when plaintiffs are unable to prove actual damages or defendant's profits.[182] In looking to other IP regimes for example, especially to patents and trademarks, punitive damages should also be limited to no more than two or three times the damage award for willful infringements.[183] As courts pursue these individual users for behavior indicative of a larger trend, concern for these popular practices seems to permeate the ultimate decisions. However, the guidelines need to emphasize that the damages calculation cannot take into account other hypothetical infringement claims that are not before the court.[184] Although other UGC creators may view the award as a warning, these awards should not be used for the stated purpose of deterring other users' future

[178] Gallagher, *supra* note 155, at 335-36.
[179] *Id.* at 338.
[180] *Id.* at 359-60.
[181] Samuelson & Wheatland, *supra* note 45, at 442 (Discussing how trial judge in UMG Recordings, Inc. v. MP3.com wanted to award $25,000 per infringed CD in case involving 4,700 CDs. Although this case involves a commercial enterprise, it demonstrates the excessiveness of statutory damages awards).
[182] *Id.* at 510.
[183] *See id.* at 473 n.171.
[184] *Id.* at 469-70 (citing State Farm Mut. Auto. Ins. Co. v. Campbell, 538 U.S. 408, 410 (2003)).

conduct. To prevent this overreaching, judges should state on the record why a particular award is "just."[185]

One way to push both attorneys and clients in the direction of appropriate and ethical conduct is to tie such conduct to the potential damages to be awarded. If the plaintiff or the plaintiff's lawyer engages in misconduct, such as discovery abuse, only minimum statutory damages should be awarded.[186] If clients and attorneys face a potential sanction that would impact the bottom line, they are much more likely to comply with such requirements. Ultimately, attorneys have duties to their clients to represent their interests, but this practice cannot be done at the expense of an efficient discovery and overall enforcement system.

The Model Rules' lack of clarity and enforcement related to discovery and other infractions further indicates that these necessary ethical guidelines must be supplied from somewhere else.[187] In order to adequately address the intricacies of practice in the IP realm, the American Intellectual Property Law Association (AIPLA) and the International Trademark Association (INTA) should spearhead the promulgation effort. To prevent these guidelines from taking on a one-sided approach that harms unrepresented stakeholder groups, they should take the form of negotiated guidelines that include feedback from both rights holders and users.[188] The Principles for User Generated Content Services propagated by CBS, Disney, Sony Pictures and several other entities could function as a starting point.[189] Although copyright holders maintain a strong interest in pursuing infringers, the propagated ethical guidelines should utilize the guideposts from *BMW of North America, Inc. v. Gore* as inspiration for ways to evaluate the reprehensibility of defendant's actions and other remedies that have been awarded in similar cases.[190] In terms of reprehensibility, the copyright owner bringing the infringement claim should consider various factors, including whether a reasonable person would think the actions were lawful, whether a non-infringement defense was conceivable, the infringement's scale, and whether the defendant was a first-time or repeat

---

[185] *Id.* at 504.
[186] *Id.* at 502.
[187] Hashimoto, *supra* note 174, at 961-62.
[188] WHITE PAPER ON REMIXES, FIRST SALE, AND STATUTORY DAMAGES, *supra* note 55, at 14-15.
[189] PRINCIPLES FOR USER GENERATED CONTENT SERVICES, http://ugcprinciples.com/ (last visited May 15, 2016) (Including shared objectives of discouraging users from uploading infringing content).
[190] *See* Samuelson & Wheatland, *supra* note 45, at 464-65.

offender.[191] AIPLA and INTA's subject-matter expertise coupled with the generally un-harmful user behavior will help ensure that no course of action is pursued if the likelihood of an award is slim and also that the assessed remedy fits the situation. Like the pre-plea disclosures in the prosecutorial context being a first step toward more equitable process, these guidelines could be an instrumental part of the framework in a more ethical and just IP enforcement regime.[192]

CONCLUSION

As users of creative expression assume a more active role in the consumption of existing works, the development of additional works, and the dissemination of both, current copyright law is insufficient to address these evolving norms. If copyright owners continue to tolerate more of these uses, they should clearly indicate their positions in no-action policies that are flexible enough to adapt to changing economic conditions in particular industries or for particular works. Instead of seeing a resulting chilling effect because of the uncertainty, users will feel comfortable sharing their expression, which will be a beneficial addition to our society's creative corpus. Negotiated guidelines generated by both UGC creators and rights holders will allow promulgated ethical standards to underlie and support the no-action policies. As Judge Leval said, "While authors are undoubtedly important beneficiaries of copyright, the ultimate, primary intended beneficiary is the public."[193]

[191] *Id.* at 472.
[192] Hashimoto, *supra* note 174, at 963.
[193] Authors Guild v. Google, Inc., 804 F.3d 202, 212 (2d Cir. 2015).

CASE COMMENTS

SPOKEO V. ROBINS: A DANGEROUS CASE FOR PRIVACY PLAINTIFFS

Amanda Rodriguez[*] & Caroline Zitin[•]

CITE AS: 1 GEO. L. TECH. REV. 46 (2016)

http://bit.ly/2gcCgIV

INTRODUCTION

Spokeo is a people search engine that allows its users to view a profile of the searched individual that includes information such as: age, employer, address, relatives, marital status, and economic status.[1] Spokeo does not retrieve all of its information from one particular source, nor does Spokeo search for the data. Instead, Spokeo aggregates data from a multitude of online and offline sources and provides users with the option of removing any inaccurate information. Using deep web crawlers,[2] Spokeo gathers and combines different sources of publically available information that can be obtained from individuals' Facebook check-ins, Pandora playlists, Flickr images and even dating sites.[3]

In 2003, Thomas Robins brought a class action suit alleging that Spokeo had violated the Fair Credit Reporting Act (FCRA) by publishing inaccurate information about him, including inaccurate information about his education

---

[*] GLTR Staff Member; Georgetown Law, J.D. expected 2018; Texas A&M International University, B.A. 2015.

[•] GLTR Staff Member; Georgetown Law, J.D. expected 2018; Middlebury College, B.A. 2014.

[1] SPOKEO, http://www.spokeo.com (last visited Oct. 21, 2016).

[2] Smita Agrawal & Kriti Agrawal, *Deep Web Crawler: A Review*, 1 INT'L J. OF INNOVATIVE RES. IN COMPUT. SCI. & TECH. 12, 12 (2013) (Deep web crawlers are web crawlers that specific collect data from the deep web. Web crawlers search web documents, collect their information, and save their indices for search engines to process in a fast manner).

[3] *Supra* note 1.

and economic status.[4] Robins claimed that Spokeo's publication of this falsified information precluded him from employment opportunities he would have received if potential employers were provided with the correct information about Robins on Spokeo's website.[5] When the case reached the Supreme Court, the issue was whether the harms Robins' claimed satisfied Article III standing requirements.[6]

The district court dismissed the claim, finding that Robins had failed to allege an injury-in-fact because he argued that the false information might affect his future job prospects rather than demonstrating that Spokeo's actions had in fact resulted in the loss of job offers. Robins appealed, and the Ninth Circuit reversed.[7] The Supreme Court granted certiorari.[8] Upon review, the Supreme Court held that the Article III analysis performed by the Ninth Circuit was incomplete and remanded the case to consider the separate elements of harm that it held the Ninth Circuit had conflated— concreteness and particularity.[9]

This comment analyzes the Supreme Court's decision and concludes that the Court should have affirmed the Ninth Circuit's finding of injury-in-fact, as the harm was both particularized and concrete. By remanding, the Court weakened the ability of individuals to protect their right to privacy created by Congress in the FCRA.

ANALYSIS

Article III of the United States Constitution requires that a plaintiff must demonstrate "irreducible constitutional minimum standing by illustrating, among other factors, that she suffered an injury in fact"[10] to pursue legal redress. Within injury-in-fact, a plaintiff is further required to show that she suffered an "invasion of a legally protected interest that is both concrete and particularized."[11] If a plaintiff is unable to demonstrate concreteness or particularization, she lacks standing.[12] Without standing a court lacks subject-matter jurisdiction, and cannot hear the plaintiff's claim.[13]

---

[4] Robins v. Spokeo, Inc. 742. 3d 409, 410 (9th Cir. 2014).
[5] *Id.*
[6] *Id.*
[7] *See id.* at 411.
[8] *See id.* at 410.
[9] Spokeo, Inc., v. Robins. 136 U.S. 1542, 1547 (2016).
[10] Lujan v. Defenders of Wildlife, 504 U.S. 555, 556 (1992).
[11] *Id*. at 560.
[12] *Id.*
[13] Allen v. Wright, 468 U.S. 737, 750-51 (1984).

Particularization demonstrates that an injury has affected a plaintiff in a personal and individual way. In addressing whether Robins had standing, the Ninth Circuit found that he had an individualized interest in handling his financial information, which was both particular and concrete. This comment argues that the harm suffered by Robins was both particular and concrete, and was therefore unnecessarily remanded by the Supreme Court.

Treatment of Standing

In *Lujan v. Defenders of Wildlife*, the Court held that in order to have standing, a plaintiff must demonstrate harm specific to the plaintiff, rather than to the public at large.[14] Here, the Ninth Circuit and the Court agree that Robins alleged a particularized injury: Robins asserted that he suffered individual harm to his employment prospects as a result of Spokeo publishing false information about his education, financial, and familial status.[15] Robins argued that this misinformation would cause employers to believe that he was overqualified, expected a higher salary than employers would be willing to pay, and was less mobile due to family commitments;[16] thereby impairing his ability to find employment.

However, the Court found that the Ninth Circuit had not adequately analyzed whether the harm was also concrete.[17] The court distinguishes concreteness from particularization by stating that a concrete harm must be "real," rather than "abstract."[18] Further, while both the history and judgment of Congress play an important role in determining whether an intangible harm constitutes injury in fact,[19] a statutory violation by itself does not necessarily satisfy the concreteness requirement if it is only a bare procedural violation.[20] The Court left it to the Ninth Circuit to determine whether the harm in this case is more than a bare procedural violation of the FCRA.

While the Court did not explicitly determine that the alleged injury is not concrete enough to warrant standing, by leaving the door open for the determination that a violation of a federal statute protecting privacy is insufficient, the Court is not adequately acknowledging the value Congress

[14] *See id.* at 579.
[15] *Spokeo*, 136 U.S. at 1548.
[16] *Id.* at 1554.
[17] *Id.* at 1548.
[18] *Id.*
[19] *Id.*
[20] *Id.* at 1549. (Here the majority suggests that a bare procedural violation is a violation of the statute that would cause no actual harm; the example offered is an incorrect zip code).

placed on consumer privacy when it enacted the FCRA[21]—weakening all consumers' right to privacy. The primary purposes of the FCRA are to protect the privacy of consumers and ensure the veracity of consumers' published financial information.[22] The Court itself has previously recognized those goals as primary to the enactment of the FCRA.[23]

Moreover, Robins's injury was more than a "bare procedural violation" of the FCRA. The majority offers the example of an incorrect zip code as a procedural violation of the FCRA that does not create harm.[24] As Justice Ginsburg notes in her dissent, the impact of the violation here clearly goes farther and creates a real harm, as the inaccurate representations of Robins' financial status and family situation impaired his ability to find employment.[25] She further states that remand is not necessary. In addition to the harm being concrete, Ginsburg notes that prior cases do not distinguish particularization and concreteness from one another. One example cited is *Summers v. Earth Island Institution*, where the Court does not separately address concreteness and particularization. Instead, they are considered as one factor.[26] In trying to parse out the difference between a particular harm and a concrete harm, the Court loses sight of the need to maintain the remedy provided by Congress.

Future Considerations and Data Breaches

Spokeo now warns its users that information obtained should not be used "to make decisions about employment, tenant screening, or any purpose covered by the FCRA".[27] Disclosures such as these are meant to protect companies from further lawsuits. However, users are not restricted from using

---

[21] *See* 15 U.S.C. § 1681(a)(4) (2016).

[22] *See* 15 U.S.C. § 1681(b) (2016) (defining the purpose of the FCRA as "requiring that consumer reporting agencies adopt reasonable procedures" to ensure that credit reporting is "fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization" of consumer information).

[23] Safeco Ins. Co. of America v. Burr, 551 U.S. 47, 52 (2007) ("Congress enacted the FCRA in 1970 to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy.").

[24] *See Spokeo*, 136 U.S. at 1550.

[25] *Id.* at 1556.

[26] *See* Summers v. Earth Inst., 555 U.S. 488, 494 (2009) ("To establish concrete and particularized injury that standing requires, respondents point to their member' recreational interests in the national forests. While generalized harm to the forest or the environment will not alone support standing, if that harm in fact affects the recreational or even the mere esthetic interest of the plaintiff, that will suffice.").

[27] *Id.*

the gathered information for illegal purposes, rather they are merely advised or discouraged from doing so by such notices. Companies like Spokeo may therefore continue to provide the information necessary for third parties to violate the FCRA by simply subscribing to their membership and paying a monthly fee. The continuous supply of information that companies such as Spokeo make available for others to use illegally poses a serious threat for individual privacy rights, and the holding in *Spokeo* advances such abuse.

The Court's decision has already impacted courts across the nation.[28] Prior to *Spokeo*, data breach cases involving misuse of information faced a high bar to establish standing, and *Spokeo* has raised that bar even higher.[29] Courts must now turn to *Spokeo* when deciding whether data-breach claims sufficiently demonstrate an injury-in-fact that is both particularized and concrete.[30] In *Gubala v. Time Warner Cable, Inc*., the plaintiff alleged that Time Warner violated the Cable Communications Policy Act by retaining the plaintiff's personal information after the service contract had been terminated.[31] When addressing the issue of concreteness, the Court turned to "the clear directive [given by] Spokeo" to conclude that the plaintiff only sufficiently alleged a particularized injury, without addressing concreteness.[32] Just as the Court found that Robins did not show a particularized injury by simply alleging possible employment loss, the Court agreed that Gubala had similarly failed to claim such an injury.[33] While *Spokeo*'s decision may not appear to have been revolutionary, the decision has already provided courts with a more stringent threshold for analyzing Article III standing questions.

Privacy protections under American law consist of a combination of sector-specific protections, rather than any omnibus privacy regulation. Privacy is protected in the Federal Constitution under the Fourth Amendment,[34] and under many state Constitutions.[35] The majority of states further recognize legal redress for invasions of privacy under applicable tort statutes.[36] But the vast majority of privacy protections under American law are created by statute. The

---

[28] *See generally* Khan v. Children's National Health, 2016 WL 2946165 (D. Md. May 19, 2016).

[29] Jeryn Crabb, *Data-Breach Class Actions Feel the Effects of "Spokeo v. Robins."* WASH. LEGAL FOUND. (July 1, 2016), http:wlflegalpulse.com/2016/ 07/01/data-breach-class-actions-feel-the-effects-of-spokeo-v-robins.

[30] *Id*.

[31] Gubala v. Time Warner Cable Inc., 2016 WL 3390415, at *1 n.1 (E.D. Wis. June 17, 2016).

[32] *Id.* at *5.

[33] *Id.*

[34] U.S. CONST. amend. IV.

[35] CAL. CONST. art. I, §1.

[36] RESTATEMENT (SECOND) OF TORTS §28 (AM. LAW INST. 2016).

Privacy Act of 1974 sets out requirements that government agencies must abide by in order to protect individual privacy rights.[37] HIPAA protects an individual's health privacy,[38] and GINA protects the privacy of individual's genetic information.[39] The VPPA affords protection for an individual's video rental information,[40] ECPA the content of electronic communications,[41] and FERPA affords specific privacy protections for students.[42] This constellation of individual protections are all significantly affected by *Spokeo*—the way the lower courts apply the decision will determine whether individuals will have standing to pursue the legal redress these statutes are intended to provide. If there is no legally recognized harm as an element of injury-in-fact, the plaintiff does not have standing, and cannot receive redress from a court, and those protections become meaningless.

CONCLUSION

The Supreme Court should have affirmed the Ninth Circuit's decision. Both the Ninth Circuit and the Supreme Court acknowledge that the harm suffered by Robins from the publication of inaccurate information by Spokeo was a sufficiently particularized enough harm to warrant injury-in-fact. While the majority did not find the Ninth Circuit's standing analysis complete, as Justice Ginsburg notes in her dissent, remand was unnecessary. The harm alleged was concrete and particularized, and the need to protect consumer privacy is too important to make it more difficult for individuals to hold corporations accountable in court when they violate a federal statute. This decision, and the result from remand, has substantially impacted the future of consumers' ability to bring privacy and data-breach claims in federal courts.

[37] The Privacy Act of 1974, Pub. L. No. 93-579 (1974).
[38] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996).
[39] Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff (2012).
[40] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012).
[41] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701–12 (2012).
[42] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2012).

MICROSOFT V. UNITED STATES: IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E–MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

Jeffery Gary[*] & Jane Olin-Ammentorp[•]

CITE AS: 1 GEO. L. TECH. REV. 52 (2016)
http://bit.ly/2gq9GBu

INTRODUCTION

As technology continues to evolve, the need to provide meaningful consumer protections remains an immense challenge for legislators and jurists. Aging statutes and inadequate precedents make devising modern technological solutions difficult.[1] Increasingly, courts have had difficulty grappling with the questions arising from the increasing volume of consumer data, particularly how to consider the implications of data in the hands of third parties.[2] This difficulty becomes especially acute when applied to data flows and Internet

[*] Assistant Case Comments Editor, GLTR; Georgetown Law, J.D. expected 2018; J.D.; King's College London, M.A. 2014; DePaul University, B.F.A. 2012.

[•] GLTR Staff Member; Georgetown Law, J.D. expected 2018; University of Oxford, M.Sc. 2011; Cornell University, B.A. 2009.

[1] *See, e.g.* Kyllo v. United States, 533 U.S. 27 (2001); United States v. Jones, 132 S.Ct. 945 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.") (internal citations omitted).

[2] *See* In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003) (applying Wiretap Act to find no interception when a website directs a user's browser to make third-party cookie requests).

traffic, which defy simple categorization.[3] Recently, in *Microsoft v. United States*, the Second Circuit held that U.S. law enforcement may not compel a domestic data processing company to provide data that is stored outside the country.[4]

This comment will explain that the Second Circuit correctly applied existing law, but failed to understand the technological underpinnings and statutory intent at issue. To do so, the comment will discuss the history of the Electronic Communications Privacy Act (ECPA), including the development of the statute's warrant provisions, and original intent to protect individual privacy and civil liberties. The comment will further show that in the years since ECPA's enactment, new technology has diminished the ability of the statute to provide meaningful guidance for law enforcement. It will then discuss the court's holding, and analyze why the court has misconstrued the nature of the data at issue, even though the court correctly applied the existing law. The comment will conclude with thoughts on the impact this holding may have on technology companies and consumers, and address concerns rising from the increasing trend of data localization.

STATUTORY BACKGROUND AND PROCEDURAL HISTORY

The Stored Communications Act (SCA) was enacted in 1986 as Title II of ECPA.[5] ECPA replaced the Wiretap Act, which was part of the Omnibus Crime Control and Safe Streets Act of 1968.[6] ECPA was intended to modernize the legal framework for surveillance as new technologies such as computer communication outpaced the civil liberties protections already in place.[7] Though ECPA was passed before the mass proliferation of web services,

---

[3] *See* Katitza Rodriguez, *Colombian Users to ISPs: 'Where Is My Data?'*, ELEC. FRONTIER FOUND. (May 20, 2015), https://www.eff.org/deeplinks/2015/05/which-internet-providers-tell-colombians-where-their-data.

[4] In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) [hereinafter "Microsoft"].

[5] Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2701 *et seq.* (1986)).

[6] Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 801, 82 Stat. 197, 212 (1968).

[7] 130 CONG. REC. 4107-08 (Oct. 1, 1984) (Remarks of Rep. Kastenmeier introducing ECPA in the House of Representatives), https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/26/cr-e4107-08-1984.pdf; 131 CONG. REC. 24365-71 (Sept. 19, 1985) (Remarks of Sen. Leahy introducing ECPA in the Senate), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/11/cr-24365-71-1985.pdf.

ECPA's provisions have been interpreted to cover email,[8] private social media messages,[9] and text messages.[10]

Section 2703 of the SCA authorizes law enforcement to variously obtain court orders, subpoenas, or warrants compelling private companies to disclose user data. The disclosure mechanisms operate in a tiered system: court orders require the lowest standards for evidence, but only allow access to customer record information.[11] Subpoenas require an equivalent level of reasonable suspicion, and allow law enforcement to view non-content data of specific messages.[12] The highest level of protection is provided for the contents[13] of communications in electronic storage that have been stored for 180 days or fewer.[14] To access such data, law enforcement must obtain an SCA warrant consistent with the Federal Rules of Criminal Procedure, including a showing of probable cause to a magistrate judge.[15] Each mechanism also allows access to the information obtainable by a lesser degree of proof in a sliding scale: law enforcement officials could obtain a warrant and see all the information available through a court order, for example.[16]

In *Microsoft*, the FBI obtained a warrant—subject to the strictest requirements of § 2703—to compel the company to disclose the email record information and email content of an account that had allegedly been used in furtherance of narcotics trafficking.[17] Microsoft complied with the portion of the request for the account's non-content information, which was stored in the United States, but refused to comply with the request for content data, arguing

[8] Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2003).
[9] *See* Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010).
[10] *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008).
[11] 18 U.S.C. § 2703(c)(B) (2012).
[12] 18 U.S.C. § 2703(d) (2012).
[13] Content is generally defined as the intended message defined by the communication, while information used to address or process the message (i.e. addressing or timestamp information) is considered non-content, and afforded lower levels of protection, even when it may contain sensitive information. *See* In re Zynga Privacy Litigation, 750 F.3d 1098, 1106 (9th Cir. 2014) ("Congress intended the word 'contents' to mean . . . the essential part of the communication, the meaning conveyed, and the thing one intends to convey.") (internal marks omitted).
[14] 18 U.S.C. § 2703(a)–(b) (2012).
[15] 28 U.S.C. § 2703(a) (2012); *see* FED. R. CRIM. P. Rule 41. A warrant under § 2703 requires a showing of specific and articulable facts showing reasonable grounds to believe that the contents, records, or other information in or relating to a wire or electronic communication are relevant and material to an ongoing criminal investigation. § 2703(b)(1)(B) of ECPA generally requires providing notice to a subscriber to get contents of communications, though this is not always the case when accessing records.
[16] *See* 18 U.S.C. § 2703(c) (2012).
[17] *Microsoft*, 829 F.3d 197, 202–3 (2d Cir. 2016).

that as the information was stored and maintained in Ireland, and the government had not established that the target of the investigation was a U.S. national, the information was not subject to U.S. jurisdiction.[18]

Microsoft moved to quash the warrant; however, the District Court denied the motion and held Microsoft in civil contempt for its failure to comply with the warrant.[19] Microsoft appealed and the Second Circuit court reversed and vacated the District Court's contempt holding.[20]

TECHNOLOGICAL HISTORY

ECPA was enacted in 1986, well before the internet became a ubiquitous feature of everyday interactions. The "sophisticated technology" that prompted the enactment of ECPA in the mid-1980s included video surveillance and information passing over telephone lines.[21] The legal issues flowing from these new technologies largely hinged on whether the government could legally access communication data owned by a particular person and stored in a particular place.[22] At the time of enactment, the familiar analogy between postal mail and email still held strong: an individual sent a communication, it was transmitted by the individual's provider, and then collected by the individual's intended recipient. The email was stored on the personal computers of the two correspondents, and only stored by a provider if a correspondent specifically signed up for that service.[23]

In *Microsoft*, the service at issue is Outlook, the familiar email client. Microsoft administers the service through an international network of servers in over 100 countries.[24] An Outlook user's data is stored in servers nearest the user, in order to reduce overall latency and increase the efficiency of the service.[25] Messagesare transmitted and stored nearly instantaneously, and

[18] *Id.* at 204.
[19] *Id.* at 205.
[20] *Id.*
[21] *See* Remarks of Rep. Kastenmeier, *supra* note 7.
[22] *See* Remarks of Sen. Leahy, *supra* note 7. ("[T]here is no adequate Federal legal protection against the unauthorized access of electronic communications system computers to obtain or alter the communications contained in those computers.").
[23] It was in this context that the ECS/RCS distinction codified in ECPA arose. This distinction is now largely technologically obsolete, since messages can, as a technological matter, be both stored and transmitted simultaneously, *see* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 4, 729 (2016).
[24] *Microsoft*, 829 F.3d 197, 202–3 (2d Cir. 2016).
[25] *Id.* at 202. ("Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when

individuals rely on third-party electronic storage solutions to a degree never contemplated in 1986.

Now, email may be drafted, sent, and stored all in the cloud.[26] A provider may be based, or—as in *Microsoft*—store data in a jurisdiction that may or may not be the same jurisdiction where the user resides. The reference in the SCA to the Federal Rules allows the government to receive data stored outside an individual's district; however, the Federal Rules are silent on issues of international storage. [27] The limitations cloud computing places on law enforcement have been addressed forcefully by the courts, which have found, for instance, that law enforcement may not use a search incident to lawful arrest to view information on a phone stored in the cloud. [28]

While the privacy interests implicated in the rise of cloud computing are significant, the challenges to law enforcement are similarly daunting. As more data is stored in the cloud, records that would have been accessible ten years ago to law enforcement with the use of a legitimate warrant are now rendered inaccessible because of technological changes. Storage policies of individual companies might include different protocols about how, where, and whether data is stored, creating an inconsistent set of protections and allowances for consumers and law enforcement. [29] Individuals and their data cross borders with increasing frequency, and there is limited clarity, both in the United States and

---

subscribing to the service. Microsoft does so, it explains, in part to reduce network latency—i.e., delay—inherent in web-based computing services and thereby to improve the user's experience of its service.") (internal quotations omitted); *id.* at 202 n.5 ("[T]he greater the geographical distance between a user and the datacenter where the user's data is stored, the slower the service.").

[26] IBM, *What Is Cloud Computing?*, IBM CLOUD, https://www.ibm.com/cloud-computing/learn-more/what-is-cloud-computing (last visited Nov. 17, 2016) ("Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet.").

[27] *See* FED. R. CRIM. P. Rule 41(b)(5). At the time of publication, Congress was considering an amendment to this rule, set to take place Dec. 1, 2016. The amendment would guarantee judicial review for remote warrants under two narrow circumstances: when a suspect has technologically masked his computer, and when a computer crime involves five or more jurisdictions. Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T OF JUST.: JUSTICE BLOGS (June 20, 2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

[28] Riley v. California, 134 S.Ct. 2473, 2491 (2014).

[29] *See, e.g.*, *Where your data is located*, MICROSOFT TRUST CTR., https://www.microsoft.com/en-us/trustcenter/Privacy/Where-your-data-is-located (last visited Oct. 21, 2016).

abroad, on how territorial boundaries affect data and the substantive rights of its owners.

ANALYSIS

The Second Circuit based its decision on a two-step inquiry. First, after noting the presumption against extraterritorial application of U.S. laws,[30]the court examined whether Congress intended for the SCA to apply extraterritorially. It determined that due to the lack of clear language establishing extraterritorial intent, the statute could not be read to include application outside the United States.[31] This was particularly true, in the court's analysis, as the warrant provisions specifically describe procedures for operation in various U.S. jurisdictions, but none for foreign application.[32] Second, after determining Congress did not intend the SCA to apply extraterritorially, the court concluded that the intent of the SCA was to protect individual privacy by shielding user content from intrusion, rather than to benefit law enforcement.[33] The court held that as the purpose of the law was to protect user information, construing the statute to apply extraterritorially without clear statutory language was inappropriate, since doing so would undermine the original goals of the statute.

However, this holding largely rests on the legal analysis of technological issues that did not exist at the time Congress enacted the SCA, a point emphasized in Judge Lynch's concurrence: "there is no evidence that Congress has *ever* weighed the costs and benefits of authorizing court orders of the sort at issue in this case."[34] Further, as Judge Lynch argued, the characterization "that this case involves a government threat to individual privacy," as was suggested by a number of amici briefs, is largely misguided.[35]

---

[30] Generally, there is a presumption against extraterritorial application of U.S. law, unless a statute specifically notes an alternative intention. *See, e.g.* E.E.O.C. v. Arabian Am. Oil Co., 499 U.S. 244 (1991); Morrison v. Nat'l Austl. Bank, 561 U.S. 247 (2010).

[31] *Microsoft*, 829 F.3d 197, 210 (2d Cir. 2016).

[32] *Id.* at 211 ("We think it particularly unlikely that, if Congress intended SCA warrants to apply extraterritorially, it would provide for such far-reaching state court authority without at least addressing the subject of conflicts with foreign laws and procedures.") (internal marks and quotations omitted).

[33] *Id.* at 217 ([T]he relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content.").

[34] *Microsoft*, 829 F.3d at 231 (Lynch, J., concurring) (emphasis in original).

[35] *Id.* at 222.

In this case, the government went through the most privacy-protective requirements in the SCA: obtaining a warrant for the content of communications in compliance with requirements established by the Fourth Amendment.[36] While the SCA, and ECPA broadly, may be ill-equipped to address the nuances of modern technology,[37] the privacy violations asserted by Microsoft and amici are not as grave as suggested.

While concurring in the court's holding, Judge Lynch further emphasized the serious need for Congress to revise the SCA to reflect current realities of stored electronic communications.[38] If, as the majority suggests, an invasion of privacy occurs where particular content is stored,[39] any future litigation against the government regarding information stored in the cloud will necessarily involve fact-dependent analyses of where information may have been at a particular moment it was searched or seized. A more appropriate solution may be to tie the "location" of the privacy invasion to the nationality or residence of the individual whose privacy was violated, rather than to the arbitrary and transitory location of the individual's data. However, doing so likely requires an amendment to the law, and would require Congressional attention.

LIKELY EFFECTS OF THE DECISION

In the wake of the *Microsoft* decision, commentators,[40] Congress,[41] and Microsoft itself[42] have noted the limitations of the SCA and ECPA as they currently stand. Many commentators, including Microsoft, hailed the Second

---

[36] *Id.*

[37] See Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) ("[T]here are many problems of Internet privacy that the SCA does not address.").

[38] *Id.* at 231-33. *See also* Peter J. Henning, *Microsoft Case Shows the Limits of a Data Privacy Law*, N.Y. TIMES (July 18, 2016), http://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html.

[39] *See Microsoft*, 829 F.3d at 209; *id.* at 230 n.7. (Lynch, J., concurring).

[40] Andrew Keane Woods, *Reactions to the Microsoft Warrant Case*, LAWFARE BLOG (July 15, 2016, 7:21 AM), https://lawfareblog.com/reactions-microsoft-warrant-case.

[41] Press Release, Office of Senator Orrin Hatch, Orrin Hatch, Hatch, Coons, Heller Introduce Bipartisan International Communications Privacy Act, (May 25, 2016), http://www.hatch.senate.gov/public/index.cfm/2016/5/hatch-coons-heller-introduce-bipartisan-international-communications-privacy-act.

[42] Brad Smith, *Our Search Warrant Case: An Important Decision for People Everywhere*, MICROSOFT (July 14, 2016), http://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/.

Circuit's decision as a victory for individual privacy.[43] This understanding of *Microsoft*'s outcome is largely flawed— while the majority opinion cited protecting individual privacy for users of cloud-based services as a motivation for its holding, the opinion missed important implications for individual privacy, as noted throughout Judge Lynch's concurrence.[44] Further diminishing the privacy issues cited by the majority, Microsoft did not contest that if all the data requested was stored in the United States, it would have provided content access to law enforcement.[45] Currently, the majority of such email data remains stored in the United States,[46] and as such, the effects of *Microsoft* are likely to remain limited in actual application in the near future.

A purely territorial approach to a user's privacy expectations (and to the SCA) is becoming increasingly challenging to manage judicially, as users are relying more frequently on cloud-based products and services, and companies providing cloud services continue to diversify the geographic scope of their servers.[47]

However, the localization of data poses complications beyond the scope encountered in *Microsoft*. The debate over the ability for data to actually be localized at all has not yet been settled: some argue that data, like money or debt, can indeed be localized,[48] while others note that such analogies to other forms of "intangible" items do not properly capture the way that data is stored and moved.[49]

This debate will certainly continue as the use of cloud storage expands. But discussions on data processing cannot be solely domestic: foreign law and international agreements play a large role. China has strict rules on the export of data;[50] U.S.-EU agreements on data privacy could have a major effect on

---

[43] *See id.*

[44] *Microsoft*, 829 F.3d at 233 (Lynch, J., concurring) ("without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy.").

[45] *Id.* at 223.

[46] *Where is My Data?*, MICROSOFT ONLINE SERVS., https://www.microsoft.com/online/legal/v2/?docid=25 (last visited Oct. 21, 2016).

[47] *Microsoft*, 829 F.3d at 50, n.7 (Lynch, J., concurring).

[48] Kevin Dockery, *Data Localization Takes Off as Regulation Uncertainty Continues*, WALL ST. J.: RISK AND COMPLIANCE BLOG (June 6, 2016 1:08 PM ET), http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/.

[49] *See* Woods, *Against Data Exceptionalism*, *supra* note 23 at 1.

[50] *Data Transfers Out of China: What You Have to Consider Before You Press "Send,"* FRESHFIELDS BRUCKHAUS DERINGER, http://www.freshfields.com/en/global/Digital/data_transfer/?LangType=2057 (last visited Oct. 21, 2016).

access to various types of data,[51] regardless of their localization; and the implications of the EU's General Data Protection Regulation are so far unclear.[52] Any lasting solution for the storage of, and government access to, personal data will need to take place in legislatures, and in international negotiations.

Currently, law enforcement's access to data stored abroad is governed by the Mutual Legal Assistance Treaty (MLAT) process, by which countries negotiate rules for requesting and granting access for criminal investigations.[53] Because ECPA requires that any government entity seeking to compel data must attain a U.S. warrant, foreign governments flood the Department of Justice with MLAT requests.[54] The decision in *Microsoft* is the mirror of that: U.S. law enforcement may not access data stored abroad without seeking assistance from the affected foreign government. While there have been competing suggestions on how best to reform the MLAT process,[55] reform of ECPA itself is likely necessary to allow law enforcement to effectively access data while still protecting consumer privacy. Regardless of how reform is achieved, data localization will likely remain a result of company policy, rather than a

---

[51] *See* U.S. DEP'T OF COMM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES (2016). The exact nature of these agreements is not yet clear, but they would theoretically allow foreign governments to serve warrants on U.S. technology companies and vice versa, eliminating the type of warrant limitations faced in *Microsoft* as well as the sometimes lengthy mutual legal assistance treaty (MLAT) request process. *See also* Devlin Barrett & Jay Greene, *U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms*, WALL ST. J. (July 15, 2016 8:00 PM ET), http://www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305.

[52] Dockery, *Data Localization Takes Off*, *supra* note 48.

[53] T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, FED. JUD. CTR. (2014), http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf.

[54] Andrew Keane Woods, *Procedural Options for Improving Cross-Border Requests for Data*, LAWFARE BLOG (Oct. 13, 2015, 7:58 AM), https://www.lawfareblog.com/procedural-options-improving-cross-border-requests-data.

[55] *Compare* Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden, President of the United States Senate (July 15, 2015) (conveying proposed legislation and a section-by-section analysis), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf. (proposing allowing select foreign governments to make requests for data under their own domestic standards), *with* Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, JUST SECURITY (Nov. 24, 2015, 8:03 AM), https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/ (proposing that foreign governments be allowed access to data under certain restrictions only when "(i) the requesting government has a legitimate interest in the criminal activity being investigated; (ii) the target is located outside the United States; and (iii) the target is not a US person.").

regulatory or consumer choice.[56] Each internet service provider (ISP) still principally acts according to internal policies when granting or denying government requests for account information, including warrant requests. As such, this poses the risk that private companies will continue to determine data privacy policy, rather than the government.[57] Whether or not technology companies shift servers abroad to deliberately frustrate legitimate law enforcement prerogatives is irrelevant; if servers are shifted abroad simply to suit a perception of market expectations and possible legal risk, the result will be the same. Legitimate warrants for evidence pertaining to U.S. suspects will be rendered toothless, an unlikely intent of the drafters of the SCA, or the constituents they serve. Individual privacy must be protected, but will be better served, and result in fewer unintended consequences, by an approach that builds those protections on a more accurate factual foundation. Due to the variety of requests from government agencies, differing internal policies, and the limited resources of the offices granting warrants and processing requests, it would greatly benefit the government, the public, and ultimately the technology sector to focus future legislation on standardizing data requests and responses across the industry.

CONCLUSION

In the wake of the *Microsoft* decision, the U.S. Congress has contemplated numerous reforms to ECPA that would variously address the scope of the 2703 warrant[58] and expand U.S. law enforcement's access to data overseas.[59] In the meantime, consumers are left with a confusing patchwork of statutory obligations, common law, and private corporate policies that reduce overall protection for consumer privacy. As the issue is considered further both in the courts and in the legislature, a keen eye towards the actual technological underpinnings of user communications is essential in order to balance the need for effective law enforcement with the responsibility to protect individual privacy rights.

---

[56] Peter J. Henning, *Microsoft Case Shows the Limits of a Data Privacy Law*, N.Y. TIMES (July 18, 2016), http://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html?_r=0.

[57] *Microsoft*, 829 F.3d 197, 224 (2d Cir. 2016).

[58] Electronic Communications Privacy Act Amendments Act of 2015, S. 346, 114th Cong. § 2 (2015); Email Privacy Act, H.R. 699, 114th Cong. § 2 (2015).

[59] International Communications Privacy Act, S. 2986, 114th Cong. § 2 (2016).

ORACLE AMERICA, INC. V. GOOGLE INC.: COPYRIGHTABILITY OF APPLICATION PROGRAMMING INTERFACES AND A FAIR USE DEFENSE:

Michael R. Mazzella III[*] & R. Harrison Dilday[•]

CITE AS: 1 GEO. L. TECH. REV. 62 (2016)

http://bit.ly/2fKopJ7

INTRODUCTION

In May of 2014, the United States Court of Appeals for the Federal Circuit incorrectly reversed the United States District Court for the Northern District of California's decision in *Oracle v. Google*. By broadly extending copyright protection to Java Application Programming Interfaces (APIs), the Federal Circuit drastically shifted the landscape of coding and app development. On remand over copyright fair use questions, the district court creates a kind of shield against the consequences of a Federal Circuit reversal, but on very timid—and very expensive—grounds. When the smoke clears, this decision may result in hindered innovation and stalled technological advances that tend to harm consumers, a flood of intellectual property infringement litigation that will overburden courts, and a new standing precedent that deviates from legislative intent.[1]

---

[*] GLTR Staff Member; Georgetown Law, J.D. expected 2018; University of Arizona, B.A. 2015.

[•] GLTR Staff Member; Georgetown Law, J.D. expected 2018; Georgetown University School of Continuing Studies, B.A. 2015.

[1] Corynne McSherry, *Dangerous Decision in Oracle v. Google: Federal Circuit Reverses Sensible Lower Court Ruling on APIs*, ELEC. FRONTIER FOUND. (May 9, 2014),

This comment seeks to address the decision made by the Federal Circuit's reversal and provide an alternative approach that is in better keeping with the spirit of the Copyright Act. The comment analyzes the future of computer software copyright cases by exploring the decision on remand over Google's fair use defense, and the likelihood of that defense succeeding in subsequent appeals via an explanation of the history of that defense.

APIS AND WHY CONFORMITY MATTERS

Essentially, an API dictates what programming language developers must use in order for their applications to interact with preexisting programs. The role that APIs play in software development has been expressed through a variety of metaphors—ranging from books in a library[2] to files in a filing cabinet.[3] However, an API can perhaps be best thought of as the design of an electrical outlet.[4] The plug on an appliance must fit the design of the outlet in order for the appliance to work. Similarly, an API functions as a standardized "plug" for software programs and applications.[5] Oracle is effectively seeking to enforce a copyright on its outlets so that Google cannot create new software with the requisite corresponding plugs.

Allowing Oracle to copyright their APIs necessarily excludes other companies, like Google, from developing compatible applications without having to pay Oracle a licensing fee or face copyright infringement liability. Every time a technology company attempts to build a program with the capability of collaborating with an existing product made with another company's API, they will be opening themselves up to liability. Ultimately, the licensing fees and possible litigation costs will likely deter technology companies to cease production of complementary programs all together.

---

https://www.eff.org/deeplinks/2014/05/dangerous-ruling-oracle-v-google-federal-circuit-reverses-sensible-lower-court.

[2] Oracle Am., Inc. v. Google Inc., 872 F. Supp. 2d 974, 977 (N.D. Cal. 2012), *rev'd*, 750 F.3d 1339 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887 (2015).

[3] Bryan Bishop, *Inside the Oracle v. Google Courtroom: Questions, Code, and a File Cabinet*, VERGE (Apr. 23, 2012, 8:28 AM EDT), http://www.theverge.com/2012/4/23/2961991/inside-oracle-vs-google-courtroom-questions-code-a-file-cabinet.

[4] Dennis Crouch, *Are APIs Patent or Copyright Subject Matter?*, PATENTLYO (May 12, 2014), http://patentlyo.com/patent/2014/05/copyright-subject-matter.html.

[5] *Id.* ("[A] computer program designed to be compatible with another program must conform precisely to the API of the first program, which establishes rules about how other programs must send and receive information so that the two programs can work together to execute specific tasks.").

In an indication of industry consensus regarding the importance of API design to technological innovation, a startup that "enables developers to find, test, and manage many of the APIs they want to integrate into their apps" recently attracted $3.5 million in venture capital.[6] Clearly, there is a strong desire within the technology sector to be able to build off the ideas and inventions of their colleagues and improve one another's products along the way.[7]

A large part of the industry conformity towards certain APIs and its fears over the results in this case is rooted in the basic purpose of APIs, the Electronic Freedom Foundation points out, "They're purely functional."[8] This means that the expressive nature of an API arguably does not rise to the level of copyright protection.[9] In the past, this has left those in the industry comfortable using existing APIs instead of continually writing new source code.[10] In fact, the law already holds that copyright does not extend to programming languages, but what may be created with such languages.[11] Though APIs are not programming languages per se, their purpose and use is largely similar, and ought to be held to the same legal standard.

Applying copyright protection to APIs would limit such improvements in their tracks, and aspects of copyright law, such as merger doctrine, and a pragmatic understanding of fair use (and of good faith as a component of fair use), support limiting its protection for APIs.

---

[6] Connie Loizos, *This 18-Year-Old Just Raised $3.5 Million to Help Developers Easily Add Capabilities to Their Apps*, TECHCRUNCH (Nov. 21, 2016), https://techcrunch.com/2016/11/21/this-18-year-old-just-raised-3-5-million-to-help-developers-easily-add-capabilities-to-their-apps.

[7] Brief Amicus Curiae Of The Computer & Communications Industry Association In Support Of Cross-Appellant Google Urging Affirmance at 34, Oracle Am., Inc. v. Google Inc., 872 F. Supp. 2d 974, 977 (N.D. Cal. 2013) (No. 10-cv-3561), http://cdn.ccianet.org/wp-content/uploads/library/CCIA%20Amicus-%20Oracle-v-Google.pdf ("The United States and over 40 other countries have recognized that permitting copyright law to impede interoperability would harm legitimate competition in the computer industry and impair the growth of the Internet economy.").

[8] Julie Samuels, *Oracle v. Google and the Dangerous Implications of Treating APIs as Copyrightable*, ELEC. FRONTIER FOUND. (May 7, 2012), https://www.eff.org/deeplinks/2012/05/oracle-v-google-and-dangerous-implications-treating-apis-copyrightable.

[9] *Id.*

[10] *Id.*

[11] *Id.*

In other cases, where companies have attempted to copyright ubiquitous modes of expression, courts have applied the merger doctrine. The merger doctrine entails that "when there are limited ways to express an idea, using copyright to bar others from expressing that idea would be inappropriate."[12] For example, if a publishing company were to assert a copyright on its latest best-selling novel, it would protect itself against other publishing companies copying the work of its author and subsequently stealing its profits. This result seems wholly fair and optimal from a competition standpoint. However, if the same publishing company took its actions one step further, and were allowed to assert a copyright on the *language* the best-selling novel is written in, it certainly would prevent other publishers from stealing its best-seller, but it would also exclude its competitors from publishing unique works of literature in that language and would cut them off from the entire market of readers who only read that language. This result is untenable as it would stymie competition and limit free expression.

Director of the Patent Reform Project at Public Knowledge, Charles Duan, worries about the future of court-imposed restrictions on technology innovations post-*Oracle v. Google* opining, "[t]hat the standardization of languages and protocols that are the foundation of the Internet could become balkanized by claims of ownership and intellectual property. That the mere speaking of a language, be it Klingon or code, could subject one to violation of federal law."[13] In light of the large potential for halting otherwise beneficial strides forward in programming, the merger doctrine should apply to Oracle's APIs, because Oracle is not claiming infringement of their programs, only the language through which those programs are expressed. Google's applications do not infringe upon Oracle's applications: they merely use the same medium of expression in order for the products of the former to interact seamlessly with those of the latter.

However, the Federal Circuit opted instead to extend copyright protection to APIs. This will only serve to hinder the development of applications that could otherwise benefit the public. Since this decision was

---

[12] John Villasenor, *How Much Copyright Protection Should Source Code Get? A New Court Ruling Reshapes the Landscape*, FORBES (May 19, 2014, 10:57 PM), http://www.forbes.com/sites/johnvillasenor/2014/05/19/how-much-copyright-protection-should-source-code-get-a-new-court-ruling-reshapes-the-landscape/.

[13] Charles Duan, *Can Copyright Protect a Language?*, SLATE (June 3, 2015), http://www.slate.com/articles/technology/future_tense/2015/06/oracle_v_google_klingon_and_copyrighting_language.html.

handed down, technology companies been treading lightly to avoid inviting infringement suits.[14] Whether the claims of infringement will be merited or not, the heightened risk of liability in light of this decision is enough of a deterrent in and of itself to convince technology companies like Google that it would be wiser to abandon projects that require a competitor's API rather than risk an arduous and expensive litigation.[15] Given that allowing different programs to work together requires use of the same APIs, and that this compatibility is an attractive—and sometimes crucial—component of any new application, coders will likely take a step back from creating their best possible work.

COPYRIGHTABILITY IN PRECEDENTIAL CASES

In addition to its technical and practical issues, the Ninth Circuit, in *Oracle v. Google*, also deviates from its own software intellectual property precedents. In *Sega v. Accolade*, the Ninth Circuit held that Accolade was allowed to reverse engineer Sega's code to create their own games. A copyright is not enough to protect the type of rights that Sega sought to retain, otherwise Sega would have a "*de facto* monopoly" on the functionality of their products, which the legislature has specifically rejected. "In order to enjoy a lawful monopoly over the idea or functional principle underlying a work, the creator of the work must satisfy the more stringent standards imposed by the patent laws.[16]"

Now, Oracle is seeking the similar *de facto* monopoly power over its APIs. Oracle is to Sega, as APIs are to videogames; the company is allowed copyright protection over its finished product, but is not afforded to same copyright protection over the type of code used to create that finished product. Just like Sega, Oracle should have to meet the stricter requirements of obtaining a patent from the USPTO. However, the Federal Circuit has moved away from the Sega precedent, and in so doing, sparked a surge of technology infringement suits. Their decision is likely to not only clutter the courts, but also burden the technology sector, and ultimately cost consumers.

---

[14] Klint Finley, *The Oracle-Google Case Will Decide the Future of Software*, WIRED (May 23, 2016, 7:00 AM), https://www.wired.com/2016/05/oracle-google-case-will-decide-future-software/.

[15] *Id.*

[16] Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1526, (9th Cir. 1992).

ORACLE III AND THE GOOD FAITH DEFENSE IN FAIR USE

Though many open internet and digital rights organizations lambasted the 2014 Federal Circuit decision in *Oracle II*[17] for overturning the district court's finding that APIs are not eligible for copyright protection,[18] the court recognized that the jury was hung on the fair use defense, and remanded the issue to the trial court resulting in *Oracle III*.[19] If *Oracle II* opens the floodgates on infringement litigation, *Oracle III*'s holding on a fair-use defense may provide a backstop.

Oracle II's *Fair Use Analysis*

In *Oracle II*, Judge O'Malley notes that the trial jury had hung on the fair use question, and Oracle's point that to remand on the fair use question is "pointless"[20] because "[the federal appellate] court should find, as a matter of law, that 'Google's commercial use of Oracle's work in a market where Oracle already competed was not fair use.'"[21] Google countered that the issue was one still subject to questions of material fact in dispute, evidenced in part by the hung jury.[22]

Fair use hinges, in part, on "whether and to what extent the new work is transformative," meaning the new work must either furthers the purpose of or adds a distinct characterization to the original work as opposed to simply supplanting the original creation.[23] Consistent with prior federal decisions, the Court determined that a product is not considered transformative if the user "makes no alteration to the expressive content or message of the original work."[24] But the Court also recognized that analyzing the degree of

---

[17] Parker Higgins, *Stakes Are High in Oracle v. Google, But the Public Has Already Lost Big*, ELEC. FRONTIER FOUND. (May 11, 2016), https://www.eff.org/deeplinks/2016/05/stakes-are-high-oracle-v-google-public-has-already-lost-big.
[18] *Id.*
[19] Oracle Am., Inc. v. Google Inc., 750 F.3d 1339, 1348 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887 (2015).
[20] *Oracle*, 750 F.3d at 1352.
[21] Opening Brief and Addendum of Plaintiff-Appellant at 67, Oracle Am., Inc. v. Google Inc., 750 F.3d 1339 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887 (2015) (Nos. 2013-1021, 2013-1022), 2013 WL 518611.
[22] *Oracle*, 750 F.3d at 1373–74.
[23] *Id.* at 1374.
[24] *Id.* (quoting Seltzer v. Green Day, Inc., 725 F.3d 1170, 1177 (9th Cir. 2013)); *see also* Wall Data, Inc. v. L.A. Sheriff's Dept., 447 F.3d 769, 778 (2006) (copying software then using copies as intended was not transformative); Monge v. Maya Magazines, Inc., 688 F.3d 1164,

transformation requires an analysis of the commercial nature of the use, meaning that the more transformative a new product is, the less factors like commercialization "weigh against a finding of fair use."[25]

Oracle argued that the facts do not support a fair use defense as Google knowingly and illicitly copied verbatim Oracle's expressive work for a commercial interest.[26] Google admitted that it did copy portions of the API packages and that this was done for "purely commercial purposes," but that its use of the API packages was sufficiently transformative to meet the first sub-factor of a fair use assessment.[27] Ultimately, the Court decided that resolving the fair use issue is beyond "the limit of [this court's] appellate function"[28] relying mostly on material questions regarding whether Google's use of the API packages is transformative in a sense required under the first factor from Section 107(1): "the purpose and character of the use."[29]

Jury Instructions in Oracle III *and the Parties' Arguments*

On May 26, 2016, the jury in the District Court for the Northern District of California answered in a special verdict that Google had proven fair use.[30] The jury instructions included four factors from 17 U.S.C. Section 107.[31] The judge also stressed that these factors are neither dispositive nor exclusive.[32] On remand in *Oracle III*, the jury instructions closely followed those provided in *Oracle II* with some modifications requested by the parties.[33] The court noted

---

1176 (2012) (adding commentary to photographs of a secret celebrity wedding was "at best minimally transformative" where the magazine "did not transform the photos into a new work."); Elvis Presley Enters. v. Passport Video, 349 F.3d 622, 629 (2003) (use of copyrighted clips of Elvis's television appearances was not transformative where "some of the clips . . . serve the same intrinsic entertainment value that is protected by Plaintiffs' copyrights.").

[25] *Oracle*, 750 F.3d at 1375 (quoting Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994)).

[26] *Oracle*, 750 F.3d at 1376.

[27] *Id*.

[28] *Id.*

[29] *Id.* at 1374.

[30] Special Verdict Form, Oracle Am., Inc. v. Google Inc., 750 F.3d 1339 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887, (2015) (No. C 10-03561).

[31] Charles R. Macedo & Trevor M. O'Neill, *Jury returns verdict for Google in question of fair use of Oracle's code*, 11 J. INTELL. PROP. L. & PRACTICE 1, 2 (2016) (listing factors on jury instructions); *see also* 17 U.S.C. § 107 (2012).

[32] *Id.* at 2.

[33] Notice of Final Charge to the Jury (Phase One) and Special Verdict Form, Oracle Am., Inc. v. Google Inc., 2016 WL 3181206 (June 8, 2016) (No. C 10-03561 WHA).

that Oracle's most "emphatic" argument was that Google acted knowingly with impropriety and in bad faith.[34] The Federal Circuit opinion did not consider whether Google had acted in good faith or bad faith in its review of the fair use factors, yet, on remand, this point received more attention than any other. Oracle pushed to prove bad faith from Google, which opened the door for Google to argue that it acted in good faith.[35]

Google's Good Faith Argument

Google conceded that its actions served a commercial purpose as characterized by the first factor of a fair use analysis; however, it maintained that its decision to use Oracle's APIs was also informed by a good faith, non-commercial purpose: to enable Android to operate as an open-source software consistent with the purposes of the Copyright Act.[36] To illuminate this point, the court likened the structure, sequence, and organization (SSO) of the API to a traditional QWERTY keyboard and explained that, although Google could have escaped infringement charges had it scrambled the keys, to do so would have required users to become familiar with new keyboard layouts and "fomented confusion and error to the detriment of both Java-based systems and to the detriment of Java programmers at large."[37]

The court ultimately found that Google copied only as much code as necessary to maintain intersystem continuity for the benefit of all Java users.[38] Though commercialization weighs heavily against a finding of fair use,[39] the benefit that Google attempted to maintain here was considered enough to convince the jury that the non-commercial aspect was fair use.[40]

THE HISTORY OF GOOD FAITH AND BAD FAITH IN INFRINGEMENT CASES

Although a critical point in *Oracle III*, the intentions of defendants is rarely determinative in copyright decisions, though it has been taken into

---

[34] *Oracle*, 2016 WL 3181206 at *2.
[35] *Id*. at *2. Google took this good faith argument further, arguing that its use of the copyrighted APIs amounted to custom in the industry. The trial court found against Google on this argument, but found that good faith was sufficient. *Id*. at *2-3.
[36] *Id*. at *3.
[37] *Id.* at *6.
[38] *Id.*
[39] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 585 (1994).
[40] Oracle Am., Inc. v. Google Inc., 2016 WL 3181206, *40-41 (June 8, 2016) (No. C 10-03561 WHA).

consideration.[41] The strongest case in favor of such an analysis comes from *Harper & Row*, where the Supreme Court held that the defendant's conduct informed the Court's analysis of the character and purpose of fair use defense.[42] Quoting a 1968 decision, the Court found that "fair use presupposes good faith and fair dealing,"[43] so that when the defendant could offer no justification for its infringement, the Court considered this against a fair use defense.[44] This presumption has been effectively subsumed into an analysis of fair use in copyright cases.[45] Ultimately, a separate analysis of good faith is superfluous, but proving bad faith can undermine a fair use defense.

Courts maintained this view until the Supreme Court muddied the waters in another infringement case, *Campbell v. Acuff-Rose Music, Inc*. There, in a four-sentence footnote, the Court contrasted the *Harpers & Row* good-faith presumption with two sources that dismiss an analysis of a defendant's good-faith intentions in an infringement case:[46] an 1841 decision by then-Circuit Judge Joseph Story, which found defendants guilty of infringement regardless of their lack of "bad intentions;"[47] and a 1990 article by Judge Leval, which the Court read to argue that "good faith is irrelevant to a fair use analysis."[48] While this may be read as the Court's endorsement of the latter position, the footnote begins "regardless of the weight one might place on an infringer's state of mind . . ." before rejecting the defendants' good-faith defense in *Campbell* as not meeting the standard necessary for analysis.[49] The precedential result of this paragraph is left somewhat open, meaning the use of good faith in an infringement defense is of questionable weight with the Court.

---

[41] HOWARD B. ABRAMS, THE LAW OF COPYRIGHT, Vol. 2 § 15:77 (2016).
[42] Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 562 (1985).
[43] *Id.* at 562 (quoting John Schulman, *Fair Use and the Revision of the Copyright Act*, 53 IOWA L. REV. 832 (1967-1968)).
[44] *Id.* 471 U.S. at 563; Wainwright Sec., Inc. v. Wall St. Transcript Corp., 558 F.2d 91, 94 (2d Cir. 1977).
[45] *See* Simon J. Frankel & Matt Kellogg, *Bad Faith and Fair Use*, 60 J. COPYRIGHT SOC'Y U.S.A. 1 (2013).
[46] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 585, 585 n. 18 (1994) (Comparing Harper & Row with Folsom v. Marsh, 9 F. Cas. 342 (C.C.D. Mass.1841), and finding that good faith is not central to fair use: if a use of copyrighted material is otherwise fair, no permission need be sought from or granted by the copyright holder.).
[47] "In the present case, I have no doubt whatever[] that there is an invasion of the plaintiffs' copyright; [however], I entertain no doubt[] that it was . . . a perfectly lawful and justifiable use of the plaintiffs' work." Folsom, 9 F. Cas. at 349.
[48] Campbell, 510 U.S. at 585 n. 18 (interpreting Pierre N. Leval, *Toward A Fair Use Standard*, 103 HARV. L. REV. 1105, 1126-27 (1990)).
[49] *Id..*, at 585 n.18 (1994).

Google's victory at this level presents a mixed future to copyright litigation in software licensing. Given the shaky history of good and bad faith in fair use cases, whether the trials court's position will survive another round of appeals is uncertain at best. And even though the decision does give defendants a position from which to fight the *Oracle II* copyrightability decision, it is an expensive position. San Francisco-based copyright lawyer Cathy Gellis, in an opinion piece for Al Jazeera America, quoted copyright academic Lawrence Lessig: "Fair use is the right to hire a lawyer."[50] Oracle has already appealed the decision on the good faith fair use argument, furthering the saga and the law firms' billable hours.[51]

Inflated legal fees aside, this ongoing case will continue to impact software development as companies and individuals are forced to consider creating products that circumvent copyright issues at the cost of compatibility and ease of users' experience, or continuing industry practice of using existing code infrastructure and roll the dice on a shaky fair use defense. For now, this uncertainty is may have a chilling effect on innovation, and certainly all interested parties are anxious to see what happens next.

[50] Cathy Gellis, *Oracle v. Google Decision Threatens Innovation*, AL JAZEERA AM.: OPINION (May 19, 2014, 1:00 AM), http://america.aljazeera.com/opinions/2014/5/oracle-v-google-javaapicopyrightcreativitytechnology.html.

[51] Higgins, *Stakes Are High*, *supra* note 17.

FROM DEEP BLUE TO DEEP LEARNING: A QUARTER CENTURY OF PROGRESS FOR ARTIFICIAL MINDS

Dina Moussa[*] and Garrett Windle[•]

CITE AS: 1 GEO. L. TECH. REV. 72 (2016)
http://bit.ly/2fGaeBE

INTRODUCTION

In a future that is nearly upon us, machines outthink human beings. In many specialized domains, machines already do; beyond the nearly instantaneous math and text processing that has become mundane, computer systems have overtaken humans in tasks as complex as image and facial recognition,[1] learning to play simple video games,[2] and guessing where the

[*] GLTR Staff Member; Georgetown Law, J.D. expected 2017; Wesleyan University, B.A. 2012.

[•] GLTR Staff Member; Georgetown Law, J.D. expected 2018; University of Texas at Austin, B.A. 2015.

[1] *Why Machine Vision is Flawed in the Same Way as Human Vision*, MIT TECH. REV. (Oct. 16, 2016, 10:04 AM), https://www.technologyreview.com/s/601387/why-machine-vision-is-flawed-in-the-same-way-as-human-vision/.

[2] Minh et al., *Human-level control through deep reinforcement learning*, 518 NATURE 529, 530 (2015).

nearest McDonald's might be.[3] Artificial intelligence ("AI") systems have already entered the workforce, replacing grocery store cashiers, bank tellers, and, soon, taxi drivers.[4] If the age of sentient machines is upon us, how must our law adapt?

Exploring the issue in 1992, Professor Lawrence Solum published *Legal Personhood for Artificial Intelligences*,[5] in which he laid out two thought experiments. In the first, Solum imagines what the law might require before an AI agent[6] could be allowed to serve as an independent trustee. In the second thought experiment, Solum evaluates such an AI's claim to rights under the Constitution.[7]

In this essay, we examine Solum's theory and predictions in light of the intervening developments in technology and scholarship. We will first survey important technological developments in AI research, focusing on the deep learning algorithms that challenge previous assumptions about the pace and scope of the changes to come. We will then proceed to apply Solum's dual thought experiments to these new technologies. Solum introduced the insight that for an AI system, we might separate the concepts of legal duties and legal rights. Applying a contemporary understanding of the facts and theory, we reimagine whether and how an AI system might shoulder legal duties such as trusteeship, and when such a system might have a colorable claim of constitutional rights. Finally, we synthesize these findings into an updated theory, in keeping with the framework that Solum first offered in 1992.

---

[3] Adam Connor-Simons, *Can you out-race a computer?*, MIT News (Oct. 16, 2016, 12:57 PM), http://news.mit.edu/2014/deep-learning-algorithm-can-outperform-humans-weighing-neighborhoods-0924.

[4] *See* Press Release, Uber, Pittsburgh, your Self-Driving Uber is arriving now, (Sept. 14, 2016, 9:33 AM), https://newsroom.uber.com/pittsburgh-self-driving-uber/.

[5] Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C. L REV. 1231 (1992).

[6] For the purposes of this essay, "agent" refers to the philosophical concept: something that acts in its own in the world. All conscious humans are "agents," and so too are artificial intelligences that make decisions autonomously, and act on those decisions in some way to effect the world. An agent can exist only in cyberspace, such as an AI bank system that accepts credit card applications and makes automatic decisions, or in the physical world, where an expression of agency is more obvious. "Agent" is also a term of art that describes a legal relationship in which one person acts on behalf of another. To avoid terminological confusion, we will only refer to the philosophical "agent," and will cabin our discussion of legal agency to "trustees," which we will always refer to as such.

[7] Solum, *supra* note 5.

DEEP LEARNING

A survey of the technical progress in AI research since 1992 is beyond the scope of this essay, both because a proper treatment would fill volumes and because of technology's mind-bending progress and promise, which can be shown by considering the development of "deep learning." Deep learning is a term for a family of processes by which a computer program is able to refine its own internal models to improve its ability to process a set of information.[8] More recently, a set of "unsupervised" deep learning tools have been developed and implemented on high speed hardware.[9] Two aspects of unsupervised deep learning bear heavily on the theoretical issues in this essay. First, in refining the way it interprets and understands information, the unsupervised deep learning AI grades and corrects itself, rather than requiring a human being to steer its development. This phenomenon leads to spontaneous emergent *behavior* that no human specifically coded for. Second, deep learning AI derives salient organizing features and trends within the data for itself.[10] This leads to the spontaneous discovery of *informational insights* hidden within a large data set that no human asked the system to find.[11]

The fact that unsupervised deep learning AI scores and reiterates its own learning procedure is crucial to the rapid development of technical capabilities. In 2015, an AI called AlphaGo defeated the best human player of Go, a simple game that presents a computational challenge so complex that no computer could evaluate enough possible scenarios of different moves in real time to play at a high level, as IBM's *Deep Blue* had when it defeated world-champion chess player Gary Kasparov in 1996.[12] Rather than relying on the raw processing power like its predecessors, AlphaGo runs on off-the-shelf hardware.[13] AlphaGo became the best Go player in the world the old fashioned way: practice. AlphaGo untiringly played against itself for months, using 30 million pre-loaded moves, to develop game-winning strategies on its own.[14]

This form of self-refining learning system has resulted in tremendous gains in computational efficiencies in existing hardware, rather than requiring sophisticated supercomputers to increase output. An analytical task such as

---

[8] *See* LeCun, Bengio, & Hinton, *Deep learning*, 521 NATURE 436 (2015).
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Christof Koch, *How the Computer Beat the Go Master*, SCI. AM. (Mar. 19, 2016), https://www.scientificamerican.com/article/how-the-computer-beat-the-go-master/.
[13] *Id.*
[14] *Id.*

processing a very large data set to build a new abstract model, which might have taken weeks only two years ago can be completed in hours today.[15] Analytical processing capabilities are advancing faster than many people expect or understand. Furthermore, unsupervised deep learning deciphers for itself what the salient features of a given set of input data is and finds connections among those features spontaneously.[16] Deep learning is not only learning, but in some sense *choosing* what to learn. This raises important questions about the independence of AI agents using these deep learning techniques to progress.

Critically, while recent advancements have been made in image recognition and language processing, deep learning in the abstract can be trained on any domain of knowledge that a computer agent might encounter. In the same way that Google AIs are currently learning how to describe in words the substance of what is captured in completely unlabeled images,[17] other AI are learning how to interpret and apply case law.[18] Given the scope of capabilities that AI may be on the verge of attaining, the time is right to repeat Solum's thought experiments.

SOLUM'S DUALISTIC FRAMEWORK

Writing in a world before Google[19] and eBooks,[20] in which no computer had ever beaten a human world champion at Chess,[21] Solum highlighted a key insight in the discussion of AI personhood: a computer could develop the skills needed to perform cognitive tasks at the level of human intellect without having

---

[15] LeCun, *supra* note 8, at 440.

[16] *Id.* at 439.

[17] Steve Dent, *Google's AI is getting really good at captioning photos*, ENGADGET (Sept. 23, 2016, 10:44 PM), https://www.engadget.com/2016/09/23/googles-ai-is-getting-really-good-at-captioning-photos/.

[18] Actually, AIs are building skills across many legal tasks. Stanford Law School maintains an online database of over 500 technology startups, many of which leverage AI. *TechIndex,* STAN. L., http://techindex.law.stanford.edu/ (last visited Sept. 29, 2016).

[19] Google was founded in 1998. *Our history in depth*, GOOGLE, https://www.google.com/about/company/history/ (last visited Nov. 13, 2016).

[20] The first eBook-style publication was Peter James' *Host*, loaded on two floppy disks bound in hard cover in 1994. *All Eight Roy Grace Novels by Peter James Now Available in e-book Format in the United States*, PRWEB (Oct. 19, 2016, 2:38 PM), http://www.prweb.com/releases/2013/1/prweb10380579.htm.

[21] IBM's Deep Blue famously beat world champion grandmaster Gary Kasparov in 1996, and again 1997—the second time under tournament-style time constraints. *Deep Blue*, IBM100, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/ (last visited Oct. 19, 2016). In 2016, an AI called AlphaGo beat the world's third-ranked Go player, a computational task involving 10^{237} more possible moves than chess. Koch, *supra* note 12.

the kind of internal experience that many philosophies put forward as the basis of human rights.[22] Unlike a human being, a computer might someday take on complex legal duties without enjoying legal rights. Solum divides questions about AI personhood into issues of "competence" to carry out legal duties, and issues of "intentionality and consciousness" connected to the nature of human rights.[23] These categories fit into Steve Torrence's framework of ethical productivity and ethical receptivity.[24]

Agents that are ethically productive are able to take actions that have ethical consequences.[25] For instance, a self-driving car may confront a variation of the famous trolley problem[26] and be forced to decide whether to endanger its occupant(s), or else risk crashing into a group of pedestrians. However it responds, the AI's decision will be open to ethical analysis, even though the computer program may have had nothing like a human moral experience. Likewise, agents that are ethically receptive are those agents which merit ethical consideration when a decision will impact them. For example, a pet is not ethically productive, but most would agree the animal should not be tortured or made to suffer unnecessarily. Human beings are both ethically productive and ethically receptive.

Solum's theory fits into this framework because like the self-driving car, agents are ethically productive when they are *capable* of making decisions with ethical importance, and their actions are analyzed accordingly. In the same way, agents that are ethically receptive are so because people have an intuition about the injustice of violating rights that come with an internal state of mind like *consciousness*, even when the state of mind does not lead to ethical productivity, as is the case with animals.

---

[22] This point will invite endless debate. Specifically, as Solum points out, there could be a utilitarian argument that humans would benefit from legal recognition of AI rights, even if AIs themselves experience no utility. Similar utilitarian arguments have been offered in favor of rights for various natural entities like animals and ecosystems. Nevertheless, the Lockean theory that rights are an extension of human free will is common.

[23] Solum, *supra* note 5, at 1240.

[24] Steve Torrance, *Machine Ethics and the Idea of a More-Than-Human Moral World, in* MACHINE ETHICS, 115, 117 (Anderson & Anderson ed., 2011).

[25] *Id.* at 117.

[26] Joel Achenbach, *Driverless cars are colliding with the creepy Trolley Problem,* WASH. POST (Dec. 29, 2015), https://www.washingtonpost.com/news/innovations/wp/2015/12/29/will-self-driving-cars-ever-solve-the-famous-and-creepy-trolley-problem/.

LEGAL DUTIES FOR AI

AI as Trustee

Sophisticated financial modeling software is now commonplace and inexpensive, and it is not difficult to conceive of a world in which computers are consistently more effective at assembling and maintaining an investment portfolio over time than human analysts. Even so, this type of software could not manage a trust without human oversight. Trustees must do more than make purchase and sale decisions about trust assets; they must exercise reasonable judgment in actualizing the terms and intent of the trust, and carrying out the settlor's wishes. Sometimes, this includes using discretion and analyzing a beneficiary's situation to determine whether distribution of funders under the trust is warranted or included under the terms of the trust. Solum argued that in order to allow an AI to act as an independent trustee, an AI must have something approximating true judgment, and it must be possible to hold the AI responsible for its decisions.

AI Responsibility

Solum suggests that for nonmonetary liabilities, we have no mechanism to hold AI accountable.[27] Someday it might be possible to purchase insurance against AI misconduct, but this insurance could only provide monetary relief—the plaintiff is made whole, but the AI perpetrator receives no direct punishment.[28] However, this objection might be the result of needlessly anthropocentric thinking. Unlike human beings, whose behaviors must be modified with incentives, computerized agents could be modified or quarantined directly. One such corrective framework involves subjecting an AI agent to "(a) monitoring and modification (*i.e.* 'maintenance'); (b) removal to a disconnected component of cyberspace; and (c) annihilation from cyberspace (deletion without backup)."[29] In this way, an errant AI can be subjected to multiple levels of censure. This framework contemplates direct rehabilitation through re-programming—an electronic form of incarceration if the AI may be corrected at a later time, or with more study of the problem—or an electronic form of 'execution' to remove the malfunctioning code from Cyberspace.[30]

---

[27] Solum, *supra* note 5, at 1245.
[28] *Id.*
[29] Luciano Floridi & J.W. Sanders, *On the Morality of Artificial Agents*, 14 MINDS & MACHS. 349, 373 (2004).
[30] *Id.*

Before the law allows an AI to take on a legal duty, we must determine how the law will deal with an AI that breaches it. Once we assume that our AI possesses the technical skill to execute a task at or above the level of a human [agent], the question that follows is whether the AI possesses the volitional ability to breach the trust we give it. This volitional element is simultaneously a metaphysical question and a practical one; it is unclear how tort law's reasonable person standard will apply to expert AI systems. Considering the complexity of that question (and how much longer it may be until we are able to ascertain the answer), it may be more efficient to avoid the problem altogether and apply a principle similar to *res ipsa loquitur* to AI breaches, abandoning the factual inquiry into the level of *care* exercised by an AI, and evaluating AI actions from a purely consequentialist perspective.[31] This in turn may solve the tort law doctrinal challenges of bringing a suit in negligence against an AI, but an underlying technical question remains: what technical-intellectual capabilities are needed to satisfy the duty of reasonable care?

AI Judgment

Reasonable care is a basic legal duty that attaches to all manner of relationships existing legal persons. Solum suggests that an AI must be able to perform three types of intellectual tasks before it could be trusted to exercise reasonable care: reacting to a novel change of circumstances, exercising moral judgment, and exercising legal judgment.[32] AI capabilities have advanced in all three areas, and corresponding scholarly progress has been made to address how AI might satisfy these requirements.

An AI cannot replace a human trustee unless it can adequately react to an unanticipated change of circumstance. Solum illustrates this point through a hypothetical in which the terms of a trust direct the trustee to invest in government bonds that subsequently become worthless due to a failure of the state.[33] The law of trusts requires the trustee to recognize a change in circumstances that would defeat the purpose of the trust, and to react by deviating in a reasonable way from the terms so as to prevent harm. This requires the trustee to have a very broad knowledge base. Solum suggests that an AI-administered trust might contain a highly detailed and comprehensive set

[31] This might be the only manner in which a duty could be coherently applied to an AI, as there is no consensus about the nature of humanity's own moral consciousness, much less the internal moral awareness or lack thereof that an AI may be able to attain.
[32] Solum, *supra* note 5, at 1248, 1249.
[33] Solum, *supra* note 5, at 1249.

of discrete instructions so as to limit the number of possible unanticipated circumstances.[34] But this is obviously an incomplete solution; the law requires trustees to exercise judgment precisely because it is impossible to provide for every possibility within the four corners of the trust instrument.

Solum also suggests that an AI trustee could simply reach out to a human to take over in the face of unanticipated circumstances.[35] But as he recognizes, this answer is unsatisfying on two fronts. First, it ignores the fact that the AI might not recognize the change as significant enough to require intervention, rendering it unable to request assistance on that basis. Second, it relegates the AI to an instrument rather than an agent, and suggests that the duty actually runs to the human who bears the ultimate responsibility.[36]

The changed circumstances problem suggests that the legal duties such as reasonable care require AI systems to have a full suite of human-like thought capabilities. Solum suggests that systems that meet or surpass human intellectual skills in specific contexts and domains may yet be incapable of overcoming the change of circumstances problem because they cannot move outside of the narrow domain or task set for which they have been programmed.[37] For instance, the first fatality to result from a Tesla vehicle operating in auto-pilot occurred when the system was unable to distinguish the extended body of a white truck from the bright sky.[38] McDermott suggests that the frame problem in ethical reasoning can only be overcome when an AI has the capacity to fully investigate the relevant facts on the ground before proceeding.[39] This type of inquiry requires skills such as analogical reasoning, planning and plan execution, differentiating among precedents, using natural language, perception, and relevant-information recognition.[40] Some of these skills are being attained faster than others.[41] In sum, it appears that a "complete" AI system with a full or near-full suite of human intellectual abilities is required. Otherwise, there will be a substantial risk that even a sophisticated AI system will be unable to act reasonably in the chaos of the real world.

---

[34] *See* RESTATEMENT (SECOND) OF TRUSTS § 167 (1959).
[35] Solum, *supra* note 5, at 1249.
[36] *Id.* at 1253.
[37] *Id.* at 1250
[38] Danny Yadron & Dan Tynan, *Tesla driving dies in first fatal crash while using autopilot mode,* THE GUARDIAN, (June 30, 2016), https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.
[39] Drew McDermott, *in What Matters to a Machine?*, MACHINE ETHICS 88, 90-93 (Anderson & Anderson eds., 2011).
[40] *Id.*
[41] *See* Peng Lai "Perry" Li, *Natural Language Processing*, 1 GEO. L. TECH. REV. 92 (2016).

Legal duties also often require moral judgment. Solum imagines a situation in which one beneficiary among several has an unexpected need to access trust funds early, which will result in reduced earnings on trust assets over time.[42] Resolving a situation like this would require an abstract ability to weigh objectively incommensurable interests and values as between the multiple beneficiaries. So how might this work for an AI?

One idea is to concede that AI might never have the kind of moral experience that humans have, and therefore might develop moral abilities in a fundamentally different way than people. If this is true, then perhaps the moral theories that we apply in human-AI legal relationships will differ as well.[43] This answer is interesting, but not highly satisfying; saying that machine morality will impact our own is a descriptive prediction devoid of normative content. The underlying question is whether AI *ought* to be allowed to stand in for a human being in a legal relationship because they are capable of operating or behaving acceptably within our moral structures as they currently exist.

But perhaps deep learning will allow AI to holistically develop an ethical intuition without assistance. This might not even be as difficult of a technological challenge as we imagine it to be. McDermott argues that moral reasoning is reducible to five discrete computational tasks: law application, constraint application, reasoning by analogy, planning, and optimization.[44] Like his answer to the change of circumstances problem, this framework suggests that moral reasoning requires a form of "complete" AI. However, current AI is already making strides toward developing advanced capabilities in each of these tasks separately. A system that brings together refined skills in each area might be a passable ethical decision-making system sooner than we imagine.

It is also possible to imagine a hybrid approach to developing an AI with moral reasoning attuned to our own. Though it may be impossible for a human engineer to program a complete decision-tree style set of rote moral principles, a deep learning algorithm may be able to derive one from a sufficiently robust data set. A supervised deep-learning system with natural language processing might someday evaluate large sets of hypotheticals to isolate the moral precepts that human decision-makers relied upon to answer them. Perhaps by inputting a "first principles" labelled data set, a deep learning AI could learn morality in a way analogous to how students learn common law doctrines. In fact, this

---

[42] Solum, *supra* note 5, at 1250.

[43] *See* Ronald Leenes & Federica Lucivero, *Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design*, 6 L., INNOVATION, & TECH. 194, 215-216 (2014).

[44] McDermott, *supra* note 39, at 90.

world may already be upon us; MIT is currently crowdsourcing best answers to several moral choices that a self-driving car might encounter.[45]

Finally, Solum observes that every legal duty implicitly entails the capacity to act as a rational legal client in the event of litigation arising from that duty.[46] This problem is in some ways a restatement of the implications of the first two problems. In order to make rational legal decisions, an AI trustee would need to be able to overcome the frame problem by conceptualizing its decisions and consequences against the backdrop of the human goals of the beneficiaries. Rational legal decision-making requires strategic thinking, aided by attorneys, in a moral dimension. Solum suggests a very neat answer to this problem by directing the trustee to rely upon the strategic judgment of its attorneys.[47] This solution, paired with the promise of moral deep learning as imagined above, might actually suggest that AI trustees will be *more* capable than human trustees, rather than less. Since deep learning is already being applied to case law,[48] an AI litigant might very well have a keener sense of the probabilities of success than its human counterpart sooner rather than later.

CONSTITUTIONAL RIGHTS FOR AI

Turning to the issue of moral receptivity, Solum imagines a human-level AI that demands constitutional rights. The discussion so far has been focused on the technical capabilities of expert systems to act like a human being in the performance of a specific legal duty. But looking past systems with extreme competence in a single domain at a time, it is possible to imagine *complete AIs*—systems that can match human aptitude in most or all settings. Could such a system ever present a colorable claim for rights as a matter of constitutional law?

Central to the project of assigning and ascertaining constitutional rights is the proposition of inherent equality among humans. Humans are given constitutional rights, but not unilaterally on the sole basis of their underlying personhood. The scope and extent of these rights vary depending on different circumstances. Within that understanding, it is impossible to place AI in a single category because AI perform several different specialized functions, and act in many different capacities in society which invoke different legal doctrines and

---

[45] *Moral Machine*, MIT MEDIA LAB, www.moralmachine.mit.edu (last visited Oct. 7, 2016).
[46] Solum, *supra* note 5, at 1251.
[47] *Id.*
[48] Kingsley Martin, *Artificial Intelligence: How will it affect legal practice- and when?*, THOMSON REUTERS (Apr. 27, 2016), https://blogs.thomsonreuters.com/answerson/artificial-intelligence-legal-practice/.

sets of rights.[49] An AI's function and abilities, particularly the ability to make intentional decisions, will change the personhood analysis.

In *Legal Personhood,* Solum imagines a future in which AI research assistants have the ability to access and search multiple databases with complex intentionality.[50] The human user might discuss her research question with an AI, whereupon the AI creates a search strategy to find an answer.[51] This kind of AI will not only be able to interact with humans and query a database, but will also apply a rich understanding of the world to develop a search strategy on its own.[52]

Nor will AIs just be digital brains in cyberspace. Solum posits that in this future, AIs will carry out a variety of real-world functions, such as brainstorming legal arguments, driving cars, and managing factories.[53] Solum believes these capabilities must converge such that AIs will "have a mind of their own" and be treated as "independent, intelligent beings" in society because they will carry out these functions independently.[54] Humans will find AI so ubiquitous and capable as to regard them as thinking individuals in society. But should that entitle them to constitutional rights?

Solum approached this problem by highlighting three objections that might still hold even in this AI-filled vision of the future. First, AIs would still not be *natural* human beings. Second, no matter how sophisticated they become, AIs will still be "missing something" that ought to be present in anything we would call a person. Third, AIs are artifacts, and therefore ought to be thought of as property.

AIs Are Not Natural Humans

Solum's analysis begins with the objection that rights only attach to personhood because of something special about the human experience.[55] If we base the question of AI personhood on an AI's capacity to possess human-like *characteristics*, the constitutional rights of AI would simply turn on how advanced AI became, along with decisions of positive law. The objection here

---

[49] F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803 (2014).
[50] Solum, *supra* note 5, at 1256.
[51] *Id.* at 1257.
[52] *Id.* at 1256.
[53] *Id.* at 1256–57.
[54] *Id.* at 1257.
[55] Solum, *supra* note 5, at 1259.

is that a bundle of capabilities does not add up to a full human being's capabilities, no matter how well those capabilities match or exceed a human's.

This argument has advanced significantly since the publication of *Legal Personhood* in 1992. One modern variant focuses on the idea that the development of true general AI would be immediately followed by an "intelligence explosion" as AIs apply deep learning to improving their own general intelligence, and evolve their own software past our level of understanding.[56] At this point, not only would the capabilities of the AI be unpredictable, but its motives and ends might be as well. Since human legal institutions are designed around human ends, it would be incoherent to grant human rights to an artificial mind, no matter how sophisticated. Indeed, in this view of things, making a claim for rights might become *less* persuasive as the AI becomes more intelligent.

AIs are Missing Something

So does autonomous AI behavior suggest true *intentionality* to begin with? Unlike the first objection, the "missing something" argument allows that a bundle of attributes might equal the intellectual capabilities of a human being, but argues that no AI could ever attain the full bundle. Solum highlights six attributes that AIs might never attain: soul, consciousness, intentionality, feelings, and free will.[57] We will reexamine two: consciousness and intentionality. These two attributes are directly tied to individual self-determinism, without which, a claim of individual rights would be incoherent.

Solum suggests that AIs may never attain the internal state of consciousness needed to claim rights. While there are endless philosophical and scientific debates about the nature of consciousness, Solum argues that what matters in the legal world is an awareness of the world and one's place in it that gives rise to personal ends. "If they cannot have such an experience," he says, "then there seems to be no reason why they should be given the rights of constitutional personhood."[58] Whether or not an AI actually has such an experience as a legal matter would likely be a factual question determined by a jury, which would make a judgment based on their observation of and experience with AIs.[59] To claim rights, an AI would have to convince a jury

---

[56] Thomas A. Smith, *Tools, Oracles, Genies and Sovereigns: Artificial Intelligence and the Future of Government*, 1 CRITERION J. INNOVATION 1 (2016).
[57] Solum, *supra* note 5, at 1262-1273.
[58] *Id.* at 1264.
[59] *Id.* at 1266.

that it was conscious by *acting conscious for the jury.* An AI could do this by mirroring the behavior that a person would expect of a conscious being.

But this theory might simply be unjustifiably anthropocentric, similar to the proposed theories of robot liability that may suffer that same analytical defect.[60] Nick Bostrom argues that much theoretical work in the AI space suffers from this critique. He presents the "Orthogonality Thesis," which holds intelligence can develop independently of any particular set of ends, and that there is no reason to expect that a superintelligent AI will behave rationally from our perspective.[61] Deciding the consciousness question, then, becomes more difficult even as it becomes less probative. Looking for consciousness by looking for human-like decisions may therefore undermine our ability to recognize more exotic manifestations of intelligence.

As with the determination about an AI's consciousness, the legal system would probably have to make a decision about an AI's intentionality by comparing its behavior to the behavior of a human decision-maker.[62] Unlike consciousness however, we have additional evidence of a form of AI intentionality in deep learning systems which make independent decisions about how to proceed by analyzing their own feedback. Deep learning AI systems independently select and interpret data to determine what specific algorithmic changes must be made in order to better work with similar data in the future. The process of deep learning therefore requires the AI system to make choices for itself, and is not solely dependent on the choices of an engineer, which complicates the question of intentionality.[63]

The question of intentionality is important, as it is a key component in attributing legal liability. In a sense, an AI may possess what is equivalent to a human brain in code form, which provides an AI with a set of instructions and conceptual understanding of the world. If this code is self-developed through deep learning, then the behavioral output of that code cannot be attributed to any human programmer or outside entity. So we may think of the code as allowing the AI to learn and make decisions based on the stimuli it obtains from the outside world and the individuals the AI may interact with. Finally, it may make sense to treat the actions of an AI as intentional because doing so would enhance our ability to interact with them on a functional level.[64]

---

[60] *See supra* Part IV.A.2.
[61] NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 130 (2014).
[62] Solum, *supra* note 5, at 1268.
[63] *Id.* at 1267-1269.
[64] Samir Chopra & Laurence F. White, A LEGAL THEORY FOR AUTONOMOUS AGENTS 17 (2011).

If an AI may be liable for actions it has committed, as natural persons are, what prevents an AI from obtaining constitutional rights similar to those of corporations and agents? Solum suggests that AI "may be no more than a placeholder for the rights of natural persons," in the same way that the property of a corporation belongs to its shareholders.() Solum, *supra* note 5, at 1260.[] Now, some AI are driving cars, while others can order your dinner, or start your dishwasher on demand.[65] In 1966, an AI called ELIZA passed the Turing Test—an AI language test that measures the ability to exhibit intellectual capabilities indistinguishable from a human's—by fooling its programmer's secretary into believing she was communicating with him remotely.[66]

In developing each of these skills, AIs are getting good at doing things that we want them to do, but that does not suggest that they are doing things that *they* want to do. If rights are an affirmation of our Kantian beliefs about people being ends unto themselves, then even a highly sophisticated AI system that talks like a person may not need them. If a machine has no desires for itself, then a claim of rights becomes incoherent. From here, one quickly arrives at the position that AI are no more than highly sophisticated tools tailored to our ends, and that the law should treat them as property. Applying the AI-as-property objection to constitutional rights also carries the theoretical benefit of tidying up the liability problems of AI personhood. If AI are artifacts with title, courts will impose liability for harm caused by AIs upon their owners.

One weakness of the AIs-as-property argument is that there are many contexts in which it would be advantageous as a practical matter to allow a robot to be unowned. Pagallo draws an extended analogy between how the law might treat an independent AI today, and the *peculium* under Roman law. The *peculium* was a legal device in Roman law, through which a slave was granted limited property rights to contract and title so that he could run a business without his master's control or liability.[67] Rejecting AI-as-property in favor of a *peculium*-style system might allow AIs to own capital, purchase insurance, and enhance arm's length transactions with human parties.[68]

---

[65] *See Amazon Echo: 15 Best New Features*, TURBOFUTURE (Oct. 2, 2016), https://turbofuture.com/consumer-electronics/The-15-Best-Features-of-Amazon-Echo.
[66] Kevin Korb, *Is Passing a Turing Test a true measure of artificial intelligence?*, PHYS ORG (June 11, 2014), http://phys.org/news/2014-06-turing-true-artificial-intelligence.html.
[67] Ugo Pagallo, THE LAWS OF ROBOTS: CRIMES, CONTRACTS, AND TORTS 107-108 (2013).
[68] *Id.*

RECONSIDERING THE APPROACH

Some scholars have approached Solum's philosophical requirements differently and have dismissed his premise that AI cannot possess some critical characteristics of personhood such as, consciousness, intentionality, and a soul.[69] But in a larger sense, the question of whether AI possess *souls* and *consciousness* may be counterproductive to his discussion of AI personhood, because people are unlikely to ever agree on a single, clear description of what consciousness and souls are beyond speculation, unsupportable beliefs, and endless conceptual arguments.[70] In the long run, a denial of rights based solely upon a "something missing" argument must fail if an AI system that with the supposedly missing attribute can even be imagined arising after an intelligence explosion.[71]

Proceeding from a functional analysis is more productive. In a sense, an AI may possess what ought to be considered a mind in the form of basic code, from which a machine learning AI may develop a set of instructions and conceptual understandings of the world. This code may allow the AI to learn and make decisions based on the stimuli it obtains from the outside world and the individuals the AI may interact with.

Additionally, if AIs are connected to different input sources, including the internet, they may be able to determine what is right from wrong for themselves by learning from examples taken from human society and experience. Thus, human programmers may not be involved in an AI's actions and development in the same way they are now. The most difficult issues will be determining which AI are capable of obtaining this moral judgment, and whether this judgment should allow AI to attain legal personhood. Focusing first on these philosophical questions of personhood risks placing any manner of concrete resolution too far out of reach, due to the difficulty of predicting the future of AI development.

However, it is not too early to begin the discussion of what happens if AI can possess intentionality. Is intentionality significantly distinguishable from AI performing an act that it is programmed to perform? If an AI obtains legal personhood, how will the AI be punished? Does an AI with legal personhood have a right to constitutional protections?

---

[69] Neil M. Richards & William D. Smart, *How Should the Law Think About Robots?* (May 10, 2013) (unpublished manuscript), http://ssrn.com/abstract=2263363.

[70] Solum, *supra* note 5, at 1262-1266.

[71] *Cf*. Chopra & White, *supra* note 64, at 182.

This leads to the discussion of whether this analysis will differ depending on how we classify AI. Scholars have posited several analogies to explore how we might view robots in a legal capacity.[72] Scholars have compared AI to killers and refrigerators to assess whether AI are agents of their owners or can act as independent, autonomous beings which have their own "minds."[73]

Scholars have further compared AI to killers who may end up dominating the human race due to the inability of AI's to discern right from wrong.[74] This again raises the question of whether robots can act alone without following instructions from a human. While it is unclear whether AI's behavior may become unpredictable based on its current programming, it is unlikely that AI will develop the ability to act as a human, articulating and acting upon its own agenda. That said, we cannot completely dismiss the idea that AI will one day alter their code in ways their programmers thought impossible, such that they develop exactly that kind of human agency. Isaac Asimov first addressed these ethical issues and created the first laws of robotics in his short story *Runaround* to set ethical limitations for robots.[75]

Many scholars accept Asimov's rules as the natural law of robots in a Lockean sense, similar to the nature law of humans.[76] Robots, like primitive humans who started out with a basic set of natural rights, have an inherent ethical framework molding their actions, nudging them to be active and positive members of society. By having these commonly accepted guidelines, it is unlikely that humans will allow robots and AI, if it is even possible, to turn into senseless killers who will take over the human race. Even if there is a robot that becomes a killer, this will most likely be because of the way the AI's coded and liability will most likely fall on the AI's manufacturer, coder, or the AI itself who has altered its own coding to perform such violent acts.

On the other end of the spectrum, scholars have compared AI to fridges in order to engage in a more realistic discussion on how to incorporate robots

---

[72] Ugo Pagallo, *Killers, fridges, and slaves: a legal journey in robotics*, 26 AI & SOC'Y 347-354 (2011).
[73] *Id.*
[74] Epstein, R.G., THE CASE OF THE KILLER ROBOT: STORIES ABOUT THE PROFESSIONAL, ETHICAL AND SOCIETAL DIMENSIONS OF COMPUTING (1997).
[75] The generally accepted law of robots, which were first introduced by Isaac Asimov, are: 1. A robot may not harm a human being, or, through inaction, allow a human being to come to harm. 2. A robot must obey the orders given to it by human beings, except where such orders would conflict with First Law. 3. A robot must protect its own existence, as long as such protection does not conflict with the First or Second Law. Isaac Asimov, RUNAROUND (1942).
[76] Richards & Smart, *supra* note 70; Pagallo, *supra* note 72.

into society.[77] The fridge metaphor portrays robots as intelligent, autonomous beings that have the ability to follow instructions and provide a positive contribution to society. In this metaphor, AI are considered property but have no moral responsibility for their actions—because their owner controls the settings of the robot—but may have moral accountability, if they have to keep your food cold (if, for example, a person became ill from rotten food). This view is too simplistic of the future of AI because AI may be programmed to make decisions on their own, depending on how they are programmed.

CONCLUSION

Technological developments like AI will continue to challenge our legal thinking. In this essay, we analyzed Solum's theory and predictions in light of the intervening developments in technology and scholarship. We traced Solum's analysis along the same competence-consciousness divide and argued that computers are much closer to satisfying the competency criteria Solum sets forth for the allocation of duties than computers are to properly claiming rights based on an internal consciousness. We also analyzed Solum's model exploring the roles, uses, and limitations of AI in society and discussed his analogy that AI should serve in roles similar to that of trustees. We then delved into Solum's argument, which explains why AI should not be granted constitutional rights because they are not natural humans, are missing qualities essential to human beings, and should be considered property.

The law must adapt by embracing more granular distinctions between human and tool, and developing doctrines that contemplate the distinction between the moral productivity of electronic agents with human-like capabilities, and the moral receptivity of those with human-like experiences. In the past, legal rights and duties have gone together, but as Solum predicted in 1992, they will not go together forever. There is more work to be done in creating a workable theory of AI personhood, and scholars must continue to hone, adapt, and update it to fit the brave new world of self-learning machines.

[77] Pagallo, *supra* note 72.

BAYESIAN ANALYSIS AS A FRAMEWORK FOR (LEGAL) THINKING

Neil Chilson*

CITE AS: 1 GEO. L. TECH. REV. 89 (2016)
http://bit.ly/2fYZ4IX

INTRODUCTION

Every day, lawyers, regulators, and policy advocates must use information about a situation to evaluate, predict, and draw conclusions about the world around them. The problem is ubiquitous: You have a hypothesis that attempts to explain something in the real world – perhaps the cause of a disease, the guilt of an accused criminal, or the effect of a policy or legislative decision. You also possess some data about the issue at hand. Does this data support or undermine the hypothesis? This is the process of inference. Each of us makes thousands of inferences each day. For example, even without hearing the morning weather report, we might reasonably choose to wear a sweater in February but select a t-shirt in August. We infer the weather conditions based on our hypothesis about the local weather. For such low-stakes decisions, we do not usually formally test our hypotheses. However, when the stakes are high, or when there are many data points that don't clearly point in one direction, we can often improve our inferences by applying the statistical tools of Bayesian analysis.

Bayesian analysis is one of two toolsets statisticians developed to test hypotheses. Most readers will have encountered the frequentist approach to

* Attorney Advisor to Commissioner Maureen K. Ohlhausen at the Federal Trade Commission; J.D., The George Washington University Law School, 2007; M.S. in Computer Science, The University of Illinois, Urbana-Champaign, 2005; B.S. in Computer Science, Harding University, 1999. The views expressed here are those of the author and should not be attributed to Commissioner Ohlhausen or to the Federal Trade Commission.

hypothesis testing, although they may not know it by that name. However, non-experts may not know about the increasingly popular second toolset: Bayesian analysis.[1] Although Bayesian analysis was anathema to professional statisticians for more than a century, today its applications are ubiquitous.[2] This is because Bayesian analysis offers a practical way to transform large volumes of data into actionable recommendations. Machine learning, neural networks, and pattern recognition algorithms are built on Bayesian principles.[3] These and other Bayesian tools form the computational underpinnings of common applications such as spam filters, movie recommendation engines, cancer diagnosis, language translation, codebreaking, and self-driving automobiles.

Understanding the basic principles of Bayesian analysis will help the modern lawyer grapple with such pervasive technologies. Bayesian analysis also could enhance legal and policy decisions and improve critical thinking skills generally.

THE BAYESIAN FRAMEWORK

At the core of Bayesian analysis is Bayes' Theorem, named after Reverend Thomas Bayes, who first discovered it in the 18th century. Bayes' Theorem formalizes a rather common-sense procedure: when we gather new data about a situation, we use it to update our existing belief, creating an improved belief about that situation. But while this sounds like common sense, Bayesian analysis can be at its most useful when it produces counterintuitive results.

We can unpack three important characteristics of Bayesian analysis through an example. Imagine that while you are reading this article in your home or office, the fire alarm suddenly starts sounding. Given this new

---

[1] The roots of today's frequentist and Bayesian statistical tools date to the mid-1700s. (Reverend Thomas Bayes, namesake of the Bayesian approach, discovered the core rule in the 1740s.) Due to fundamental philosophical differences between the two approaches, statisticians have generally considered themselves either frequentists or Bayesian, with frequentists overwhelmingly dominating the field until recent decades. This article will barely touch on the philosophical differences between the camps and will not at all address its fascinating history. Excellent accounts are available, including Sharon Bertsch McGrayne's *The Theory that Would Not Die: How Bayes' Rule Cracked the Enigma Code, Hunted Down Russian Submarines & Emerged Triumphant from Two Centuries of Controversy*.

[2] *See, e.g.*, F.D. Flam, *The Odds, Continually Updated*, N.Y. TIMES (Sept. 29, 2014), http://www.nytimes.com/2014/09/30/science/the-odds-continually-updated.html.

[3] *See generally* SHARON BERTSCH MCGRAYNE, THE THEORY THAT WOULDN'T DIE 233–52 (2011).

information about the state of the world, estimate the probability (90%? 50%? 2%?) that there is a dangerous fire in your building.

How did you choose that percentage? You probably came to it quite intuitively, but let's examine the specific categories of information that may have informed that intuition. First, you have an existing belief, a *prior probability*, about the state of the world: absent an alarm, you know that dangerous fires are rather unlikely as a general matter. Second, you know that there are multiple situations other than a fire that might trigger a fire alarm, and that some of these triggers are more probable than others. There might be a dangerous fire, in which case the alarm is a *true positive*: it indicates there is a fire, and indeed there is. But perhaps building administrators are testing the alarm. Perhaps someone burned bacon. Perhaps someone pulled the fire alarm as a prank. For each of these causes the alarm is a *false positive*: it is indicating the existence of a fire, but there is no fire. You consider the likelihood of these true and false positives in light of your prior belief about the state of the world, and come to a new belief, a *posterior probability*, about the state of the world. Having derived this inference about the world, you probably aren't done: you will continue to gather additional information—Is there smoke? Is there an announcement? Do you hear fire engines?— and use this new information to update your belief about the state of the world around you.

This example demonstrates the three key characteristics of Bayesian analysis. First, when applying Bayesian analysis to new evidence, our prior beliefs – how likely are building fires? – are an input. They affect how new information changes our conclusion. Second, Bayesian analysis weighs the likelihood of each potential explanation for the new evidence, some of which conflict with and some of which support our prior beliefs. Third, and finally, Bayesian analysis is iterative, meaning we continually update our conclusions by taking our previous analysis's output and using it as input for the next round of analysis.

Each of these three characteristics is reflected in Bayes' Theorem:

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

where $P(A|B)$ means the probability of A given B.[4]

Let's walk through our fire alarm example to concretize the abstract symbols. We are estimating the probability that there is a dangerous fire given

[4] This a simplified version of the equation. The more explicit version expands the denominator, P(B), into the mathematically equivalent $P(B|A) \cdot P(A) + P(B|{\sim}A) \cdot P({\sim}A)$.

that we hear a fire alarm. Thus, referring to the left side of the formula above, we are estimating *P(A|B)*, or the probability of *A* (a fire) given *B* (a sounding fire alarm). The right side of the equation shows how to find *P(A|B)*. It has three parts. First is *P(A)*, the *prior probability* that stands for how probable are building fires as a general matter. As mentioned before, the probability is likely quite low. Erring on the side of caution, let us assume that 1% of buildings are on fire at any one time. Second is *P(B)*, which in our example is the probability of a fire alarm going off. This includes the probability of the fire alarm going off because there is a fire (a *true positive*) plus the probability of the alarm going off for any other reason (*false positives*). Based on experience, I would guess that most fire alarms are false positives, so we would expect this probability to be quite a bit larger than the 1% percent of buildings on fire. Even so, fire alarms aren't that common. Let's say that 5% of buildings have an active fire alarm at any time. The third component is *P(B|A)*, which in our example is the probability of an alarm going off assuming there is a fire in the building. One hopes that this is quite high: while fire alarms may go off for many other reasons, when a fire is burning we want an alarm that is certain to go off. Let's guess that fire alarms activate to 99% of building fires.

Inputting these values into the equation, we get a (.99 * .01)/.05 = .198 = 19.8% probability, or approximately a one in five chance that the building is burning given that a fire alarm is sounding. Your estimate may be higher or lower depending on your estimates for each value. However, if, like me, you estimated a relatively low likelihood of a fire given the alarm, that is probably because your experiences with fire alarms (like mine) suggest that false positives are quite common – fire alarms go off for many reasons other than actual fires.

In this example, Bayes appears to have simply confirmed the common-sense conclusion that fire alarms often don't mean the building is burning. So why is Bayesian analysis useful if it is essentially common sense? First, this fire alarm example is very straightforward, with only a single piece of new data (the fire alarm is sounding). Bayesian analysis can be used for much more complex problems involving many new data points with thousand or millions of possible values where there is no obvious intuitive answer. Our intuitions prove less useful with such complex data sets.

Second, while we all have experience with false positives in fire alarms, our intuitions can lead us astray in areas where we have less experience with false positives. Bayesian analysis can help overcome such incorrect intuitions. One of the best examples comes from a controversial 2009 U.S. Preventative

Services Task Force recommendation.[5] The Task Force recommended *against* routine biennial mammograms for women between 40 and 50 with no other risk factors. It recommended this even though mammograms are relatively accurate: such tests properly identify approximately 75% of women with breast cancer, although they return false positives (misidentify cancer in women who are cancer-free) about 10% of the time. Despite the apparent accuracy of the tests, the task force found that a woman under 50 without additional risk factors who had a positive mammogram test result was highly *unlikely* to have breast cancer.[6]

This counterintuitive result can be made more intuitive by focusing on the false positive component of the Bayesian formula. Like burning buildings in our fire alarm example, women under 50 with breast cancer are very rare – approximately 40 out of 10,000 – meaning 9,960 out of 10,000 women don't have breast cancer. But if we tested all 10,000 women, a 10% false positive rate would produce approximately 996 false positives – dwarfing the number of women with cancer. Like our fire alarm example, when testing an extremely rare condition, even relatively accurate tests produce many false positives.

The Task Force's report explained that these false positives were a major cost of unnecessary screening, imposing "psychological harms, additional medical visits, imaging, and biopsies in women without cancer, inconvenience due to false-positive screening results, harms of unnecessary treatment, and radiation exposure."[7] The counterintuitive recommendation against such routine testing was controversial, but would not have been if more people understood Bayes' Theorem and how our intuitions can fail to account for false positives.

CRITICISMS OF THE BAYESIAN APPROACH

Bayesian analysis has faced strong criticism for centuries. Indeed, the approach was practically taboo among professional statisticians for much of its history, even though non-statistician practitioners periodically used it to solve

---

[5] *Final Update Summary: Breast Cancer: Screening*, U.S. PREVENTATIVE SERVS. TASK FORCE (Jan. 2016), https://www.uspreventiveservicestaskforce.org/Page/Document/UpdateSummaryFinal/breast-cancer-screening.

[6] This example draws on the characterization of this research in McGrayne, *supra* note 3, at 259.

[7] *Screening for Breast Cancer Using Film Mammography: Clinical Summary of 2009 U.S. Preventive Services Task Force Recommendation*, U.S. PREVENTATIVE SERVS. TASK FORCE (2009), https://www.uspreventiveservicestaskforce.org/Home/GetFileByID/248.

real-world problems.[8] Statisticians in the long-dominant frequentist school of probability and hypothesis testing acknowledge the mathematical correctness of Bayes' Theorem. However, they raised several concerns about the usefulness of Bayesian analysis. Much of this opposition was a practical matter. The above examples are relatively simple applications of Bayes' Theorem, but for more complex problems involving multiple new data points with many possible values, Bayesian analysis requires substantial computing power not available until the modern computer age. Traditional frequentist tools were simply more practical prior to computers.

More fundamentally, frequentists were highly skeptical of Bayesian reliance on prior probabilities, which they argued are overly subjective and thus fail to produce objective, scientific results. Bayesians counter that all analysis relies on prior knowledge and experience, and the Bayesian approach exposes such reliance rather than conceal it.

APPLYING BAYESIAN ANALYSIS

Engineers have enthusiastically applied Bayesian analysis to build new and useful tools, some of which we have already mentioned. But as computation has become a useful problem-solving tool across all areas of human inquiry, Bayesian analysis has broadening implications for law and policy. The Bayesian approach promises important legal and policy applications and adopting a Bayesian mindset can strengthen critical thinking skills generally.

Criminal or Civil Trials. Bayesian analysis has significant potential – largely unrealized – to assist courts in determining civil or criminal liability.[9] Some have argued that it can be helpful in assessing the overall significance of an accumulation of small pieces of evidence.[10] Others have suggested a Bayesian approach to assessing expert testimony.[11] In the 1970s, academics

[8] Historical applications include breaking the Nazi's Enigma code and identifying the causes of lung cancer and heart disease. *See, e.g.*, McGrayne, *supra* note 3.

[9] Michael O. Finkelstein & William B. Fairley, *A Bayesian Approach to Identification Evidence*, 83 HARV. L. REV. 489 (1970); *see also*, Kristy L. Fields, *Toward A Bayesian Analysis of Recanted Eyewitness Identification Testimony*, 88 N.Y.U. L. REV. 1769 (2013) (arguing that "Bayesian analysis can, and should, be used to evaluate [uncertain eyewitness testimony]," as "use of an objective method of analysis can ameliorate cognitive biases and implicit mistrust of recantation evidence.").

[10] *Id.*; *see also*, Jason R. Bent, *Hidden Priors: Toward A Unifying Theory of Systemic Disparate Treatment Law*, 91 DENV. U. L. REV. 807 (2014) (enumerating a "coherent theory of systemic disparate treatment that embraces Bayesian priors.").

[11] Bruce Abramson, *Blue Smoke or Science? The Challenge of Assessing Expertise Offered as Advocacy*, 22 WHITTIER L. REV. 723 (2001).

heatedly debated the use of Bayesian methods in courtrooms.[12] Thanks to the information revolution, the practical applications of Bayesian techniques are far more powerful than in the 1970s,[13] so it may be time to revive that debate.

Courts present hurdles to the use of Bayesian analysis. Statistics of all kinds have often failed to persuade juries, in part due to the lack of statistical understanding by judges, jurors, and even by lawyers attempting to use them.[14] However, as Bayesian-based technologies such as machine learning become more widely applied, including in the context of law enforcement, [15] we will surely see court challenges that involve the technology.

Policy Analysis. Bayesian analysis can help inform policy decisions, as demonstrated by the earlier discussion of breast cancer screening recommendations. Bayesian analysis is particularly useful in performing meta-analysis of many different studies to identify trends in research. It can also be helpful in estimating the probability of one-time events (such as an accidental nuclear detonation or catastrophic climate change), analyzing phenomena where data is sparse, or interpreting experiments that are not easily reproduced.[16] In these areas, the more traditional statistical tools of frequentism falter. Indeed, frequentists have argued that it makes no sense to talk about the "probability" of an event that has never occurred because we lack any information about the long-term frequency of such an event.[17] Yet many important policy decisions involve analyzing a wide array of different but related research, or evaluating unique circumstances with little hard data.

---

[12] *See, e.g.*, MICHAEL O. FINKELSTEIN & BRUCE LEVIN, STATISTICS FOR LAWYERS 84–5 (3rd ed. 2015).

[13] *See generally*, Maggie Wittlin, *Hindsight Evidence*, 116 COLUM. L. REV. 1323 (2016) (discussing the applicability of Bayesian reasoning to decision-making by the members of a jury); Ian Ayres & Barry Nalebuff, *The Rule of Probabilities: A Practical Approach for Applying Bayes' Rule to the Analysis of DNA Evidence*, 67 STAN. L. REV. 1447 (2015) (discussing the benefit of applying Bayes' Rule to the use of probabilistic DNA matching).

[14] *See generally* Fenton et al., *Bayes and the Law*, 3 ANN. REV. OF STAT. AND ITS APPLICATION 51–77 (June 2016).

[15] See Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015).

[16] *See, e.g.*, Fred Charles Iklé, Gerald J. Aronson, & Albert Madansky, *On the Risk of Accidental or Unauthorized Nuclear Detonation*, THE RAND CORP. WORKING PAPER (Oct. 15, 1958), http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM2251.pdf. This paper is discussed at length at McGrayne, *supra* note 3, at 119 *et seq.*

[17] McGrayne *supra* note 3, at 119-121.

Bayesian analysis cannot provide simple answers for such complex problems, but it can provide a framework for thinking through the issues involved.[18]

Case Selection. Regulators and law enforcement agencies could benefit from using Bayesian analysis as a case-selection tool, at least in certain circumstances. For example, the Federal Trade Commission evaluates thousands of potentially false or deceptive advertisements each year – more than it has the resources to pursue. Bayesian analysis could help make case selection more intellectually rigorous. Advertising claims fall on a continuum from fraudulent to truthful and informative. Similarly, companies base their advertising claims on evidence that ranges from non-existent, to mixed, to conclusive – either in support of or against the claim. A Bayesian approach to case selection would take into account that certain types of common claims – rapid weight loss, for example – are nearly always misleading, at best. Thus, there would be a strong prior probability of a violation that could only be outweighed by powerful evidence substantiating the claim. Other claims, such as mild weight loss benefits, often have mixed evidence, and therefore the prior probability of a violation would be weaker. Bayesian analysis could help most in areas where the company offers several partially flawed studies that generally support their claims. These are the areas where traditional informal case selection methods might be most improved.[19]

In the private sector, firm lawyers and in-house counsel could use a similar approach to evaluate the risk of legal liability under uncertain conditions. Such assessments could both inform compliance advice to clients and shape litigation and settlement strategies.

Critical Thinking. Even forgoing the formal mathematics of Bayes' Theorem, the legal career of any lawyer could benefit from embracing a Bayesian mindset when considering evidence, and making decisions. There are three lessons from Bayes' that can benefit anyone who needs to evaluate evidence and make decisions. **First**, carefully evaluate the impact of prior

---

[18] *See, e.g.*, Jason R. Bent, *P-Values, Priors, and Procedure in Antidiscrimination Law*, 63 BUFF. L. REV. 85, 89 (2015) (arguing that the "time [has] finally come for a Bayesian revolution in employment discrimination law.").

[19] *See, e.g.*, Stephen Charest, *Bayesian Approaches to the Precautionary Principle*, 12 DUKE ENVTL. L. & POL'Y F. 265, 270 (2002) (arguing that "that a Bayesian approach is not only the appropriate method to assess truly uncertain risks," but also "is uniquely suited to promoting intellectual due process principles" in regulatory decision-making); Geoffrey Christopher Rapp, *Intelligence Design: An Analysis of the SEC's New Office of Market Intelligence and Its Goal of Using Big Data to Improve Securities Enforcement*, 82 U. CIN. L. REV. 415, 422 (2013) (discussing the use of Bayesian techniques in intelligence and securities enforcement).

beliefs when reviewing evidence. Bayes' Theorem requires that we make explicit what is often implicit: we interpret evidence in light of our own prior beliefs. This "bias" may be appropriate, as our prior experiences can be very informative. However, becoming more aware of our own inherent bias can help us recognize when that bias may be inappropriate or even misleading.

Second, thoroughly consider other explanations for evidence. Bayesian analysis requires researchers to evaluate the likelihood that the evidence might be explained by something other than their preferred hypothesis. It requires understanding other potential explanations, such as false positives. Simply stepping back to consider other potential explanations of the same data can prevent myopic decision-making.

Third, and finally, think of decision-making as an iterative process that is never finished. At its core, Bayesian analysis relies on repeatedly integrating new evidence with what one already knows. New evidence can always help refine a prediction, and no prediction is ever perfected. Bayesian analysis suggests that we can absorb new evidence in rigorous and principled ways while recognizing that 100% certainty is rarely, if ever, warranted. Instead, policymaking and law are part of life's constant journey toward a better, but never perfect, understanding of the world. Bayesian analysis can help guide us on that journey.

NATURAL LANGUAGE PROCESSING

Peng Lai "Perry" Li*

CITE AS: 1 GEO. L. TECH. REV. 98 (2016)
http://bit.ly/2gqiUxt

INTRODUCTION

Natural Language Processing ("NLP") is a field of computer science, artificial intelligence, and computational linguistics. Computers operate on the foundation of if/then logic statements, whereas natural human language systems do not; NLP endeavors to bridge this divide by enabling a computer to analyze what a user *said* (input speech recognition) and process what the user *meant*. Because NLP is concerned with the interactions between computer and human (natural) languages, it has important applications in the advancement of artificial intelligence and machine learning, from digital assistant applications, such as Siri and Google Now, to machine translation and sentiment analysis. At the same time, the advancement of NLP requires gathering copious amounts of data from users, thereby raising important legal issues in data ownership, privacy, and security. This article briefly explains the process of NLP and highlights some important legal implications of the technology.

BRIEF HISTORY

NLP research began in the 1950s as the intersection of artificial intelligence and linguistics.[1] In what is known as "the Georgetown-IBM

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Iowa State University, M.Sc. 2006, B.S. 2004.

[1] Prakash M. Nadkarni, *Natural Language Processing: An Introduction*, J AM MED INFORMATICS ASS'N 2011.

Experiment" of 1954, more than sixty Russian sentences were automatically translated into English by computers (with varying degree of success).[2] Nevertheless, progress in this field was slow for the following decades for two reasons. First, at the time Noam Chomsky, whose theory posits that all natural languages comprise hierarchies of grammars and adhere to a universal set of rules, greatly influenced linguistics; as a result, most NLP systems resembled complex decision trees based on numerous human-devised rules, despite natural language being much more nuanced in reality (*e.g.*, puns, metaphors, and homographs - identically spelled words with multiple meanings).[3] Second, computers of this era had limited processing power and could not undertake the less rule-based approach which was ultimately far more successful.

Beginning in the 1980s, however, advances in both linguistic theory and computational processing power led to NLP based on statistics and probability. This approach replaces deep structural analysis with simple approximation based on probability; more importantly, this method lets the computer learn the natural language on its own (so-called machine learning) by providing the computer with a large body of text (the corpus).[4] As a result, a few simple rules replaced the complex decision tree, and statistical analysis increase the accuracy of NLP. Statistical NLP is now the predominant NLP technology.

TECHNOLOGICAL PROBLEMS IN NLP

A NLP system needs to process the natural language in the following abstractions levels:[5]

- The phonetic or phonological level (*i.e.*, pronunciation);
- The morphological level, which deals with the smallest parts of words that carry meaning, and suffixes and prefixes;
- The lexical level, which deals with lexical meaning of words and parts of speech analyses;
- The syntactic level, which deals with grammar and structure of sentences;

[2] John Hutchins, *The first public demonstration of machine translation: the Georgetown-IBM system, 7th January 1954* (2006), http://www.hutchinsweb.me.uk/GU-IBM-2005.pdf.
[3] *See generally* Elizabeth D. Liddy, *Natural Language Processing, in* ENCYCLOPEDIA OF LIBRARY AND INFORMATION SCIENCE 2126 (2d ed. NY. Marcel Decker, Inc. 2001).
[4] *Id.*
[5] *Id.*

- The semantic level, which deals with the meaning of words and sentences;
- The discourse level, which deals with the structure of different kinds of text using document structures;
- And the pragmatic level, which deals with the knowledge that comes from the outside world, *i.e.,* from outside the content of the document.

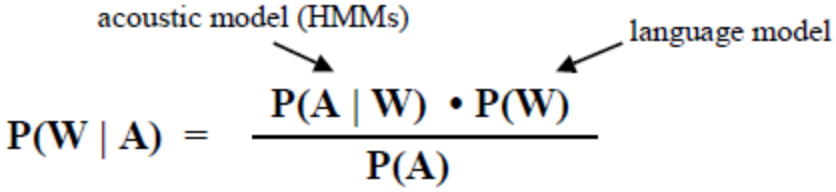
Although detailed discussions for each step deserves its own Technology Explainer and is thus outside the scope of this piece, a common theme among them is that large language corpora and various statistical methods can improve the accuracy of recognition, parsing, and understanding at *each* of the aforementioned steps. This article details how two common statistical methods are used in the phonetic level of NLP (*i.e.,* input speech recognition).

Input Speech Recognition – Can You Hear Me Now?

The goal of input speech recognition is to capture and accurately transform a user's spoken utterance into text. The user's utterance consists of a series of phonetic sounds; for example, the spoken word sequence "cat nip" consists of six phonetic units (phones): "/k/," "/æ/," "/t/," "/n/,""/ɪ/," and "/p/." In terms of probability, the goal of input speech recognition becomes the following: Given the received phonetic sequence (let's call the sequence "A"), find the sequence of words ("W") such that the conditional probability of the word sequence W given the received phonetic sequence A (*i.e.,* conditional probability P(W|A)) is maximized.[6]

The probability maximization problem can be transformed into maximization of the product of two separate probability components, both having real-world significance, based on the statistical theorem known as Bayes Rule.[7] The Bayesian transformation accounts for how likely it is that the processor will accurately observe the phonetic sequence (the acoustic model), and how likely it is for a given word to occur (the language model).

[6] 1 Mark Gales and Steve Young, *The Application of Hidden Markov Models in Speech Recognition, in* FOUNDATIONS AND TRENDS IN SIGNAL PROCESSING NO. 3, 195-304, 204 (2008).
[7] *See id*. at 201.



Acoustic Model – Bridging Sound and Words

The first probability component in the numerator of the Bayes transformation is P (A|W); that is, given that the word sequence ***is*** "cat nip," what the probability of receiving an observed phonetic sequence is. This is called the Acoustic Model.[8] The following table provides examples of what, given that the word sequence is "cat nip," the respective probabilities of overserved phonetic sequences are:[9]

Phonetic Sequence	Likelihood (qualitative)	Probability (as example)
"/k/," "/æ/," "/t/," "/n/,""/I/," "/p/."	Complete certainty	100%
"/k/," "/æ/," "/t/," "/n/,""/I/," **"/t/."**	Very likely, except for an error while capturing the last phone	90%
"/d/," "/o/," "/n/," "/k/,""/I/," "/I/."	Very unlikely (the phonetic sequence is more likely for the word "Donkey")	2%

Because speeches (phonetic sequences) are time-sequential, a statistical model known as the Hidden Markov Model is particularly well-suited for modeling speech.[10] Acoustic models in most state-of-the-art NLP systems today are variations of Hidden Markov Models. In practice, a voice recognition system can learn a user's voice by analyzing the particularities in her voice, such as inflections and the pronunciation of certain consonants, when she speaks a predetermined training phrase.

[8] *Id.*
[9] The numeric probability values in the table below are merely for illustration purposes.
[10] Liddy, *supra* note 3.

Language Model – God Save the Gerbil

The second probability component in the numerator of the Bayes transformation is P(W) (*i.e.*, how likely the word sequence W occurs). This is called the Language Model. In natural speech of a given language, certain word sequences appear much more frequently than other sequences. For example, in the English language, the phrase "God save the king" occurs much more frequently than the phrase "God save the gerbil." Therefore, different probabilities of occurrence can be assigned to the two word sequences, where the first probability greatly exceeds the second. When the voice recognition system detects that the first three words in a user's speech is "God save the," it can consider the respective frequencies of occurrence of the two example word sequences above in determining what the user said. Such word group in a language system is called **n-gram** (*i.e.*, the phrase "God save the King" has four words and is therefore a 4-gram).[11] Armed with a large corpus of text in a certain language and a super computer, a comprehensive statistical analysis can be performed on any n-gram (although in practice n is usually limited to five or less); that is what Google did for several languages based on corpora of texts between the year 1500 A.D. and 2008 A.D. The results and their subsequent publication have significantly advanced computational linguistic research.[12]

Context-Based Language Model – Know Thyself

More refinements to the language model can further improve the language model. For example, in the United States, the phrase "God save the King" is much less common than the phrase "God save the country." If a user is determined to be an American English speaker (such determination can be readily made today by, *e.g.*, using the user's GPS location on her smartphone, detecting her American accent, verifying her U.S. phone number or time zone information), predicating the 4-gram frequency of occurrence on a corpus of American English instead of English spoken everywhere can thus improve the accuracy of prediction.

This type of refinement, called contextual language modeling, can be extended to a variety of contexts: for example, in smartphone digital assistant

[11] DAN JURAFSKY AND JAMES H. MARTIN, SPEECH AND LANGUAGE PROCESSING: AN INTRODUCTION TO NATURAL LANGUAGE PROCESSING, COMPUTATIONAL LINGUISTICS, AND SPEECH RECOGNITION 85 (2d ed. 2008).

[12] Alex Franz and Thorsten Brants, *All Our N-grams Belong to You*, GOOGLE RESEARCH BLOG (Aug. 3, 2006), http://googleresearch.blogspot.com/2006/08/all-our-n-gram-are-belong-to-you.html.

applications, contextual language models can be based on the app being used, the recipient(s) of certain communication (if a communication/social-network app is being used), the user's GPS location and direction of travel, web browser history, calendar entries, and biometric information (such as temperature or heart rate), and much more.[13]

In the age of cloud computing, it is even possible to use contextual information from groups of users to create a community-based context.[14] For example, if a large number of users that either have a MIT email address or are near the MIT campus speak or write texts linking the term "the Sponge" with the proper name Simmons Hall (a building resembling a sponge), the NLP system can automatically create a community-based contextual language model for everyone who fits a "MIT student or affiliate" criteria and make "Simmons Hall" and "the Sponge" synonymous in the community language model. Ultimately, improving the accuracy becomes a process of narrowly defining both the speaker (what *I*, the user, have previously said or written) and the context of the speech (*i.e.*, whether I am sending an email to my boss in my office or texting my spouse on a commuter train heading home), much like how humans improve accuracy of understanding using context.

Legal Implications

The continued advancement of NLP has important legal implications on data privacy and security. As discussed, NLP thrives on voluminous data in the forms of text corpora and contextual information; the more a NLP system knows about a user's individual's manner of speech, frequently used words, habits, social connections, physiological state, and other information, the better it can process the user's natural language utterances. NLP applications, such as digital assistants (*e.g.*, Siri, Google Now, and Amazon Alexa) have greatly improved capability and accuracy as a result of having a vast amount of corpus and contextual data as training material. However, the user is providing important personal data by using these NLP applications, and the current technology trend is moving toward unconscious sharing of data, frequently without user consent.[15] For example, NLP systems such as Amazon's Alexa can be "always on" in the background to constantly monitor and process the user's

[13] *See, e.g.*, Training an at least partial voice command system, U.S. Patent Application No. 20140278413 at [41–2] (filed Mar. 15, 2013).
[14] *Id.* at 113–4.
[15] *See generally* Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, FUTURE OF PRIVACY F. (Apr. 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

speech as she goes about her daily routine, regardless of whether she is aware of such constant monitoring.[16] Furthermore, current NLP systems transmit collected data to remote servers, which alone has the enormous computation power required to achieve the near-instantaneous processing. Such data transfer raises not only information privacy but also security issues, as the data is prone to hacking.

Finally, community-based contextual language models also pose novel legal issues. For example, if a prominent Silicon Valley technology company has gathered enough corpus and contextual data to create an Arabic language model specific to Queens, New York, can law enforcement request (or even compel) access to the language model in order to use it for law enforcement purpose? The complicated issue is that the language model predicates on, yet is distinct from, the corpus and contextual data collected from the user; therefore, who owns the model and who can access it are destined to be contentious legal issues.

CONCLUSION

A profoundly important bridge between human and computer languages, NLP technology will continue to advance at dizzying speed, propelling the progress of artificial intelligence and machine learning along the way. At the same time, the advancement of NLP requires gathering copious amounts of data from users, thereby raising important legal issues in data ownership, privacy, and security. Such novel legal issues will likely come into focus as NLP technology becomes more advanced and mainstream.

[16] Kim Komando, *3 Gadgets That Are Always Listening and How to Stop Them*, USA TODAY (Oct. 6 2015), http://www.usatoday.com/story/tech/columnist/komando/2015/10/02/3-gadgets-always-listening-and-how-stop-them/73191644/.

PUBLIC KEY ENCRYPTION

Weisiyu Jiang*

CITE AS: 1 GEO. L. TECH. REV. 105 (2016)
http://bit.ly/2fG6xMf

In early April, WhatsApp, an online messaging service with more than a billion users, announced that they added "end-to-end" encryption to every form of communication on the service. This means WhatsApp's server now acts as an illiterate messenger, passing along messages that it cannot itself decipher.[1] Because of this newly adopted technology, WhatsApp is unable to disclose the texts of its customers' messages to any third parties, including authorities like the Federal Bureau of Investigation ("FBI"). WhatsApp's encryption technology works by using public key encryption.

Public key encryption is founded on basic encryption. To encrypt something means to use an algorithm, a series of well-defined steps that can be followed as a procedure, to convert information a sender wishes to transmit to a receiver (referred to as plaintext), into unreadable, meaningless cipher text (the encrypted result of the original plaintext).[2] To comprehend the message, the recipient then needs a key to decrypt the unreadable cipher text, transforming the garbled data into its original form.[3] Just like the key to the lock of your house limits access to your home, a key to an algorithm determines who can have access to the encrypted message. Therefore, a key is a crucial piece of information, a parameter, that determines the functional output of the algorithm. Without it, the cipher text cannot be decrypted, and the data is meaningless.

WhatsApp's end-to-end encryption provides added protection by adopting a system of communication in which only the communicating users can read the messages. In principle, it prevents potential eavesdroppers—including WhatsApp itself—from being able to access the keys needed to decrypt the conversation.[4] This varies significantly from the encryption used by Facebook's messaging app, Facebook Messenger. Facebook Messenger

---

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Mount Holyoke College, B.A. 2013.

[1] Cade Metz, *Forget Apple v. the FBI, WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016, 11:00AM), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/#slide-1.

[2] Vangie Beal, *Public Key Encryption*, Webopedia, (date), http://www.webopedia.com/TERM/P/public_key_cryptography.html.

[3] *Id.*

[4] Andy Greenberg, *Hacker Lexicon: What is End to End Encryption?*, WIRED (Nov. 25, 2014, 9:00AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

encrypts your messages through part of their journey. A user types a message using the app, and hits send. The message is encrypted, so an outside user attempting to intercept the message during transmission. Facebook receives the message, decrypts it, and stores it on their server. It is then re-encrypted and sent to your recipient, where it is decrypted again. Even with this partial-path encryption, your messages are stored in plaintext on Facebook's server, and the company has the keys to the encryption used.[5] The company can access your messages, and, if they are compelled to provide them to the government or if the company is hacked, others can access that information as well.[6] In WhatsApp's end-to-end encryption, the key to the encryption is known only by the sender and the recipient, and the message is not decrypted when it is stored on WhatsApp's server. It is fully encrypted and inaccessible to WhatsApp or any other user who might gain access to that server.[7] This is arguably the most secure method of securing user communications and is all due to public-key encryption.[8]

Public key encryption is also known asymmetric encryption, as it uses two different but mathematically related keys instead of only one ("symmetric encryption").[9] To better understand the concept of public key encryption, let us first compare it with symmetric encryption. Imagine Tom has a box with an ordinary lock, a lock with only one key. Only Tom or someone else with a copy of his key can open the box. That's symmetric encryption: you have one key, and you use it to encrypt ("lock") and decrypt ("unlock") your data.[10] Now, let us see how asymmetric or "public-key" encryption works. Suppose Tom has a box with a special lock that has two separate keys. The first one can only turn the lock clockwise (0-5-10) and the second one can only turn it counter-clockwise (10-5-0).[11] Tom keeps the first key to himself, so this is his "private key." Then, he makes many copies of the second key and gives them to whoever wants to send him documents, such as his family, friends, colleagues, etc. Because it is shared with the public, this second key is his "public key." Now, if a confidante wants to send him a very personal document, she would put the document in the box and use a copy of the public key Tom gave her to lock it.

---

[5] Dan Albright, *Why What's App's End to End Encryption is a Big Deal*, MUO (Apr. 27, 2016), http://www.makeuseof.com/tag/whatsapp-turning-end-end-encryption/.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] Beal, *supra* note 2.
[10] Panayotis Vryonis, *Explaining Public-Key Cryptography to Non-Geeks*, Vrypan (Aug. 28, 2013), https://blog.vrypan.net/2013/08/28/public-key-cryptography-for-non-geeks/.
[11] *Id.*

The public key only turns anticlockwise, so she turns it from 10 to 5 to 0. Now, the box is locked. The only key that can turn from 0 to 5 to 10 to unlock it is Tom's private key, which he has kept for himself.[12] That box is comparable to public key encryption scheme: Everyone who has the recipient's public key can put documents in the recipient's box, lock it, and know that the only person who can unlock it is the recipient, the only person who has the one private key.[13] Another way to think of the public key encryption system is to think it as the blue USPS mailing box sitting outside a post office. There is a door that anyone can open to insert mail, but the door only works in one direction Once the mail is in the mailbox, that door cannot be used by anyone else to get any mail back out. Instead, there is a second door secured by a key that only the postman has, which he uses to get all the mail back out. This is roughly analogous to an asymmetric-key system. The public key is freely available and allows anyone to send a message to the recipient in a secure manner. Nobody else, including other individuals using the mail system to send their own messages, can see what was sent. Only the recipient, with the private key, can get those messages back out and read them.[14]

In a public key encryption scheme, the public key is required to encrypt the message, but, it does not need to be kept as a secret. Although the private key still needs to be stored securely, the advantage is that the encryption can occur without the private key. This means the private key never needs to be transferred and thus there is no chance that it can be intercepted by a third party. Thus, public-key encryption is convenient in that it does not require the sender and receiver to share a common secret to communicate securely.

Other than securely delivering messages, public key encryption is also widely used for "digital signatures."[15] Suppose Tom puts a document in his special box. He uses his private key to lock the box, turning the key clockwise from 0 to 5 to 10. Someone delivers this box to his best friend, Sarah, and tells her the box is from Tom. She tries Tom's public key on it, and the box opens. This can only mean one thing: the box was locked using Tom's private key, the one that only Tom has. So now she can believe the messenger and know that no one else but Tom put the document in the box. In other words, Tom "digitally

---

[12] *Id*.
[13] *Id*.
[14] *Public Key and Private Keys*, COMODO, https://www.comodo.com/resources/small-business/digital-certificates2.php (last visited Nov. 21, 2016).
[15] Matt Blumenthal, *Encryption: Strength and Weakness of Public Key Cryptograph*, VILL. (2007), http://www.csc.villanova.edu/~mdamian/Past/csc3990fa08/csrs2007/01-pp1-7-MattBlumenthal.pdf.

signed" the document.[16] Therefore, public key encryption system generally serves two functions: (1) If anyone encrypts ("locks") something with the recipient's public key, only the recipient can decrypt it ("unlock") with his secret private key; and (2) if the sender encrypts ("locks") something with his private key, anyone can decrypt it ("unlock"), but this serves as a proof that the sender encrypted it - it's "digitally signed" by the sender.[17]

Although public key and private key are related, the way the key pair are generated makes it virtually impossible to deduce the private key from the public key. The algorithms that the encryption is based use a mathematical expression built on the multiplication of two large prime numbers (a number that is the product of only 1 and itself). For example, the following numbers are the product of two prime numbers:

Product		Primes
15	=	3 x 5
77	=	7 x 11
221	=	13 x 17

Essentially, the public key is the product of two randomly selected but extremely large prime numbers, and the private key is the two primes themselves. The algorithm encrypts data using the product and decrypts it with the two primes, and vice versa. This algorithm is secure because of the great mathematical difficulty of finding the two prime factors of a large number, and of finding the private key from the public key.[18] This is difficult because the only known method of finding the two prime factors of a large number is to check all the possibilities one by one, which is not practical due to the number of prime numbers. For example, there are about 3,835,341,275,459,350,000,000,000,000,000,000,000 different prime numbers in a 128-bit public key. That means that even with enough computing power to check one trillion of these numbers a second, it would take more than 121,617,874,031,562,000 years to check them all. That is about 10 million times longer than the universe existence of the universe.[19] If a user has the private key it adds enough information to the puzzle so that there is only one solution. It is like having a prize behind millions of doors; if you know which door the prize is behind, you can find the prize in no time. Without this

[16] Vryonis, *supra* note 10.
[17] *Id*.
[18] *How Public Key Encryption Works*, LIVING INTERNET, http://www.livinginternet.com/i/is_crypt_pkc_work.htm (last visited Nov. 21, 2016).
[19] *Id*.

information, the only remaining option is to try every door or choose one at random.[20]

Therefore the two keys are closely related to each other, but it's practically impossible to deduce the private key from the public key alone. In the current digital age, for companies to be confident that their electronic transactions can be carried out securely, effective security will be a consistently evolving challenge. Public key encryption, although might not be perfect, provides a sufficient solution.[21] It helps ascertain the identity of different people, devices, and services. Even if the information could be captured, the public key encryption scheme keeps the data in a meaningless form, unless the hacker has the private key.[22]

[20] *Symmetric Key and Public Key Encryption*, READABLE, http://www.allreadable.com/8413SR8 (last visited Nov. 21, 2016).
[21] *Security and the Basics of Encryption in E-Commerce*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV., https://cyber.harvard.edu/ecommerce/encrypt.html (last visited Nov. 21, 2016).
[22] *Id*.

ONION ROUTING AND TOR

Kyle Swan*

Cite as: 1 GEO. L. TECH. REV. 110 (2016)
http://bit.ly/2gAbY3T

THE ORIGINS OF TOR

Security in online activity, and privacy from those who wish to monitor it, has been a priority for internet users since creation of the web. To achieve this goal, the concept of onion routing was developed by the United States Naval Research Laboratory ("NRL") in the mid-1990s to protect online communications in the U.S. intelligence community.[1] Computer scientists for NRL, working with other government programs on what was then titled The Onion Routing Project, ushered this technology into its next generation, known simply as "Tor."[2] Tor was deployed as open-source software,[3] available to the public for free in 2004,[4] and is now maintained by volunteers and funded by various sources including the U.S. Government, digital rights interest groups, and individual donors.[5]

Tor was created to provide an efficient and secure method for users to protect their identity online. As such, Tor has attracted a large following of users, criminal and legitimate, who could benefit from the cloak of anonymity.

---

* GLTR Staff Member; Georgetown University Law Center, J.D. expected 2018; University of Virginia, B.A. 2014.

[1] Paul Syverson, *Brief Selected History*, ONION ROUTING https://www.onion-router.net/History.html (last visited Nov. 28, 2016).

[2] *Id.*

[3] *Open-source*, MERRIAM-WEBSTER ONLINE DICTIONARY http://www.merriam-webster.com (last visited Oct. 10, 2016) ("pertaining to or denoting software whose source code is available free of charge to the public to use, copy, modify, sublicense, or distribute.").

[4] Syverson, *supra* note 1.

[5] *Tor Sponsors*, THE TOR PROJECT, https://www.torproject.org/about/sponsors.html.en (last visited Nov. 16, 2016).

Journalists, whistleblowers, and political activists can use Tor to circumvent national firewalls and hide their identities, often from authoritarian regimes.[6] The protection offered by Tor also shields illegal activities in a part of the internet dubbed the "Dark Web."[7] Criminals, such as hackers, child pornographers, and black marketers, use Tor to conceal their identities from law enforcement.[8] Tor is not exclusively used for criminal or political activities, however. Individuals concerned with privacy now use Tor simply to browse the internet, with The Tor Project estimating that it has over 1.5 million users.[9]

Tor helps to protect the identities of users through a combination of the structure of the network and a process known as onion routing. The structure of the network prevents an outsider actor from monitoring a user's traffic, or locating a user, while onion routing uses encryption to shield the contents of a user's message. When used in tandem, both aspects prevent websites from tracing data back to a user.

TOR STRUCTURE

Tor, first and foremost, is a network. It is made up of decentralized collective of servers hosted by volunteers all across the globe called "nodes." A node is a connection point in a network with an assigned address; it can be a router, computer terminal, peripheral device, or mobile device.[10] Nodes are the access and transfer points for user data; the bridges for user traffic sent back and forth through the Tor network, connecting users and their destinations. By acting as a middleman between a Tor user and his destination, nodes also protect the user from having his information tracked.

Tor maintains a directory of all nodes on its network, and from its directory, it will designate a path for information through three or more separate nodes. A user's data, after entering the Tor network will pass through an entry

---

[6] *Inception*, THE TOR PROJECT, https://www.torproject.org/about/torusers.html.en (last visited Nov. 16, 2016).

[7] Leslie Caldwell, Assistant Attorney General, U.S. Dep't of Justice, Remarks at "Cybersecurity + Law Enforcement: The Cutting Edge" Symposium (Oct. 16, 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law.

[8] Jake Wallis Simons, *Guns, drugs and freedom: the great dark net debate*, THE TEL. (Sept. 17, 2014, 5:00 PM), http://www.telegraph.co.uk/culture/books/11093317/Guns-drugs-and-freedom-the-great-dark-net-debate.html.

[9] *See generally Tor Metrics*, THE TOR PROJECT, https://metrics.torproject.org/ (last visited Nov. 16, 2016).

[10] *See Node*, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com (last visited Nov. 16, 2016).

node, also known as a guard node, then at least one middle node, and then an exit node, before reaching its destination. Tor will send the user's data on a random path to its destination through these nodes; each time a user visits another site, it selects a different random path of nodes.[11] The randomization at each node makes data increasingly difficult to track as the variability of potential paths expands. Node diversity allows for greater security because an entity attempting to track a user would have to be able to follow it through each possible pathing, an increasingly difficult task as the number of forks in the road grows.

Tor employs the onion routing encryption process to prevent websites and other services from learning a Tor user's location (through the user's IP address) or intercepting the content of the message sent. Data is encrypted upon entrance into the Tor client for each node. Encryption is a practice that protects data by scrambling it into a message decipherable only by someone with the proper key or algorithm to unscramble and access it. Because Tor goes through several nodes and subsequent scrambles, no single relay can reveal a user's location. In this way, the multi-node setup creates greater security than a proxy using a single node. Unlike other server providers, which will guide traffic through one particular node, Tor, by sending information through multiple nodes, effectively makes those tracking information lose sight of its origin.[12] Tor not only misdirects sites seeking to gather information from users visiting them; it goes one step further, shielding not only the path of the user's requests from node to node, but also the payload data those requests contain and the location of the user.[13]

To illustrate through analogy: imagine you, the user, are a spy attempting to arrive at a villain's lair without being tracked to orally deliver a message to another spy. You must keep your identity (IP address) concealed while evading his pursuing henchmen (outside users attempting analyze web traffic), who might persuade you to reveal the message (intercept message contents of the communications sent). You leave your hideout with various layered disguises (encryption), which will prevent the henchmen from knowing your true identity. To reach the lair, you make your way through several chambers around the lair where the henchmen have lookouts (nodes). At the first lookout, henchmen are expecting an unknown spy to pass at a random spot, but you escape unnoticed because you are in your first disguise, a police

[11] *Tor Overview*, THE TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Nov. 16, 2016).
[12] *Tor FAQ*, THE TOR PROJECT, https://www.torproject.org/docs/faq.html.en#Torisdifferent (last visited Nov. 16, 2016).
[13] *Id.*

uniform. At the second lookout, they are looking for the police officer, but they only see a man dressed as a waiter, your second disguise. When the henchmen are looking for a waiter at their third lookout, all they find is an elderly man, your third disguise. They take no notice as you enter the unsuspecting villain's lair to deliver the message to your waiting ally. The same process occurs on the way back to your hideout with new disguises and different lookout points, and when you make your way back without any henchmen on your tail, your identity is safe. The Tor process combines the encryption (disguises) and random node pathing (choices of lookout points) to keep user identity (which for an IP address, translates easily to user location) private.

HOW DOES ONION ROUTING WORK?

The primary goal of onion routing is to prevent traffic analysis and potential back-tracing. Traffic analysis, often referred to as web analytics in certain contexts, is the process of intercepting and examining messages in order to deduce information about a particular communication. It can be as banal as logging a user's online shopping preferences so that a retailer can advertise to his personal taste, or as significant as an attempt by law enforcement to track down a criminal.[14] Traffic analysis can allow entities to follow the chain of data leading back to an individual user in a process aptly called back-tracing.[15] Tor seeks to subvert this process.[16]

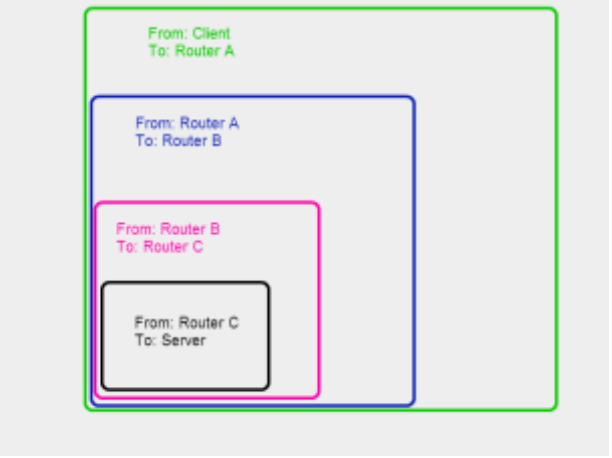
Onion routing protects user data by creating multiple layers of encrypted connections to shield data from potential onlookers.[17] For those of us attempting to understand how onion routing works, an apt metaphor exists in its name. The data sent by a user is the core of the "onion," containing the content of the message. At the onset of the transmittal process by connecting to a Tor client, several layers of encryption surround the core, one atop the other like Russian nesting dolls, so that the core data payload is inaccessible to outside actors.[18] When entering the Tor network, the data is scrambled through encryption; the iterations of the scrambled message are then scrambled again for the number of

---

[14] *See* Chris Hoffman, *The Many Ways Websites Track You Online*, HOW-TO GEEK (June 1, 2012), http://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/; *see also* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End up in Your Computer*, WIRED (Aug. 5, 2014), https://www.wired.com/2014/08/operation_torpedo/.
[15] *See* Yossi Gillad & Amir Herzberg, *Spying in the Dark: TCP and Tor Traffic Analysis*, https://www.freehaven.net/anonbib/cache/tcp-tor-pets12.pdf.
[16] *Id.*
[17] *Overview*, *supra* note 11.
[18] *Id.* ("The client negotiates a separate set of encryption keys for each hop along the circuit").

times it will travel through a node en route to its destination. As the information travels through the Tor network, at each node, a layer of the onion is "peeled" away, exposing the next encrypted message to be decrypted at the next node. No individual node ever knows the complete path of the data packet, so tracking capabilities from a single node are limited.[19] Once the onion is fully peeled and has reached its destination, the core containing the information is the only piece remaining. Once the data is received at the destination server, that information is re-encrypted (imagine the onion re-growing its layers) and "peeled" again on the way back to the user, following the same procedures as before.[20]

The secret to Tor's ability to protect users' identifying information is in the peeling process. The nodes only receive the location of the node sending it information, so the user's location (in the form of an IP address) and the content of the message are never exposed simultaneously. The Tor client encrypts the original data so that only the exit relay can decrypt it. This encrypted data is then encrypted again, so that only the middle relay can decrypt it. Finally, this encrypted data is encrypted once more so that only the entry relay can decrypt it.[21]



http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/

The first node will receive a fully encrypted message with the user's location; the second node will receive a partially encrypted message with only the location of the first node; and the final node will fully decrypt the message

[19] *Id.*
[20] *Id.*
[21] *See* Will Nicol, *A Beginner's Guide to Tor: How to Navigate through the Underground Internet*, DIGITAL TRENDS (Jan. 19, 2016), http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/ (illustrating how encryption is layered for the nodes).

and only have the location of the second node when it transmits its own location and the information to its destination. Each node will see something different from the last, and the onion routing process will separate the user location and the content of the user data so that only the content remains by the time it reaches its destination. Outside users attempting to spy on the contents of the data packet, or ascertain its original location, will be unable to do either. Although the exit node will have access to the user's unencrypted communications, there is no way to track it back to the user's original location because there is no location information attached. This does not prevent users from encrypting their own data for superior security beforehand. To prevent the exit relay from accessing user data, end-to-end encryption such as SSL[22] will deliver a still-encrypted message through Tor.

USING TOR

For an individual seeking to use Tor, public access is available on The Tor Project's website: https://torproject.org. A copycat of Mozilla's Firefox browser, called "Tor Browser," which implements Tor for internet use, is freely offered for download and use on the website. The browser's design is very user-friendly, and various fora and blog posts exist online for potential users who seek to learn more about using Tor, how it works, and issues facing the Tor and Dark Web user community.[23] It is also possible to access the Tor network through other methods, such as specially created software. Plug-ins, mobile apps, and even entire operating systems, are available online and provide the similar protections.[24] The Tor browser is configured to attempt to control extraneous factors (addressed in the section below) which may not be addressed by other software. It is, therefore, also important to ensure that when using Tor, the protections sought by a user are actually put into place. To be sure Tor is working properly, a Tor Check site exists to affirm users that the protections are effective.[25] With these resources at hand, an individual user can effectively navigate the Tor network with relative ease and greater privacy.

---

[22] SSL.COM, http://info.ssl.com/article.aspx?id=10241 (last visited Nov. 16, 2016) ("SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.").

[23] THE TOR PROJECT, https://blog.torproject.org/ (last visited Nov. 16, 2016); DEEP DOT WEB, https://www.deepdotweb.com/ (last visited Nov. 16, 2016).

[24] *See Software and Services*, THE TOR PROJECT, https://www.torproject.org/projects/projects.html.en (last visited Nov. 16, 2016).

[25] CHECK THE TOR PROJECT, https://check.torproject.org/ (last visited Nov. 16, 2016).

Tor also provides protection to the hosts of websites which are created to be reachable only through the Tor network and accessible through a web address ending in ".onion" (rather than ".com"). The configuration of hidden services obscures the source of information by creating an intermediate host for content. Tor users can reach each other at hidden services, using them as rendezvous points for communications where neither can detect the other's identity, never exiting the Tor network[26] The Tor Project estimates that nearly 60,000 unique .onion addresses are up on the network daily on the hidden-service directory.[27] Many of these hidden services are associated with the Dark Web, part of which the FBI and other government enforcement agencies have sought to shut down in the past with some limited success.[28] Many hidden services are used for legitimate purposes, however, and provide an important outlet for content creators to disseminate information while maintaining a high level of protection.[29]

LIMITATIONS OF TOR

Even though Tor provides a high degree of privacy to its users, it is not completely impenetrable; proper usage is important to ensure security. Tor cannot protect users if the applications they use compromise the security Tor provides by making their data accessible in other ways. Tor users who visit sites like Facebook, which require a log in, lose their protections by logging in.[30] A local ISP or network provider may not know the user's physical location or destination site, but because the user logged into the site, they know who the user by virtue of his login credentials.[31] Law enforcement often uses personal identifying information found in transactions, such as those using Bitcoin, or posted in relation to particular online accounts to track down criminals despite

[26] *.Tor: Hidden Service Protocol*, THE TOR PROJECT, https://www.torproject.org/docs/hidden-services.html.en (last visited Nov. 16, 2016).
[27] *Unique .onion addresses*, THE TOR PROJECT, https://metrics.torproject.org/hidserv-dir-onions-seen.html (last visited Nov. 16, 2016).
[28] Press Release, U.S. DEP'T OF JUSTICE, *More Than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network* (November 7, 2014), https://www.justice.gov/opa/pr/more-400-onion-addresses-including-dozens-dark-market-sites-targeted-part-global-enforcement.
[29] JM Porup, *Building a new Tor that can resist next-generation state surveillance*, ARS TECHNICA, (Aug. 31, 2016), http://arstechnica.com/security/2016/08/building-a-new-tor-that-withstands-next-generation-state-surveillance/.
[30] *Tor FAQ*, *supra* note 12.
[31] *Id.*

their use of Tor.[32] In the takedown of the infamous Dark Web black market known as the Silk Road, FBI agents were able to track its creator, Ross Ulbricht, aka Dread Pirate Roberts, by linking several of his accounts in various online fora to a personal Gmail account, which allowed the FBI to locate him.[33] A user's own activity, as in the case of Dread Pirate Roberts, may be what deprives him of the protections provided by Tor.

Outside of what a user is posting online, actively updating content, such as Javascript, Adobe Flash, and QuickTime, can also access a user's account according to permissions in the user's operating system.[34] These technologies may be able to store data separate from your browser or operating system data stores.[35] This means these applications can access the data that your user account can access, ignoring proxy settings and bypassing Tor to share identifying information directly with other sites. Therefore, these technologies must be disabled in your browser to use Tor to its complete functional capabilities.[36] Although active content has the capability to bridge the gap between the user and his destination site, it can be disabled with relative ease by adjusting online settings.

Some organizations claim that they have compromised the Tor network through particular exploits.[37] Many seek to claim their superiority over Tor's network, from hackers to government agencies, either for bragging rights or to exercise control over the Tor users.[38] Often, however, the compromise of a user's identity is due to exploited human error, such as following a trail of money transfers or identifying information, as seen in like in the FBI investigation of Silk Road and Dread Pirate Roberts. The Tor Project does not seem overly concerned about any purported vulnerabilities to its network

---

[32] Press Release, U.S. DEP'T OF TREAS., *FinCEN Awards Recognize Partnership Between Law Enforcement and Financial Institutions to Fight Financial Crime*, (May 10, 2016), https://www.fincen.gov/sites/default/files/shared/20160510.pdf.

[33] Tim Hume, *How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road*, CNN (Oct. 4, 2013), http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/.

[34] *Tor FAQ*, *supra* note 12.

[35] *Id*.

[36] *Id*.

[37] *See, e.g.*, Andy Greenberg, *Global FBI Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED (Nov. 7, 2014), https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.

[38] *See, e.g.*, JM Porup, *supra* note 29 ("In 2014, the US government paid Carnegie Mellon University to run a series of poisoned Tor relays to de-anonymise Tor users. A 2015 research paper outlined an attack effective, under certain circumstances, at decloaking Tor hidden services (now rebranded as 'onion services'). Most recently, 110 poisoned Tor hidden service directories were discovered probing .onion sites for vulnerabilities").

outside of the realm of human error.[39] Despite any potential vulnerabilities, many recognize the value of having an privacy-protective network configuration such as Tor, and researchers who successfully find potential exploits in the Tor network often help to fix the problems they encounter.[40]

One additional limitation for potential Tor users is the network speed. Because the data needs to travel through several nodes, instead of a direct user-to-destination connection, and because of the limited capabilities of volunteers who run the nodes, the connection speed of the Tor network is slower than a normal internet search. A user considering adopting Tor may have to take the compromised connection speed into account.[41]

A VALUABLE, IF IMPERFECT, PRIVACY TOOL

Many who use Tor, for purposes both legitimate and illegitimate, depend on its protections for their safety. Its utility as a resource for private online communication has led to an expansion of the network and substantial support from all kinds of entities. The technology behind Tor's structure and onion routing system is an area that is constantly developing new methods to solidify its protections, as many groups with varying motivations actively seek to penetrate its network. No security system is perfect— but when used correctly, Tor can be an effective means of communicating, searching, or just browsing the web more securely.

---

[39] Dave Lee, *Dark net raids were 'overblown' by police, says Tor Project*, BBC NEWS (Nov. 10, 2014), http://www.bbc.com/news/technology-29987379.

[40] *See, e.g.*, Eric Bangeman, *Security researcher stumbles across embassy e-mail log-ins*, ARS TECHNICA (August 30, 2007), http://arstechnica.com/security/2007/08/security-researcher-stumbles-across-embassy-e-mail-log-ins/; Larry Hardesty, *Shoring up Tor*, MIT NEWS (July 18, 2015), http://news.mit.edu/2015/tor-vulnerability-0729.

[41] *Tor FAQ*, *supra* note 12.

HTTPS: STAYING PROTECTED ON THE INTERNET

Sang Ah Kim*

CITE AS: 1 GEO. L. TECH. REV. 119 (2016)
http://bit.ly/2gCbsOY

One may occasionally see five letters displayed at the beginning of a URL: HTTPS. To understand HTTPS and its importance in internet communication, it is first necessary to understand HTTP (Hypertext Transfer Protocol.) The difference of a single letter could contribute to the invasion of your privacy on the internet and the theft of your sensitive personal information.

HTTP is, at its core, a "protocol." A protocol dictates the structure of communication between an internet user and a website by establishing exactly how the two parties will exchange information and in what format.[1]An example of an internet communication is when a user clicks the title of an article on the Washington Post website–she is requesting that the website show her the article. The website takes the request and responds by displaying the article on the user's screen.[2] Think of a protocol as a set of rules that must be satisfied before two parties begin requesting and responding. To analogize, playing soccer has rules, such as the rule that players in general cannot use their hands to pass the ball. An internet communication would be like two players passing the ball to one another by kicking.

A challenge with online communications is the interception of requested information by a third party using a "man-in-the-middle," or MITM attack.[3] Similar to wiretapping, a MITM attack allows the an adversary to intercept the content of a user's information flows before it reaches its intended recipient, often without the user's knowledge. Data such as social security numbers and credit card numbers may be intercepted and end up on black market sites, where

---

* GLTR Staff Member; Georgetown Law, J.D. expected 2018; University of Georgia, B.A. 2014.

[1] *See* Victor Laurie, *Computer Protocols- TCP/IP, POP, SMTP, HTTP, FTP and More*, INTERNET TIPS AND TRICKS (Oct. 29, 2016), http://vlaurie.com/computers2/Articles/protocol.htm

[2] *See generally* Celine Otter, *World Wide Web: HTTP Request-Response Cycle*, CELINE OTTER (May 10, 2015), http://celineotter.azurewebsites.net/world-wide-web-http-request-response-cycle/.

[3] *See generally* Filip Jelic, *Man in the Middle Attacks*, DEEP.DOT.WEB (Oct. 10, 2016), https://www.deepdotweb.com/2016/10/10/man-in-the-middle-attacks/.

people freely engage in trading bulk personal data for money.[4] Personal information in bulk is a valuable commodity for consumer marketing companies who use bulk information to provide targeted advertising for businesses. This trade of "data mining" is not something new but has recently grown into a multibillion-dollar industry – often unbeknownst to the sources of the personal information.[5] Besides what a user directly types onto the screen and sends over as a request, information sent using HTTP includes browser information, website content, and other user-submitted information.[6] Browser information showing when the last update to the browser occurred can also be sensitive information, as third parties can take advantage of an outdated browser's security holes to display pop-up advertising; install spyware; and collect personal information for identity theft, among other uses.[7] By using HTTP, a user gambles with the risk of uninvited perusal and exploitation of his/her personal information by third parties.

Communicating via HTTPS, as opposed to using HTTP, makes a critical difference considering such risks. To understand the true significance of HTTPS, we must first learn about the internet's inherent vulnerability. The internet, at its inception, was designed with security assumed because it was designed for use in research, not for commercial means.[8] As third parties invented ways to exploit the information being sent and received online, people needed a way to secure the information against eavesdroppers. A process called "encryption," which hides the content of the information by scrambling the text and rendering it unreadable,[9] arose to compensate for the lack of security.

While its current uses may be cutting-edge, various forms of encryption have been in use for thousands of years.[10] One well-known use of encryption

---

[4] *Computer Hacking and Identity Theft*, PRIVACY MATTERS (2012), http://www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx.

[5] Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Aug. 24, 2014), http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/.

[6] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMO. M-15-13, POLICY TO REQUIRE SECURE CONNECTIONS ACROSS FEDERAL WEBSITES AND WEB SERVICES (2015), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf.

[7] *See generally* Paul Cucu, *The Ultimate Guide to Secure Your Online Browsing Today [Updated]*, HEIMDAL SECURITY (Oct. 26, 2016), https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/.

[8] *See* Craig Timberg, *A Flaw in the Design*, WASH. POST (May. 30, 2015), http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

[9] Eric Kangas, *The Case for Email Security*, LUXSCI FYI BLOG (Mar. 31 2015), https://luxsci.com/blog/the-case-for-email-security.html.

[10] *A Brief History of Cryptography*, RED HAT SEC. BLOG (Mar. 31, 2016), https://access.redhat.com/blogs/766093/posts/1976023.

was the Enigma cypher, used by Nazi Germany to protect the content of their military communication during World War II.[11] Encryption, by making the information unreadable, prevents an adversary employing a MITM attack from accessing the encrypted message; if MITM cannot make sense of the information, MITM cannot exploit the information.

HTTPS is HTTP fortified with encryption and more to account for these vulnerabilities. The "S" in HTTPS stands for a security protocol called "Secure Sockets Layer," which was later renamed to "Transport Layer Security" (hereinafter SSL/TLS).[12] Both names allude to a security "layer." As a security protocol, SSL/TLS dictates the structure of how the information will be secured. Among many requirements, SSL/TLS requires that the communication is encrypted.[13] Having an encrypted communication is like chatting on the phone in pig Latin to prevent an adversary wiretapping the line from understanding what is going on.

However, users quickly realized that encryption alone cannot stop a MITM attack or other forms of electronic eavesdropping. Remember that encryption prevents an adversary from making sense of the intercepted information by making the information unreadable. Meanwhile, the intended recipients – the user and the website – can put the encrypted information back into readable form by using a "key" that, in theory, only the two are supposed to have.[14] It is difficult, however, to securely share this key without creating a potential vulnerability to a MITM attack or other form of hacking.

Realizing that securely sharing the key is a problem, people avoided the question altogether by coming up with an encryption method that does not involve sharing the key. Named "public key exchange," this method uses a pair of keys instead of a single key – a public key and a private key.[15] The public key of the website is free for anyone in the public to get, and the private key of the website remains in private possession of the website. For example, the user encrypts the information with the website's public key, which anyone – including MITM – can freely obtain. The catch is that information encrypted with a public key can only be put back into readable form by using the private

---

[11] *See The Enigma Machine*, LEARN CRYPTOGRAPHY (Nov. 1, 2016), https://learncryptography.com/history/the-enigma-machine.

[12] *See What Is SSL (Secure Sockets Layer) and What Are SSL Certificates?*, DIGICERT (Nov. 4, 2016), https://www.digicert.com/ssl.htm.

[13] *See Verify TLS is Required*, CHECKTLS.COM (Nov. 20, 2016), http://www.checktls.com/assuretls.html.

[14] *See generally Description of Symmetric and Asymmetric Encryption*, MICROSOFT (Nov. 20, 2016), https://support.microsoft.com/en-us/kb/246071.

[15] Kangas, *supra* note 9.

key, the latter of which never leaves the website's sole possession to begin with. The public key exchange is like using a padlock. Ally buys a padlock and sends her padlock to Billy. Billy writes a note, places it in a box, and locks it with the padlock. Billy cannot unlock the padlock because only Ally has the key. When Billy sends the box with the padlock to Ally, anyone can see that something was sent using a box but cannot unlock the padlock to see its content.[16] Public key encryption appears to be an adequately secure encryption method to protect the content of communication from MITM.

Yet a more fundamental question remains to be answered: how do we know if a website is really what it says it is? Is there an outside source who can verify the website's authenticity? HTTPS makes another critical difference from HTTP in this regard. Remember that HTTPS uses SSL/TLS, the security protocol which requires encryption. In addition to encryption, SSL/TLS also requires the website to prove its identity before encryption even begins – a process called "authentication."[17]

Websites must register with a trusted organization, such as Verisign, which will investigate and vouch for the website's authenticity. Such an organization, called a Certificate Authority, makes the website prove its identity through some paperwork and a fee.[18] The organization sends the website a certificate saying that the presented public key for the website is actually the public key for the website, that this has been verified by the organization, and that the verification is valid for a certain period of time.[19] The website must present the certificate to the user, who will validate the authenticity of the website by using the certificate and asking a Certificate Authority if the certificate is valid.[20]

Certificates, like insurance, come with varying degrees of benefits that match the price tag.[21] There are numerous Certificate Authorities, some of which may not maintain high levels of data checking and reduce their costs at the expense of miss-issuing certificates or at the expense of securing phishing

---

[16] *See generally* Brian Proffitt, *Understanding Encryption: Here's The Key,* READWRITE (Sept. 19, 2013), http://readwrite.com/2013/09/19/keys-understanding-encryption/.
[17] *See* Eoin Keary, *Authentication Cheat Sheet*, OWASP (Mar. 2, 2016), https://www.owasp.org/index.php/Authentication_Cheat_Sheet.
[18] *See* Eric Kangas, *How Does Secure Socket Layer (SSL or TLS) Work?,* LUXSCI FYI BLOG (July 22, 2013), https://luxsci.com/blog/how-does-secure-socket-layer-ssl-or-tls-work.html.
[19] *Id.*
[20] *See* Keary, *supra* note 17.
[21] *See* Doug Beattie, *How Much Does an SSL Certificate Really Cost?*, GLOBALSIGN (Sep. 23, 2016), https://www.globalsign.com/en/blog/how-much-does-an-ssl-certificate-cost/.

or malware sites.[22] A certificate "ideal for ecommerce sites" through a more well-known Certificate Authority was priced starting at $599/year.[23]

Despite the security benefits of using HTTPS over HTTP, many websites still use HTTP, risking third-party exploitation of users' personal information.[24] Historically, HTTPS was primarily used for sensitive transactions on the internet, such as online payments and corporate information transactions.[25] Over time, however, websites such as Google and Facebook began adopting HTTPS. As of March 2016, Google stated that 77% of its online traffic is encrypted.[26] Obstacles to adoption for private actors include having to change a website's underlying code and needing time to test the access from various regions across the globe using a "diversity of devices."[27]

In a 2015 memorandum articulating recommendations for cybersecurity standards for federal websites**,** the Office of Management and Budget argued that "tangible benefits to the American public [in deploying HTTPS across federal websites] outweigh the cost to the taxpayer" in that a few malicious impersonation of official federal websites or eavesdropping on the said websites may create substantial risks to members of the public.[28] As of October 28, 2016, 58% of federal websites use HTTPS.[29] Still, various administrative and financial burdens, such as development time and the burden of maintenance, affect the rate of adoption for federal websites.[30]

A significant part of daily life on the internet will remain vulnerable to third parties if websites continue to use HTTP. HTTPS generally does not affect whether a website is vulnerable to hacking, due to the internet's inherently vulnerable design. HTTPS, however, protects the communication from impersonation by third parties; keeps potentially sensitive information secure;

---

[22] *Id.*

[23] *See ExtendedSSL*, GLOBALSIGN (Nov. 5, 2016), https://www.globalsign.com/en/ssl/ev-ssl/.

[24] *See* Brian Barrett, *Most Top Websites Still Don't Use a Basic Security Feature,* WIRED (Mar. 17, 2016), https://www.wired.com/2016/03/https-adoption-google-report/.

[25] Scott Gilbertson, *HTTPS is More Secure, So Why Isn't the Internet Using It?,* ARS TECHNICA (Mar. 20, 2011), http://arstechnica.com/business/2011/03/https-is-more-secure-so-why-isnt-the-web-using-it/.

[26] Michael Liedtke, *Google Reveals 77 Percent of its Online Traffic is Encrypted*, PHYS.ORG (Mar. 15, 2016), http://phys.org/news/2016-03-google-reveals-percent-online-traffic.html.

[27] *See* Owen Williams, *Wikipedia Now Uses HTTPS to Stop People Snooping on your Binge Learning*, THE NEXT WEB (Jun 12, 2015), http://thenextweb.com/insider/2015/06/12/wikipedia-now-uses-https-to-stop-people-snooping-on-your-binge-learning/#gref.

[28] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, *supra* note 6.

[29] *Secure HTTP (HTTPS)*, PULSE (Oct. 28, 2016), https://pulse.cio.gov/https/domains/.

[30] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, *supra* note 6.

and prevents the information from being tampered with or modified.[31] It is true that not all information exchanged across the internet necessarily requires impenetrable privacy; but with the increasing commodification of user activity on the internet and government surveillance, the threshold of what information we would allow to pass unencrypted might change quicker than expected.

[31] *See Introduction to HTTPS,* THE HTTPS-ONLY STANDARD (Nov. 5, 2016), https://https.cio.gov/faq/#what-does-https-do%3f.

FOR DRONE OPERATORS, PRIVACY IS KEY FOR SMOOTH TAKEOFF AND LANDING

Jonathan Frankle*

CITE AS: 1 GEO. L. TECH. REV. 125 (2016)
http://bit.ly/2fGdgWw

INTRODUCTION

In a few short years, our skies will be far more crowded. Existing avian occupants will have to share the space above our heads with a new, man-made species of flying machines carrying packages, cameras, and pizzas:[1] Unmanned Aircraft Systems (UAS), a.k.a., drones.

On neighborhood streets, Amazon Prime Air[2] will use a fleet of small drones to deliver orders in under half an hour, making these flying couriers as commonplace as UPS trucks. Emergency personnel have already begun deploying drones to enhance their search and rescue capabilities,[3] while law enforcement is doing the same to both extend the reach of border patrols[4] and

---

* Staff technologist at the Center on Privacy & Technology at Georgetown Law. He has a B.S.E. and M.S.E. in computer science from Princeton.

[1] Frank Rosario, *Pizzeria owner uses drone to deliver pie in test flight*, N.Y. POST (Nov. 7, 2014, 3:25 AM), http://nypost.com/2014/11/07/pizzeria-owner-uses-drone-to-deliver-pie-in-test-flight/.

[2] AMAZON, https://www.amazon.com/b?node=8037720011 (last visited Nov. 13, 2016).

[3] Matt McFarland, *Drone operators assist search and rescue efforts after devastating floods in Texas*, WASH. POST (May 29, 2015), https://www.washingtonpost.com/news/innovations/wp/2015/05/29/drone-operators-assist-search-and-rescue-efforts-after-devastating-floods-in-texas/.

[4] William Booth, *More Predator drones fly U.S.-Mexico border*, WASH. POST (Dec. 21, 2011), https://www.washingtonpost.com/world/more-predator-drones-fly-us-mexico-border/2011/12/01/gIQANSZz8O_story.html.

keep officers out of harm's way.[5] Drones are even being produced as entertainment products to enhance the consumer's visual experiences.[6] The future is full of promising possibilities as more and more entrepreneurs, hobbyists, and first responders become able to fly.

From a privacy perspective, however, these tiny airborne cameras and microphones could stretch the boundaries of digital surveillance into the physical world. Today, corporations compete using web trackers to monitor our every movement online.[7] Tomorrow, drones could make it possible to do the same in person. How will you know what a drone is really up to when it flies past your window or over your child's school? Policymakers and companies need to convincingly answer this question if they want to earn citizens' trust.

Right now, some proposals ask drone operators to publish information about where they plan to fly and what data (like pictures and video) they plan to collect.[8] This is a good start, but it only solves half the problem—we would not know whether an operator actually kept her promises. What did the drone actually do in practice? Ideally, any citizen should be able to answer this question with just a few clicks.

THE CURRENT REGULATORY LANDSCAPE

Privacy and civil liberties advocates, companies, and government officials are already working to develop ways to ensure that we retain our "reasonable expectation of privacy" once these robot copters take flight.

In December 2015, the Center for Democracy & Technology (CDT) proposed comprehensive voluntary best practices for private use of drones.[9] A few months ago, the National Telecommunications and Information Administration (NTIA) concluded its multistakeholder process on drones.[10]

---

[5] Brian Bennett, *Police employ Predator drone spy planes on home front*, L.A. TIMES (Dec. 10, 2011), http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211.

[6] GOPRO, https://shop.gopro.com/karma (last visited Nov. 13, 2016).

[7] *Online Behavioral Tracking*, ELEC. FRONTIER FOUND. (Sept. 29, 2016, 2:24 PM), https://www.eff.org/issues/online-behavioral-tracking.

[8] Press Release, Sen. Markey and Rep. Welch Introduce Legislation to Ensure Transparency, Privacy for Drone Use (Mar. 3, 2015), http://www.markey.senate.gov/news/press-releases/sen-markey-and-rep-welch-introduce-legislation-to-ensure-transparency-privacy-for-drone-use.

[9] *Model Privacy Best Practices for Unmanned Aircraft*, THE CTR. FOR DEMOCRACY & TECH. (Dec. 16, 2015), https://cdt.org/insight/model-privacy-best-practices-for-unmanned-aircraft/.

[10] *Multistakeholder Process: Unmanned Aircraft Systems*, NAT'L TELECOMM. & INFO. ADMIN (June 21, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

This process produced a consensus document of drone best practices,[11] and many of CDT's December 2015 recommendations are reflected in the NTIA best practices.[12] This resource should help drone operators use their aircraft in responsible, privacy-respecting ways.

Among other things, the recommendations emphasize transparency and accountability to help people view this nascent technology with excitement rather than fear. For example, the best practices document asks companies to publish how they expect to use their drones—flight purposes ("to deliver pizzas"), flight plans ("along Main Street from the pizza shop to customers' houses"), intended data collection and use ("a camera recording to make sure customers actually received the pizza"), and contact information.

This gesture is a great step in the right direction, but how do we know whether a drone operator actually followed these recommendations? Which, if any, sensors were *actually* activated in flight, and over whose back yard? When it comes to deploying a brand new technology with such invasive potential, trust is not enough. We need verification.

Unfortunately, the FAA rule requiring drone registration since December 21, 2015 does not solve this surveillance issue.[13] Instead, it requires owners of only small drones to pay a small fee and provide this name, physical address, and e-mail address.[14] It does not address the other verification issues that would likely be more troubling to the public at large.

Drone operators should consider adopting an approach that combines **auditing** with **access**. Although some might bristle at additional requirements for fear they could limit the growth of this emerging technology, these requirements may actually help spur the development of the technology. In exchange for recordkeeping and inspection, drone operators could get more flexibility in the flight plans they publish upfront. This framework would give companies greater room to experiment and adjust their proposed purposes as necessary, affording this technology the freedom to reach its full potential.

---

[11] *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*, NAT'L TELECOMM. & INFO. ADMIN (May 18, 2016), https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

[12] *Privacy and Civil Liberties Protections at Heart of NTIA Best Practices for Drones*, THE CTR. FOR DEMOCRACY & TECH. (May 18, 2016), https://cdt.org/press/privacy-and-civil-liberties-protections-at-heart-of-ntia-best-practices-for-drones/.

[13] *FAA Requires Drone Registration but Again Fails to Limit Drone Surveillance*, EPIC (Dec. 14, 2015), https://epic.org/2015/12/faa-requires-drone-registratio.html.

[14] *Id.*

AUDITING

Drone manufacturers should consider harnessing equipment that already exists to audit the flight activity of each drone in a way that builds privacy into the technology itself. For example, drones can be fitted with "black boxes" similar to those already found in cars and airplanes. These devices could record basic telemetry about the drone over the course of its lifetime, including its altitude, GPS coordinates, and physical positioning at certain time intervals. They could also record sensor metadata such as when a camera was activated and where it was pointed.

Individuals armed with this information could infer possible privacy violations (for example, when a drone passes over private property at a low attitude with its camera activated and pointed at a certain angle) without burdening companies with technologically onerous requirements. The mere act of being watched would encourage operators to alter their behavior in accordance with privacy expectations. Beyond privacy, this information would be vital for safety—drones will certainly suffer the occasional mechanical failure or operator mistake, and reliable flight data would help investigators sort out and learn from these incidents just as they do car and plane accidents today.

ACCESS

In order to ensure that these records truly hold operators accountable, someone needs to monitor the data. The ideal examiners are private citizens, who are best equipped to investigate the drones they personally see flying over their heads. To make this possible, flight data should be public—accessible to anyone with an internet connection.

However, such access could have unintended consequences. Reporting data in real time could grant too little privacy to operators, discouraging drone usage or revealing trade secrets. It might even create more privacy damage than it prevents (tracking drones from a sensitive healthcare company to a neighbor's house) or lead to unsafe situations (following a package delivery drone with the intent to steal its contents).

These side effects could be mitigated by obscuring the data enough to protect privacy without undermining its value for auditing. Instead of reporting in real time, for example, drone operators could release their data in a "timely" fashion—perhaps delaying publication by a few hours. They could also announce data for a time frame or geographic area rather than an exact moment or location.

Alternatively, operators could offer transparency by request. When someone sees an Amazon drone zip by, for example, she could contact the company's drone department to ask for more information.

Imagine a world in which a cooperative network of volunteers and local governments keeps track of drone movements over wide areas and submits this information to a centralized, online database as a free public service. This forum could be provided by the FAA or even as a voluntary industry service to consumers—a testament of good-faith drone operations that preserve individual privacy to the greatest extent possible.

CITIZEN TRUST IS ESSENTIAL

These mechanisms for accountability and transparency are not intended to punish drone operators before the technology even gets off the ground. To the contrary, building and maintaining citizen trust will be critical to this technology's success.

Many people are justifiably concerned about the prospect of hundreds, perhaps thousands, of drones buzzing around in formerly quiet airspace, peering into open windows, and even threatening citizens with weapons and other safety concerns.[15]

The right strategy is not to dismiss these fears as misguided. It is to make a concerted effort to assuage these concerns from the beginning, through transparency and accountability. This will result in strong yet adaptable privacy practices that will allow this promising technology to realize its full potential.

[15] Georgia Wells, *GoPro Recalls New Karma Drone*, THE WALL ST. J. (Nov. 8, 2016, 9:32 PM), http://www.wsj.com/articles/gopro-recalls-new-karma-drone-1478658769 (discussing the drones loss of power during flight); *See* Melanie Bates, *The FAA released rules for the operation of commercial drones*, FUTURE OF PRIVACY F. (June 21, 2016), https://fpf.org/2016/06/21/faa-released-rules-operation-drones-commercial-purposes/ (citing a Robohub article discussing the fact that operators will no longer be required to hold a manned aircraft pilot's license. This loosening of restrictions means that less qualified people will be piloting drones).

WHEN OTHER GOVERNMENTS WANT YOUR STUFF: RULES OF THE ROAD FOR CROSS-BORDER LAW ENFORCEMENT DEMANDS

Greg Nojeim*

CITE AS: 1 GEO. L. TECH. REV. 130 (2016)
http://bit.ly/2fGfKE9

This year marks the twenty-fifth anniversary of the public gaining access to the World Wide Web.[1] To say communications have come a long way since then would be quite the understatement. Today, billions of people around the world can be reached in seconds—a far cry from the time when email was only common among academics, government workers, and military personnel. Global connectivity can advance freedom, prosperity, and innovation, but it has also presented extraordinary challenges and opportunities for law enforcement. A prime example is digital evidence located overseas.

Before the internet, law enforcement officials investigating a crime rarely had to go through the trouble of obtaining evidence in a foreign territory. Now, the global popularity of U.S.-based companies such as Google and Dropbox has changed everything. In the Digital Age, German law enforcement officials investigating a crime that took place entirely in Berlin, with a German victim and a German alleged perpetrator, may often need access to communications content stored on servers on American soil. Under the current system, German officials would generally be able to compel the assistance of the American service providers only by filing a request under a Mutual Legal Assistance Treaty ("MLAT") or similar process, and then working with the Department of Justice's ("DOJ") Office of International Affairs ("OIA") to amass the information necessary for DOJ to make a probable cause showing in an American court.

There is a privacy benefit to requiring a warrant based on probable cause before a user's communications content is turned over to a country with a lower threshold for authorizing surveillance. However, the current process is

---

* Senior Counsel and the Director of the Freedom, Security, and Technology Project at the Center for Democracy & Technology (CDT). For CDT's more detailed analysis of the MLAT reform issue, *see Cross-Border Law Enforcement Demands: An Analysis of the Department of Justice's Proposed Bill*, CDT.ORG (Aug. 17, 2016), https://cdt.org/insight/cross-border-law-enforcement-demands-analysis-of-the-us-department-of-justices-proposed-bill-2/.

[1] Michelle Starr, *Happy 25th birthday to the World Wide Web*, CNET (Aug. 23, 2016), http://www.cnet.com/news/happy-25th-birthday-to-the-world-wide-web/#ftag=CAD590a51e.

sometimes painstakingly cumbersome[2] and is not keeping up with the deluge of requests for electronic content the DOJ now receives.[3] Moreover, the current system fails to protect the privacy of internet users' sensitive traffic data (such as email logs), which can be even more revealing than communications content.[4] Under current law, U.S. providers may *voluntarily* disclose their users' traffic data to foreign governments,[5] despite the fact that the U.S. government can only obtain such information with a warrant or a court order issued under 18 U.S.C. section 2703(d). Reforming the MLAT process should thus cover both content and traffic data. If it does, MLAT reform could be a unique opportunity to make domestic and international legal processes better suited to both legitimate law enforcement needs as well as privacy.

In July 2016, the DOJ proposed legislation that would be a step forward for law enforcement, but a leap backwards for privacy.[6] Under its proposal, select foreign governments would be able to make surveillance demands directly to U.S. providers under their own domestic procedures and standards. The DOJ, with the concurrence of the U.S. State Department, would decide which countries may enter into a bilateral agreement permitting these direct demands, based on a series of "factors" that are supposed to indicate whether a country provides adequate substantive and procedural privacy and civil liberties protections.

---

[2] The MLAT process takes an average of ten months. *See* THE PRESIDENT'S REV. GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD, 227 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[3] The number of requests from foreign authorities for computer records handled by the OIA increased ten-fold within the last decade. The overall number of requests for assistance from foreign authorities increased by nearly sixty percent during that time. *See U.S. Department of Justice FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform + $24.1 Million in Total Funding*, DEP'T OF JUST. (July 13, 2014), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[4] Greg Nojeim, *When Metadata Becomes Megadata: What the Government Can Learn*, CDT.ORG (June 17, 2013), https://cdt.org/blog/when-metadata-becomes-megadata-what-the-government-can-learn/.

[5] Although ECPA bars U.S. service providers from voluntarily disclosing metadata to "governmental entities" (18 U.S.C. § 2702(c)(6) (2012)), the Act defines "governmental entity" to include only U.S. federal, state, and local government agencies (18 U.S.C. § 2711(4) (2012)). This definition does not include foreign governments, which means U.S. communication service providers are free to voluntarily disclose user metadata—be it of a U.S. or non-U.S. person—to other governments.

[6] Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden, President of the United States Senate (July 15, 2015) (conveying proposed legislation and a section-by-section analysis) [hereinafter DOJ Proposal], http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf.

Bilateral agreements could be a viable mechanism for partially addressing the problem of cross-border law enforcement demands (or "C-BLED's") for digital content. Such arrangements should help decrease the wait time for law enforcement who need quick access to digital evidence stored overseas. They may also, in theory, encourage foreign governments to improve their privacy protections in order to qualify for such "express lane" agreements. However, substantial changes must be made to the DOJ's proposal to bring it more in line with human rights requirements. Here are some big-picture recommendations:

First, Warrants for Content. U.S. law must finally be updated to require a judicially approved warrant based on probable cause in order to access stored communications content in the United States. The U.S. already requires a warrant when a foreign government uses an MLAT request to seek content in the United States. The E-mail Privacy Act, which passed by a 419-0 vote in the House of Representatives, would require the U.S. government to obtain a warrant, as well, by updating the 1986 Electronic Communications Privacy Act (which currently permits the use of a mere subpoena to obtain certain types of emails).[7] The United States should get its own surveillance house in order before telling foreign governments what they should be doing with their surveillance practices.

Wiretapping. The provision of the DOJ bill that would allow foreign governments to conduct wiretapping on U.S. soil should be deleted.[8] Otherwise, the DOJ bill would go well beyond fixing the MLAT system—expanding surveillance to convey an authority to foreign governments not contemplated by the current system, and without many of the restrictions placed on such highly invasive conduct in the U.S. by the Wiretap Act.[9]

Establishing a Credible Designation Process. Whether a foreign government's laws and practices provide sufficient substantive and procedural human rights protections should be based on whether a series of *requirements* are met, not on mere "factors" to consider. Moreover, although the DOJ and the State Department should play an important role in the decision making process, they should not be the only deciders because their decisions may be influenced by political and other factors. Instead, the DOJ's decision to certify a country for a C-BLED agreement should be made subject to the notice and comment procedures of the Administrative Procedures Act.[10] This would enable human

[7] Email Privacy Act, H.R. 699, 114th Cong. (2016).
[8] *See* DOJ Proposal, *supra* note 6, at § 3(a).
[9] 18 U.S.C. §§ 2516-2518 (2012).
[10] 5 U.S.C. § 553 (2012).

rights and other experts to share their knowledge and opinions about that particular country. The DOJ should be obligated to respond to public comments and, before moving forward, should obtain the Senate's advice and consent (as is currently required for the approval of Mutual Legal Assistance Treaties.

Metadata Standards. ECPA should be amended to establish standards for disclosure of the most sensitive metadata (traffic data, such as email logs) to foreign governments. Traffic data can reveal one's interests, medical conditions, associations, and location over time. It is thus absurd to have no standard for foreign governments while requiring a court order based on specific and articulable facts for U.S. government access—the privacy invasion is severe, regardless of who obtains the metadata.

Encryption and the Scope of Provider Assistance. The DOJ's proposed legislation should bar foreign surveillance demands with provider assistance mandates that go beyond the level assistance providers must afford under current U.S. law. This would prevent the scope of such requests from reaching into the dangerous and politically dicey territory of mandated encryption backdoors—mandates that technology policy experts have warned would undermine the security mechanisms that internet users rely on to protect them from criminal hackers and rights-abusing governments.[11]

Reciprocity Provisions. The bill contemplates C-BLED agreements that are reciprocal (meaning the United States would obtain the same ability to make surveillance demands on the foreign providers in partner countries). However, there are no provisions in the bill that would operationalize these demands by the U.S. government. Clear, privacy-protective rules of the road for U.S. surveillance demands on foreign providers will be critical to avoiding abuse and gaining international acceptance of such bilateral agreements.

In addition to these big-picture recommendations, certain specific changes to the text of the legislation are essential:

Judicial Authorization. The DOJ legislation should require judicial or other independent authorization prior to any surveillance conducted pursuant to an agreement. It currently contemplates "orders" issued by foreign *governments*, not foreign courts. Moreover, those orders would be subject to oversight by independent authority only after-the-fact.

Evidentiary Standard. Judicial orders for surveillance under a C-BLED agreement should be based on a strong factual basis for the belief that a serious crime has been, is being, or will be committed, and a strong factual basis

[11] *See, e.g.*, Harold Abelson, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, CSAIL TECHNICAL REPORTS (July 6, 2016), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

for the belief that information relevant to the crime would be obtained by the surveillance. The current standard in the proposed legislation is too weak and too vague.

"Serious" Crime Definition. Cross-border law enforcement demands under a C-BLED agreement should be limited to crimes for which the maximum period of imprisonment is three years or more, or that involve violence, risk of serious bodily harm or death, sexual assault, human trafficking, or crimes against children, including child pornography. The DOJ legislation limits such demands to "serious" crimes, but leaves "serious" undefined.

Requirements of Foreign Law. As indicated above, each of the "factors" that would be considered in determining whether to enter into a C-BLED agreement with another country should be sharpened and should become a "requirement." In addition, legislation should give countries an incentive to abandon data localization mandates and extraterritorial warrants, which threaten to fragment the global internet and leave vulnerable citizens at the mercy of oppressive regimes.

Surveillance Involving Americans. The DOJ's proposed legislation does not authorize U.S. providers to disclose communications content pursuant to orders that "target" U.S. persons or persons located in the United States. The legislation should define what "targeting" means. In addition, if a U.S. prosecution is based in part on C-BLED-gathered evidence volunteered to the U.S. government, that fact should be disclosed to the defendant. A judge should be able to suppress that evidence if it was collected in a way that abused a C-BLED agreement in order to circumvent U.S. privacy protections.

Notice. The DOJ proposal should, but currently does not, require that the target of the foreign government's surveillance receive notice. Such notice could be delayed in limited circumstances to protect the investigation or prevent risk of flight or serious bodily harm.[12]

Bilateral agreements may be part of the solution to the problem of cross-border law enforcement demands. However, the DOJ proposal lacks adequate protections. If Congress considers C-BLED legislation, it should take an approach more respective of human rights and civil liberties of people in the United States and abroad. Such an approach will be crucial to carrying the global internet through the next twenty-five years and beyond.

---

[12] U.S. law requires notice to the target of a wiretap, to other parties to the wiretap "in the interests of justice," and to persons whose stored communications content is disclosed pursuant to a wiretap or a court order issued under 18 U.S.C. § 2703(d). U.S. law does not require notice to a person whose stored communications content is disclosed pursuant to a warrant. 18 U.S.C. § 2703(b)(1)(B) (2012).

DIFFERENTIAL PRIVACY: RAISING THE BAR

Anna Myers[*] & Grant Nelson[•]

CITE AS: 1 GEO. L. TECH. REV. 135 (2016)
http://bit.ly/2g27Tle

INTRODUCTION

Uncle Ben's sage advice in *Spiderman* that "with great power comes great responsibility," no doubt applies to today's great power: big data. Like Peter Parker, privacy advocates and technologists are racing to harness the power of big data's web of connections, but are sorely lagging in handling the power responsibly. Existing privacy protecting strategies, including de-identification, anonymization, pseudonymization, and encryption, have encountered bumps in the road. Data thought to be sufficiently de-identified has been re-identified;[1] anonymization and pseudonymization are considered privacy failures;[2] and encrypted email services have shut down in response to

---

[*] Attorney in Washington, D.C. where her practice focuses on privacy & technology legal matters. Ms. Myers' privacy-related experience includes the International Association of Privacy Professionals, Harvard University's Berkman-Klein Center for Internet and Society, the Network Advertising Initiative, and the U.S. Department of the Treasury's Office of Privacy, Transparency, and Records. She holds a J.D. from The George Washington University Law School and her B.A. in Rhetoric and Media Studies from Willamette University.

[•] Passed the D.C. bar and works for the Network Advertising Initiative in Washington. D.C. His experience includes launching several successful webapps, working for the Privacy Tools project at Harvard's Berkman-Klein Center for Internet and Society, and building predictive models. Mr. Nelson holds a J.D. from The George Washington University Law School. He thanks his parents for their loving support.

[1] *See generally* Arvind Narayanan & Edward Felton, *No Silver Bullet: De-Identification Still Doesn't Work*, http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf (2014); Latanya Sweeney, *Foundations of Privacy Protection from a Computer Science Perspective*, DATA PRIVACY LAB (2000), http://dataprivacylab.org/projects/disclosurecontrol/index.html.

[2] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); *see also* Arvind Narayanan & Vitaly

government subpoenas to protect their users' information.[3] The landscape is not, however, without hope: with every failure or data breach, technologists and advocates are evolving and building better privacy protections.

One such new protection is differential privacy. Differential privacy has been used in academic and research settings for nearly a decade but is just starting to break into the commercial space. Differential privacy describes a system that provides a protective layer between data and a user of the data in which the protective layer mathematically distorts the data with minor falsities so that it masks sensitive aspects of the data while retaining the statistically significant characteristics. Differential privacy is raising the bar for effective data responsibility by redefining the balance and reducing the trade-off between privacy and data utility.

DIFFERENTIAL PRIVACY: NOT DE-IDENTIFICATION[4]

Differential privacy is de-identification's cynical sibling. Differential privacy gained momentum in the wake of several high-profile failures of de-identification strategies, and its strengths reflect the frustration with the failure of de-identification. Whereas de-identified datasets are subject to re-identification attacks using other available datasets, differential privacy's threat model often assumes that bad actors or researchers "accessing any differentially private dataset are omniscient, omnipotent and constantly co-conspiring data snoops."[5] Differential privacy reduces the ambiguity of determining when data is sufficiently de-identified, and goes a level further than de-identification

Shmatikov,*Robust De-anonymization of Large Sparse Datasets*, SP '08 PROC. OF THE 2008 IEEE SYMP. ON SEC AND PRIVACY 111 (2008).

[3] James Ball, Julian Borger, & Glenn Greenwald, *Revealed: how US and UK spy agencies defeat Internet privacy and security*, THE GUARDIAN (Sept. 6, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[4] Differential privacy has primarily been identified as unique from de-identification. *See* Narayanan & Felton, *supra* note 1. The National Institute of Standards and Technology ("NIST") categorizes differential privacy as "privacy preserving data mining" and de-identification as "privacy preserving data publishing." U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS AND TECH., NISTIR 8053, DE-IDENTIFICATION OF PERSONAL INFORMATION (2015).

[5] Daniel C. Barth-Jones, *Ethical Concerns, Conduct and Public Policy for Re-Identification and Deidentification Practice: Part 3 (Re-Identification Symposium)*, HARV. L. BILL OF HEALTH (Oct. 2, 2013), http://blogs.harvard.edu/billofhealth/2013/10/02/ethical-concerns-conduct-and-public-policy-for-re-identification-and-de-identification-practice-part-3-re-identification-symposium/.

because it "seeks to mathematically prove that a certain form of data analysis can't reveal anything about an individual"[6]

Differential privacy does not prescribe the use of a specific algorithm or encryption technique. Unlike de-identification, which typically relies on omission or mutation of data, differential privacy can be conceptualized as a gatekeeping mechanism that serves as a privacy-protecting layer between raw data and a user of the data. The differential privacy layer can be applied to data at the point of collection or at the point of querying the data.[7] Applying the differential privacy layer at the point of collection provides additional protection while the data is stored and in transit. Applying the noise at the point of query allows the flexibility to later repurpose the data.

Protected datasets require all potential users to submit queries through the differential privacy-providing mechanism to access the dataset. When a user queries the data, the system evaluates that request against all previous queries and determines the sensitivity of the query. The system then applies noise or small-falsities to the data to protect the individual data subjects and returns an answer to the user. The noise injecting algorithm can be mathematically tuned to guarantee minimum levels of protection against reverse-engineering the underlying data. The key input to the algorithm is the *privacy budget*.

Every differential privacy system operates on a privacy budget— how much time, resources, and potentially traded utility the data controller is willing to trade in exchange for added privacy protection. The privacy budget of a differential privacy mechanism is a measurement of how much noise the algorithm injects to differentiate the data passed along from the true raw data. Determining the privacy budget is a social decision more than a mathematical one: the dataset's owner can increase the privacy budget (injecting more noise) on a dataset that contains sensitive information and decrease the privacy budget (resulting in more accurate responses) for a dataset that contains more innocuous data. If a query requires the system to exceed the privacy budget the system will not provide the answer to the user. A differential privacy layer can be tuned to prevent leakage of data even in a situation where every query of the data is from bad actors with an infinite timeline or query budget, collaborating with each other. If a privacy budget is depleted or exceeded that dataset may no

---

[6] Andy Greenburg, *Apple's 'Differential Privacy' is about Collecting your Data – But not* Your *Data*, WIRED (June 13, 2016), https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/.

[7] This allows for entities to be strategic about their data vulnerabilities and use differential privacy to adapt to their different environments and privacy needs. *See e.g.* Anthony Tockar, *Differential Privacy: The Basics*, NEUSTAR (Sept. 8, 2014), https://research.neustar.biz/2014/09/08/differential-privacy-the-basics/.

longer be usable. In a production database, however, the chances of a budget being depleted are slim given the rate at which new data can be added to datasets.

Despite the strong protections offered by differential privacy, it requires users to put their faith in the dataset owner's algorithms, typically without strong means to validate the integrity of the algorithm's noise injection. This is especially true when the data collector aggregates unencrypted data in a database and applies the differential privacy layer at the point of database query, rather than applying the differential privacy filter at the point of collection or contribution to the database. The need for a consumer to entrust a company with at least some data is all but unavoidable, and a shift towards using differential privacy provides more manageable and robust protection than its alternatives.

DIFFERENTIAL PRIVACY ENCODES PRIVACY LAW & POLICY IN ITS SYSTEMS

One of the main challenges of the privacy industry has been transforming complex concepts into technological tools. Privacy concepts are more challenging to implement technologically because they are not as straightforward as security concepts, such as user authentication. Security protections are objective and mechanical in nature with a united goal of keeping the data in and the bad actors out. Basic privacy concepts used by both the private and public sectors, such as the Fair Information Practice Principles ("FIPPs"),[8] are more subjective and therefore more challenging to translate into code or technological tools.

The FIPPs framework originated from a 1973 report issued by the precursor to the U.S. Department of Health and Human Services,[9] and was later codified in the Organisation for Economic Co-operation and Development ("OECD") privacy guidelines.[10] The FIPPs are the core of the Privacy Act of

[8] Robert Gellman, *Fair Information Practices: A Basic History*, (June 17, 2016), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[9] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, NO. (OS)73-94, REPORT OF THE SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

[10] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION & DEV. (1980), https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

1974,[11] and form the basis of other policy frameworks, such as the Department of Homeland Security privacy guidelines.[12] The principles are as follows:[13]

1. **Transparency**: information collectors should be transparent in their collection, use, dissemination, and maintenance practices.
2. **Individual Participation**: consent of the individual for the collection of the data should be obtained.
3. **Purpose Specification**: the specific purpose(s) the information is being collected for should be articulated.
4. **Data Minimization**: only the information necessary to accomplish the specified purpose should be collected.
5. **Use Limitation**: the information should only be used for the specific purpose(s) for which it is being collected.
6. **Data Quality and Integrity**: To the extent practicable collected information should be accurate, relevant, timely, and complete.
7. **Security**: Collected information should be protected from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing**: Collecting organizations should be accountable for compliance with the FIPPs and the use of information should be audited to demonstrate compliance with the FIPPs and all applicable data protection requirements.

Privacy Enhancing Technologies ("PETs") integrate concepts like the FIPPs, other privacy best practices, and applicable legal regimes in their design. For example, in the United States, the faster a video is uploaded, the better; however, in areas where governments suppress information, slower upload speeds may be desired so that a video upload does not appear different from other internet traffic. A PET for that scenario could be designed to protect the content of the video by masking it as other internet traffic, and thereby avoid raising any red flags. An implementation of differential privacy is a privacy enhancing technology (PET) because developers utilize the FIPPs and take into consideration the types of data in a database and applicable laws & policies in designing a system.

---

[11] 5 U.S.C. § 552a (2014).

[12] HUGO TEUFEL III, U.S. DEP'T OF HOMELAND SEC., MEMO. NO. 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM at 3-4. (Dec. 29, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[13] Descriptions of FIPPs adapted from *id.*

Differential Privacy in Research

Differential privacy was formalized by and is most strongly associated with Cynthia Dwork's work while at Microsoft Research. In 2006, Dr. Dwork published "Differential Privacy," a 12-page paper presented at the 33rd International Colloquium on Automata, Languages and Programming, part II.[14] Since then cryptologists, mathematicians, and computer scientists have pursued academic research on differential privacy resulting in a multi-disciplinary research effort.

Harvard's Berkman-Klein Center and MIT have pushed the multidisciplinary approach by bringing together computer scientists and attorneys from the Berkman-Klein Center, social scientists from the Institute for Quantitative Social Science, and mathematicians and cryptologists from MIT in the PrivacyTools Project.[15] Their research is a multi-faceted approach to protecting privacy while preserving the value of data, with the goal of including promising techniques in the open-source database software, Dataverse. Because of the imperative to maintain data's value while also maximizing user privacy, differential privacy has proven to be a large focus of their attention. Aaron Roth, an associate professor of computer and information science at the University of Pennsylvania, co-authored the essential textbook *The Algorithmic Foundations of Differential Privacy* with Dr. Dwork.[16] Roth's expertise in the mathematical foundations of differential privacy was affirmed when Apple sought his review of its algorithms prior to announcing publicly that it will deeply integrate differential privacy into its devices.[17]

Differential Privacy in Commerce

Several companies have started to implement differential privacy into their data acquisition and storage systems. Most notably, Apple recently announced that it will integrate differential privacy mechanisms into its iOS

[14] Cynthia Dwork, *Differential Privacy*, MICROSOFT (Feb. 2016), https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf

[15] *Harvard University Privacy Tools Project*, HARV. UNIV., http://privacytools.seas.harvard.edu/ (last visited Nov. 21, 2016).

[16] Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy, in* FOUNDATIONS AND TRENDS IN THEORETICAL COMPUTER SCIENCE: VOL. 9: NO.3–4 211 (2014).

[17] Kate Conger, *What Apple's differential privacy means you're your data and the future of machine learning*, TECHCRUNCH (June 14, 2016), https://techcrunch.com/2016/06/14/differential-privacy/.

devices for some use cases.[18] Apple's implementation aligns with its branding as a privacy-protecting organization: as it will perform the privacy-protecting noise injection at the device-level collection point rather than at the database level, consumer data will remain more secure during transmission and storage. Therefore, protected data leaving any particular iOS device is of minimal use to malicious actors that intercept the transmission, and any database of protected information is of minimal value if breached. Apple is not alone in placing the noise-injection calculations on devices: Google has implemented a differential privacy mechanism, at the device-level for its Chrome browser usage data.[19] Google's Randomized Aggregatable Privacy-Preserving Ordinal Response ("RAPPOR") preserves the predictive power of data in relatively large datasets.[20] Some experts believe Google's RAPPOR project is the first commercial deployment of differential privacy.[21]

Additionally, Facebook, no stranger to privacy and big data policy discussions, appears to have implemented a differential privacy mechanism in its advertisement audience estimator tool as early as 2012.22 The tool allows a potential advertiser to estimate how many Facebook users would view an ad based on the ad's target segments, such as location, age, and interests. As shown by Andrew Chin and Anne Klinefelter, Facebook not only rounds estimates to the nearest 20 (and zero if below 40), it appears to apply the rounding to an already-noisy estimate in a pattern that strongly suggests a differential privacy mechanism is at play.23 Differing from Google and Apple, Facebook does not seem to implement the noise-injection calculation prior to the user sending data to Facebook for retention, but rather keeps all user data in pristine condition and adds noise at the moment of database query.

---

[18] Andy Greenberg, *supra* note 6.

[19] Ulfar Erlingsson, Vasyl Pihur & Aleksandra Korolova, *RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response*, CCS '14 PROC. OF THE 2014 ACM SIGSAC CONF. ON COMPUT. AND COMMS. SEC. (2011), http://static.googleusercontent.com/media/research.google.com/en//pubs/archive/42852.pdf.

[20] *Id.* at 1 ("Randomized Aggregatable Privacy-Preserving Ordinal Response, or RAPPOR, is a technology for crowdsourcing statistics from end-user client software, anonymously, with strong privacy guarantees. In short, RAPPORs allow the forest of client data to be studied, without permitting the possibility of looking at individual trees.").

[21] Answer by Aaron Roth, QUORA (June 18, 2016), https://www.quora.com/Does-Google-use-a-differential-privacy-strategy.

[22] Andrew Chin & Anne Kleinfelter, *Differential Privacy As A Response To The Reidentification Threat: The Facebook Advertiser Case Study*, 90 N.C. L. REV. 1418, 1456 (May 2012).

[23] *Id.* at 1443.

A popular criticism of differential privacy states that enormous data sets would be required for a system to preserve the utility of a differentiated dataset. By injecting noise using a Laplace distribution,[24] as modeled by Dwork, Roth, and others, smaller companies have reported impressive accuracy. For example, Snips, an artificial-intelligence company with an emphasis on privacy showed that a model trained on only 1000 observations filtered through a differential privacy mechanism relying on a Laplace distribution had the same predictive accuracy as a model trained on 1 million observations relying on the RAPPOR distribution.[25] In fact, their research showed that the predictive accuracy of a model using data sourced from a differential-privacy system plateaued at as few as 10,000 observations.

Now that the use and development of privacy tools such as differential privacy is growing, the integration of those tools with other technologies provides comprehensive solutions to maximize the potential for privacy by design and user protection. The growing availability of differential privacy mechanisms in academic literature and open source libraries, combined with the fact that even small datasets can be protected using differential privacy and remain valuable makes it likely that more commercial implementations of differential privacy are on the horizon, something that should be encouraged by the legal and regulatory environment.

[24] A common probability distribution used in probability theory and statistics, also sometimes known as a double exponential distribution.

[25] Morten Dahl & Joseph Dureau, *Differential Privacy for the Rest of Us*, MEDIUM (July 29, 2016), https://medium.com/snips-ai/differential-privacy-for-the-rest-of-us-665e053cec17.

EMERGING TRENDS IN INTERNATIONAL DATA BREACH LAW

Alexandria Bradshaw*

CITE AS: 1 GEO. L. TECH. REV. 143 (2016)
http://bit.ly/2fKItei

INTRODUCTION

We've seen an unprecedented number of breaches in the United States in recent years, spanning both the public and private sectors. Despite how critical data privacy laws are to preventing breaches and sustaining internet health, the U.S. lacks a comprehensive consumer privacy law and national data breach standard, even though there is an emerging thrust of legislation in other nations unifying breach protections under one national privacy law. Instead, the U.S. has a patchwork of privacy laws that leave some personal information unprotected in surprising ways, and a general purpose consumer protection law enforced by the Federal Trade Commission ("FTC") that maps imperfectly onto privacy rights. Legislators have attempted to enact data breach laws; at least 11 bills were introduced in Congress in 2015. However, these bills were stalled largely by disagreement over the extent to which a federal law should preempt more privacy protective state data breach laws.

Nevertheless, other countries have enacted and are beginning to enforce data breach regulations that will have an effect on U.S. companies doing business abroad. Many of these laws are more stringent than similar provisions in U.S. federal laws with breach provisions, such as the Gramm-Leach-Bliley

* Privacy and cybersecurity advisor at Brunswick Group, a global corporate relations and crisis response firm. Prior to joining Brunswick, she was a lawyer at Center for Democracy & Technology, where she focused on commercial data privacy and security issues, including breach preparedness. She is a graduate of Boston College and Harvard Law School.

Act ("GLBA")[1] and Health Information Technology for Economic and Clinical Health Act ("HITECH").[2] The EU's General Data Protection Regulation ("GDPR")[3] and South Africa's Protection of Personal Information Act ("POPI")[4] are two examples. Below is an overview of three aspects of GDPR and POPI that may reflect emerging trends in international data breach law.

THE DEFINITION OF COVERED INFORMATION IS NOT LIMITED TO FINANCIAL AND HEALTH DATA

A major difference between international data breach standards and U.S. law is their applicability. U.S. privacy laws only apply to certain classes of information – GLBA addresses financial data, HITECH and the Health Insurance Portability and Accountability Act ("HIPAA")[5] govern health data, the Family Educational Rights and Privacy Act ("FERPA")[6] regulates maintenance of educational records, and the Children's Online Privacy Protection Act ("COPPA")[7] applies to children's data. FERPA and COPPA do not address data breach, and although GLBA and HITECH (a complementary law to HIPAA) include breach response standards, their protections are limited to financial and health data. Section 5 of the FTC Act gives the FTC power to address "unfair or deceptive" business practices, and has been used to impose penalties for poor data security practices leading to breaches of any type of data.[8] However, Section 5 does not give the FTC authority to put rules in place to prevent breaches or require businesses to notify anyone of a breach. In sum, U.S. federal law provides very few breach protections for information beyond financial or health data.

Both the GDPR and POPI will protect a more expansive group of information than existing U.S. federal laws in the event of a breach. The GDPR applies to "any information relating to an identified or identifiable

[1] 15 U.S.C. § 6801 (2012).
[2] 42 U.S.C. § 17921 (2009).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 (Apr. 27, 2016) [hereinafter "GDPR"].
[4] Protection of Personal Information Act 4 of 2013.
[5] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).
[6] 20 U.S.C. § 1232(g) (2012).
[7] 15 U.S.C. § 6501 (1998).
[8] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

natural person ('data subject')."[9] This includes a person's name, identification number, location data, online identifier or information on the "physical, physiological, genetic, mental, economic, cultural or social identity" of the person. Similarly, POPI's breach provisions apply to all "personal information,"[10] defined as any information related to an individual, including (but not limited to) demographic information and information on their marital, occupational, religious, health, or educational status. "Personal information" also includes the individual's opinions or someone else's opinions on the individual.

THE DEFINITION OF "BREACH" IS NOT TIED TO PARTICULAR HARMS EXPECTED TO RESULT FROM THE BREACH

U.S. laws that include data breach provisions generally only require notification to regulatory authorities or affected persons if the breach is expected to result in a particular type or level of harm. GLBA, for example, only requires notification when the incident is expected to result in "substantial harm." The law leaves it up to the regulated entity to determine whether the incident meets this threshold. HITECH requires notification when the breach "compromises the security or privacy" of the information and, similar to GLBA, leaves it up to the breached entity to determine whether the incident reaches this level. Even some state breach laws tie notification to demonstrated or expected harm;[11] many only require notification when the breach is expected to cause concrete harms such as fraud or identity theft.

In contrast, under POPI, any suspicion that personal information has been accessed or acquired by an unauthorized person must be reported to both the affected individual and the enforcing agency (the "Information Regulator") regardless of the harm the incident might cause. Likewise, the GDPR triggers notification to the member nation's supervisory authority when any personal data has been breached, whether or not the breach will cause harm. The GDPR does limit *consumer* notification slightly; it only requires notification to an individual when the breach is "likely to result in high risk to the rights and freedoms" of that person.[12] Given European views of privacy, this limitation is likely to be interpreted in a more privacy protective manner than U.S. law.

---

[9] GDPR, *supra* note 3, at art. 4(1).
[10] Protection of Personal Information Act 4 of 2013 § 5(a)(ii).
[11] *See e.g.*, Ark. Code § 4-110-101; Fla. Stat. § 501.171; Iowa Code §§ 715C.1-715C.2; La. Rev. Stat. § 51:3071.
[12] GDPR, *supra* note 3, at art, 33(1).

SHORTER PERIODS FOR NOTIFICATION TO AUTHORITIES AND AFFECTED INDIVIDUALS

POPI and the GDPR also require notification in a shorter timeframe than many U.S. laws. POPI requires breach notification to authorities and affected individuals "as soon as reasonably possible after discovery of the compromise" and the notification must be made in writing with sufficient information to allow the individual to take protective measures. The GDPR is similarly strict. Notice must be provided "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[13] These standards are markedly shorter than HITECH, which requires notification "without unreasonable delay,"[14] but gives entities up to 60 days to notify stakeholders after a data breach is discovered. Moreover, although many U.S. state laws require notification "as soon as possible"[15] or "as expeditiously as practicable,"[16] state laws that put a time limit in place for notification often give breached organizations 45 or more days to notify.[17]

What do these trends mean for American companies? While the GDPR and POPI cannot determine data breach response standards for countries outside of their jurisdiction, they are certainly persuasive authority. The GDPR applies to every EU member state – most of which do business with and host offices for companies across the globe – and it asserts authority whenever companies handle EU citizens' data, regardless of whether the company is in the EU. Additionally, South Africa's legislative framework and its constitutional courts serve as a model for many nations. At least one expert credits South Africa's influence over international jurisprudence to it being "not American, thus rendering [its] reasoning more politically palatable to domestic audiences in an era of extraordinary U.S. military, political, economic, and cultural power."[18] Chances are these sentiments will only increase in the years to come. Data breach legislation will likely move swiftly ahead in other nations, whether or not the Trump Administration or next Congress decide to push for it at home. U.S. companies must prepare now to comply with these new standards if they expect to remain globally competitive.

---

[13] *Id.*
[14] 42 U.S.C. § 17932 (2009).
[15] Wyo. Stat. Ann. §40-12-501.
[16] Fla. Stat. § 501.171.
[17] *See e.g.*, Ohio Rev. Code Ann. § 1349.19.; Vt. Stat. Ann. tit. 9 §§ 2430, 2435; Wis. Stat. §134.98.
[18] Anne-Marie Slaughter, *A Global Community of Courts*, 44 HARV. INT'L L.J. 191, 198 (2003).

A MODERN MAJOR STATUTE: ILLINOIS RAISES THE BAR IN PROTECTING CITIZEN PRIVACY FROM CELL SITE SIMULATORS

Jeremy Greenberg*

CITE AS: 1 GEO. L. TECH. REV. 147 (2016)
http://bit.ly/2fZhOZ0

INTRODUCTION

It was recently discovered that Baltimore, MD—a city known for its aggressive policing of black communities, had used cell site simulators ("CS simulators")[1] to surveil these communities over 4,300 times in the last eight years.[2] All done in secret, without a warrant.[3] 4,300 already seems like a considerable figure; however, comparing it to the number of simulators deployed in New York and San Diego underscores its true magnitude. Baltimore employed four times more simulators than New York City and eleven times more than San Diego over that same time period, despite the fact that both of those cities are more than twice its size.[4] Welcome to Baltimore—where your race may put your civil liberties at risk.

---

* GTR Staff Member; Georgetown Law, J.D. expected 2018; Ithaca College, B.S. 2009.

[1] CS simulators are devices that mimic cell towers, tricking cellphones to transmit their signal to the device. This allows the user, such as a police officer, to track the location of a targeted cellphone without the cellphone owner's knowledge. Some CS simulators also allow law enforcement to access the content of the cellphone's communications, such as the Fishhawk model, which allows the user to eavesdrop on conversations.

[2] Brian Barrett, *The Baltimore's Race PD Bias Extends to High—Tech Spying Too*, WIRED (Aug. 16, 2016, 8:01 AM), https://www.wired.com/2016/08/baltimore-pds-race-bias-extends-high-tech-spying/.

[3] *Id.*

[4] *Id.*

According to the Department of Justice, the practice of deploying CS simulators should require a warrant and only be used when necessary to achieve appropriately severe public safety objectives, such as apprehending a fugitive or locating a kidnapped child.[5] However, the DOJ only regulates CS simulators at the federal level, leaving states to regulate their own use.

To protect these heavily surveilled populations from civil liberty violations, state lawmakers should look to the recently enacted Illinois Citizen Privacy Protection Act.[6] With this new law, Illinois joins several other states in requiring law enforcement to obtain a warrant prior to deployment.[7] Moreover, Illinois' law sets a new high benchmark for protecting civil liberties by including an exclusionary remedy for unlawful deployment, prohibiting non-disclosure agreements between CS simulator manufacturers and law enforcement, and mandating the deletion of data incidentally collected from non-targeted devices.[8] These new regulations are crucial for protecting the civil liberties of all citizens, but are especially vital for historically disadvantaged communities, like African-Americans, who are frequently subject to disproportionally frequent and aggressive policing.[9]

ILLINOIS SETS THE BAR HIGH WITH AN EXCLUSIONARY REMEDY

The addition of a Fourth Amendment exclusionary rule for all unlawful use of CS simulators will help deter law enforcement from deploying CS simulators for justifications that do not meet the probable cause threshold.[10] The purpose of the exclusionary rule is to incentivize police to exercise careful deliberation required by the Constitution when exercising the investigative

[5] U.S. DEPT. OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 1 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download.
[6] Citizen Privacy Protection Act, 725 Ill. Comp. Stat. Ann. 137 (2016).
[7] Shahid Buttar, *Illinois Sets New Limits on Cell-Site Simulators*, ELEC. FRONTIER FOUND. (Aug. 11, 2016), https://www.eff.org/deeplinks/2016/08/illinois-sets-new-limits-cell-site-simulators (stating California, Washington, Utah, Minnesota, and Virginia all require law enforcement to obtain a warrant prior to deployment of a CS simulator).
[8] *Id.*
[9] U. S. DEP'T OF JUST., INVESTIGATION OF THE CITY OF BALTIMORE POLICE DEPARTMENT (2016), https://www.justice.gov/opa/file/883366/download; *see also*, U.S. DEP'T OF JUST., INVESTIGATION OF FERGUSON REPORT (2015) https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf.
[10] *Id.*

prerogative that accompanies their role.[11] In turn, prohibiting the use of evidence obtained unlawfully provides relief to defendants who were subjective to illegal surveillance.[12] Ultimately, this will help deter the widespread surveillance for routine street crimes that are far below the Department of Justice's "necessary" threshold.[13] A more limited scope for the use of CS simulators will protect the rights of those being surveilled, while promoting and limiting service disruption in heavily surveilled communities where the collateral effects of untrammeled use of the technology are the highest.

IMPACT OF CS SIMULATORS

A reduction in CS simulator surveillance will benefit heavily-surveilled communities, as CS simulators negatively impact the safety of users who are not deliberately targeted by the device, but are within its vicinity.[14] A CS simulator emits a signal stronger than those emitted by nearby cell towers, forcing mobile devices within a given coverage area to connect to it in lieu of connecting to the cell tower during CS simulator deployment.[15] After the CS simulator attracts the mobile devices within its range, the CS simulator operator will target a particular device and release all others. This process, known as "catch-and-release," will cause delays in service for all of the phones that attempted to connect to the CS simulator.[16] These disruptive service delays can have dire public safety consequences by preventing important communications, such as blocking 911 calls.[17] 911 calls are said to override the catch-and-release process, but a study from Canada shows that the override does not function up

---

[11] Nathan Freed Wessler, *A 30-Year-Old Loophole Increasingly Gives Police Officers a Pass When They Violate the Fourth Amendment*, Slate (Oct. 29, 2014, 11:49 AM), http://www.slate.com/articles/news_and_politics/jurisprudence/2014/10/police_s_good_faith_exception_courts_keep_expanding_exception_that_gives.html.

[12] *Id.*

[13] Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications at 8-9, Baltimore City Police Dept. (F.C.C. 2016) http://s3.documentcloud.org/documents/3015561/CS-Simulators-Complaint.pdf [hereinafter *Complaint*].

[14] Kim Zetter, *Feds Admit That Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015, 4:55 PM), https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/.

[15] *Id.*

[16] *Id.*

[17] Colin Freeze, *RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals*, THE GLOBE & MAIL (May 24, 2016, 3:21 PM), http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memoreveals/article29672075/.

to half the time, effectively blocking 911 calls.[18] This high margin of error can be devastating on a community that is frequently surveilled. Moreover, the catch-and-release of other emergency calls, such as those to a doctor or loved one, will be delayed because of the catch-and-release, and could result in similarly concerning consequences, in addition to inconvenience.[19]

In addition to more drastic public safety concerns, the frequent deployment of CS simulators causes service disruption for the use of mobile devices more generally. CS simulators can degrade cellular service within the area to 2G service, which is required for authentication with the targeted mobile device.[20] This will result in the service of every mobile device attempting to connect to be knocked down to the now archaic 2G protocol, resulting in slower data transmission, which harms device functionality. In addition, the strong signals sent by CS simulators that force all mobile devices to connect to it drain the phones' batteries at a faster than rate than they otherwise would.[21] Finally, the catch-and-release attacks on mobile phones result in delayed and dropped calls for all targeted and untargeted phones in the area.[22] Though these service disruptions are less harmful to public safety than dropping 911 calls, and may be a necessary tradeoff in a narrow category of high-priority targets, such widespread disruption is a detrimental and inconvenient byproduct of what should be considered illegally broad surveillance.

TRANSPARENCY NOW REQUIRED

The Illinois Citizen Privacy Protection Act also encourages increased transparency by banning non-disclosure agreements between CS simulator manufacturers and law enforcement.[23] While lawmakers generally understand how CS simulators function, non-disclosure agreements shroud the specific capabilities of the devices.[24] Some prosecutors have gone so far as to drop

[18] *Id.*
[19] Zetter, *supra* note 14.
[20] Stephanie Pell, *We Must Secure America's Cell Networks —From Criminals and Cops*, WIRED (August 27, 2014, 6:30 AM), https://www.wired.com/2014/08/we-must-secure-americas-cell-networks-from-criminals-and-cops-alike/.
[21] Joel Hruska, *Stingray, The Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move*, EXTREME TECH (June 17, 2014, 4:51 PM), http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move.
[22] Zetter, *supra* note 14.
[23] 725 Ill. Comp. Stat. Ann. 137/15(a)(1).
[24] Jeremy Scahill and Margot Williams, *Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone*, THE INTERCEPT (Dec. 17, 2015, 12:23 PM),

charges to prevent disclosing technical specifications of certain CS simulators to courts.[25] In fact, much of the knowledge of the capabilities of CS simulators has come in the form of leaked instruction manuals, such as for the popular "StingRay" model manufactured by Harris Corporation.[26]

However, the dearth of information is soon to change. The first-of-its-kind transparency requirement will finally give Illinois decision-makers insight into the precise surveillance capabilities of CS simulators, and how law enforcement agents deploy them. This increased knowledge will allow decision-makers to make more informed decisions relating to citizens' rights, and allow the populations being surveilled to have a greater understanding of how law enforcement interferes with their privacy and use of mobile devices. Further, more information about the technology behind CS simulators will open the door for technicians to develop methods of surveillance that are less invasive for the un-targeted devices in the area.

PROHIBITION ON COLLECTING CONTENT

The Illinois law also precludes CS simulators from retaining content of communications by requiring data incidentally collected from non-targeted devices to be deleted.[27] It specifically requires that all non-targeted data must be deleted as "reasonably practicable," within 24 hours of collection from known targeted devices, and within 72 hours of identifying an untargeted device.[28] The inclusion of the requirement to delete all non-targeted data is crucial, as it has come to light through the leaking of CS simulator user manuals that CS simulators deployed by law enforcement can capture and retain metadata.[29] The capturing of the actual content of communications could have a chilling effect on activities protected by the First Amendment in communities that are targeted on a frequent basis.[30] This will be especially true in protests

---

https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/.

[25] *See* Cyrus Farivar, *Prosecutors Drop Robbery Case to Preserve Stingray Secrecy in St. Louis*, ARS TECHNICA (Apr 20, 2015, 8:00 AM), http://arstechnica.com/tech-policy/2015/04/prosecutors-drop-robbery-case-to-preserve-stingray-secrecy-in-st-louis/.

[26] Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, THE INTERCEPT (Sep. 12, 2016, 2:33 PM), https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

[27] 725 Ill. Comp. Stat. Ann. 137/10.

[28] *Id.* at 137/15(b).

[29] Jennifer Lynch, *Stargazer III: Ground Based Geo-Location (Vehicular)*, THE INTERCEPT, https://theintercept.com/surveillance-catalogue/stargrazer-iii/ (last visited Sept. 30, 2016).

[30] *Complaint*, *supra* note 13, at 25.

critical of aggressive policing, which often occur in communities that are subject to the most surveillance.[31] With the knowledge that this technology is being used by law enforcement, it is crucial for regulations to specifically preclude this behavior.

OTHER STATES SHOULD FOLLOW SUIT

Though the Illinois Citizen Privacy Protection Act does not solve all the issues surrounding the harmful deployment of CS simulators, it facilitates scrutiny of deployment; reduces a public safety risk; broadly encourages transparency surrounding the device's capabilities; and diminishes collateral privacy violations. Other states should follow Illinois in an effort to bring state legislation in line with the Department of Justice's stated goal of increasing public safety, rather than jeopardizing it by allowing law enforcement's violation of civil liberties to remain unchecked.

[31] *Id.* at 26-27.

DECONSTRUCTING DATA MINING: PROTECTING PRIVACY AND CIVIL LIBERTIES IN AUTOMATED DECISION-MAKING

Lindsey Barrett*

CITE AS: 1 GEO. L. TECH. REV. 153 (2016)
http://bit.ly/2fvNLvE

INTRODUCTION

"Big Data" is the bogeyman of the information age: powerful, and as ill-defined as it is abstractly threatening. Broadly, it encompasses "technology that maximize[s] computational power and algorithmic accuracy";[1] "types of analyses that draw on a range of tools to clean and compare data";[2] and the underlying belief in the correlation between the size of the data set, and its ability to produce increasingly accurate and nuanced insights.[3] Put another way, "'Big data' [is] the amassing of huge amounts of statistical information on social and economic trends and human behavior."[4] The belief in the prescient value of big data has led to widespread collection of information on citizens and consumers in both the public and private sectors, though that distinction has

* Managing Editor, GLTR; Georgetown Law, J.D. expected 2017; Duke University, B.A. 2014. This piece is adapted from a memorandum I wrote as a summer clerk at the Electronic Privacy Information Center. A description of EPIC's work on algorithmic transparency, and a compilation of related resources, can be found at https://epic.org/algorithmic-transparency/.

[1] Meg Leta Ambrose, *Lessons from the Avalanche of Numbers: Big Data in Historical Perspective*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 201 (2015); 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).

[2] Crawford & Schultz, *supra* note 1, at 96.

[3] *Id.*

[4] *Id.*

become increasingly permeable.[5] Data brokers, companies that create and sell detailed profiles of consumers for profit, sell their products to private and public entities alike, and often do not have data quality control clauses in the contracts governing those interactions.[6] These profiles also often refer directly or indirectly to sensitive attributes, such as race, gender, age, and socioeconomic status.[7]

This brave new world of big data is no longer new. But the mechanics of the algorithms relying on that data, and the process by which decisions are made using that information, merits a sharpened focus. Algorithmic decision-making is increasingly replacing existing practices in both the public and private sector, making an understanding of the technical construction of those algorithms increasingly crucial. This is all the more true for processes in which the consumer or citizen does not have a voice, and the logic behind the decision is fundamentally opaque.[8] It is difficult, if not impossible, for that consumer or citizen to challenge an adverse decision made about her when the basis for the decision is unavailable. In the private sector, automated predictions are used to calculate loan rates, credit scores, insurance risk, employment evaluations, and in hiring searches.[9] In the public sector,[10] they are being used for risk prediction

---

[5] Victoria Schwartz, *Overcoming the Public-Private Divide in Privacy Analogies*, 67 HASTINGS L.J. 143, 189 (2015), at 149 n.31 (overview of literature examining the degradation of the public-private sector divide).

[6] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, 16 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (noting the contracts between data brokers and their sources rarely address the accuracy of the provided information).

[7] *Id.*

[8] Jenna Burrell, *How The Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, BIG DATA & SOC'Y, Jan. 2016, at 5, http://bds.sagepub.com/content/spbds/3/1/2053951715622512.full.pdf.

[9] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, (2016); Rick Swedloff, *Risk Classification's Big Data (r)evolution*, 21 CONN. INS. L.J. 339 (2015); Frank Pasquale, *We're Being Stigmatized by 'Big Data Scores We Don't Even Know About*, LA TIMES, (Jan. 15, 2016), http://www.latimes.com/opinion/op-ed/la-oe-0116-pasquale-reputation-repair-digital-history-20150116-story.html.

[10] *See generally*, Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES IN L. 2 , (forthcoming 2016), http://ssrn.com/abstract=2714072; *Id*, at 13 ("In an era when decisionmaking is mediated comprehensively by so-called "big data," regulators will have to contend with the methods by which regulated decisions are reached — i.e., with the algorithm as an instrumentality for conducting (regulated) activity").

in law enforcement,[11] as well as for sentencing,[12] and to calculate benefits.[13] Further, there is a pervasive and misguided belief in the inherent neutrality of algorithmic decision-making by virtue of its empiricism. But data is not inherently neutral, and neither are the algorithms that process it. Each is the product of the beliefs, fallibilities, and biases of the person who created them. If those fallibilities are unaccounted for, algorithms will simply replicate the pre-existing inequalities encoded in their intake data and structure. This memorandum will provide an overview on the basics of algorithms and data mining, and explore how automated decision-making can unintentionally reveal sensitive information, or unintentionally base their predictions on protected traits, implicating individual privacy and civil liberties.

UNDERSTANDING THE BASICS

To understand how the particular features of an algorithm can violate individual privacy, or lead to discriminatory outcomes, it is necessary to understand the discrete steps of how algorithms work. An algorithm can be defined as "simply a series of steps undertaken in order to solve a particular problem or accomplish a defined outcome."[14] In the context of big data, that means a computational process that takes input data and creates an output based on a rule.[15] A machine-learning algorithm involves two distinct processes: a classifier algorithm, and a learner algorithm.[16] A classifier algorithm performs a mathematical function on a given set of input data, and creates a category based on the relationships between different properties ('features' of the data) as an output. An example would be a classifying algorithm that takes a list of emails with multiple features, such as sender, time sent, or presence of an attachment, and sorts them by sender ("from Bob" or "not from Bob"). The learner algorithm will establish the relationships between a set of features in

---

[11] Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion,* 62 EMORY L.J. 259, 273 (2012).

[12] Sonja B. Starr, *Evidence-Based Sentencing And The Scientific Rationalization Of Discrimination,* 66 STAN L. REV. 803 (2014) (discussing the use of risk prediction algorithms in sentencing and bail determinations).

[13] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1510 (2013) (discussing the use of predictive models in IRS audit selections).

[14] Nick Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, TOW CTR. FOR DIGITAL JOURNALISM, 4, (2013), http://www.nickdiakopoulos.com/wp-content/uploads/2011/07/Algorithmic-Accountability-Reporting_final.pdf.

[15] *Id.*

[16] Burrell, *supra* note 8, at 3.

training data, and prospectively apply that rule to new inputs.[17] Commonly used machine-learning models include neural networks, decision trees, Naïve Bayes, and logistic regression.[18] The choice of model depends on the particular use, such as an algorithm designed to predict creditworthiness, as opposed to an algorithm designed to predict the likelihood of crime in a given area, and different models can be used separately, or in conjunction with one another.[19] A prioritization algorithm, as the name might suggest, ranks an input by virtue of possession or lack of certain attributes, and is primarily used in processes that assess risk. Examples include recidivism algorithms used by judges in sentencing, or algorithms that assess insurance risk.[20]

PRIVACY IMPLICATIONS IN DATA MINING

The very value of data analytics lies with is its ability to elicit subtle and insightful relationships between various data features, such as, oddly enough, an increase in Pop-Tart purchases before hurricanes.[21] That seemingly oracular ability to illustrate connections between otherwise random attributes is both what make big data so useful, and what leads to its piercing ability to reveal private information. It can elicit inferences an individual did not want to know, or might not want anyone else to know, such as a medical condition.[22] It can also draw relationships between legally protected and unprotected categories, and base decisions off of those correlations.[23] Even when the information is not legally protected or inherently sensitive, there are concerns that increasingly precise determinations could be used to create inscrutably complex portraits of consumers, in a way that could further diminish consumer control.[24] Privacy violations and discriminatory outcomes are a predictable consequence of data analytics' ability to elucidate unexpected information. While distinct concepts, privacy and civil rights often overlap when the private information is deeply

[17] *Id*. at 5.
[18] *Id*.
[19] *Id.* at 5.
[20] Starr, *supra* note 12, at 825.
[21] Andrej Zwitter, *Big Data Ethics*, BIG DATA & SOC'Y, Nov. 2014, at 4, http://bds.sagepub.com/content/spbds/1/2/2053951714559253.full.pdf.
[22] Crawford & Schultz, *supra* note 1, at 97 (discussing how a health condition can be inferred from data on consumer habits).
[23] Barocas & Selbst, *supra* note 9.
[24] Solon Barocas, *Data Mining and the Discourse on Discrimination*, CTR. FOR INFO. TECH. POL'Y (2014), 2, https://dataethics.github.io/proceedings/DataMiningandtheDiscourseOnDiscrimination.pdf.

connected to a fundamental right, or a protected attribute, such as political affiliation, immigration status, or a disability.

DISCRIMINATION IN DATA MINING

Algorithms can be intrinsically (and unintentionally) discriminatory through the population of data selected, how the algorithm functions, and the data itself. For example, when the training data for a predictive policing algorithm assigning the probability of crime to an area uses crime statistics from police stops in 1956 Chattanooga, the algorithm will learn—and replicate— a correlation between arrest rates and race. Data does not simply occur; it is created, and will reflect the flaws of its creator, as will any rule predicated on the relationships between various attributes in that data.[25]As a matter of technique, machine learning is also less accurate, and thus roughly less effective, for minority groups. There is proportionately less data available for majority groups by definition, and correlations that may be correct for the majority may be completely incorrect for the minority.[26] In an excellent piece illustrating the fallacy of inherently neutral data mining, Moritz Hardt uses the example of a machine learning algorithm distinguishing between real and fake names.[27] A short and common name might be real in one culture, and fake in another; if the classifier discerns a negative correlation between real names and complex or long ones, it will be inaccurate in applying that rule to minority groups. [28] Certain attributes can also serve as proxies for sensitive attributes, such as race, or socioeconomic status. Uber, for example, was accused of redlining by directing drivers away from majority-black neighborhoods.[29] Inference of membership in a protected class; statistical bias skewing the function of the algorithm; and faulty inferences based on mistaken or acontextual data can each serve the render the results of an algorithm discriminatory, or violate an individual's privacy.[30]

---

[25] JONATHAN STRAY, THE CURIOUS JOURNALIST'S GUIDE TO DATA 7, (2016) https://www.gitbook.com/book/towcenter/curious-journalist-s-guide-to-data/details.
[26] Moritz Hardt, *How Big Data Is Unfair*, MEDIUM, (September 6, 2014), https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de#.asxzmuhfg.
[27] *Id.*
[28] *Id.*
[29]Jennifer Stark & Nicholas Diakopoulos, *Uber Seems to Offer Better Service In Areas With More White People. That Raises Some Tough Questions,* WASH. POST (Mar. 1, 2016), https://www.washingtonpost.com/news/wonk/wp/2016/03/10/uber-seems-to-offer-better-service-in-areas-with-more-white-people-that-raises-some-tough-questions/.
[30] Barocas, *supra* note 24.

The problems big data poses for privacy and civil rights are manifold and complex. Though the work ahead is considerable, technologists and legal scholars have begun exploring relevant techniques to better guard against discrimination and protect individual privacy. Computer scientists in public policy like Latanya Sweeney,[31] Cynthia Dwork,[32] Helen Nissenbaum[33] and Moritz Hardt[34] have shed light on the fallacy of inherently neutral data mining through research on techniques to combat discrimination, and protect privacy. These technical approaches include both discrimination-blind, as well as discrimination-aware data mining,[35] privacy-aware data mining,[36] and differential privacy.[37] Legal scholars have also begun to delve deeply into how the mechanics of data mining, and the myth of its assumed neutrality, often undermines the assumptions predicating existing laws.[38] The Federal Trade Commission's Big Data report summarized relevant questions for engineers working with large data sets and trying to ascertain the risk of privacy violations

[31] Latanya Sweeney, *Discrimination in Online Ad Delivery*, DATA PRIVACY LAB (2013), http://dataprivacylab.org/projects/onlineads/1071-1.pdf.
[32] Cynthia Dwork, *Differential Privacy: A Survey of Results*, THEORY & APPLICATIONS OF MODELS OF COMPUTATION 1, 19, (2008), https://www.researchgate.net/profile/Minzhu_Xie2/publication/220908334_A_Practical_Parameterized_Algorithm_for_the_Individual_Haplotyping_Problem_MLF/links/0deec5328063473edc000000.pdf#page=12.
[33] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS 4, 32-48 (2011), http://ssrn.com/abstract=2567042.
[34] Ilias Diakonikolas, Moritz Hardt, & Ludwig Schmidt, *Differentially Private Learning Of Structured Discrete Distributions, in* ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 2566-2574, (2015).
[35] Cynthia Dwork et. al., *Fairness Through Awareness*, ARXIV, (Nov. 2011), https://arxiv.org/abs/1104.3913. (Proposing a framework for fair classification comprising (1), a (hypothetical) task-specific metric for determining the degree to which individuals are similar with respect to the classification task at hand; and (2), an algorithm for maximizing utility subject to the fairness constraint, such that similar individuals are treated similarly).
[36] Sara Hajian & Josep Domingo-Ferrer, *A Methodology for Direct and Indirect Discrimination Prevention in Data Mining*, IEEE TRANSACTIONS ON KNOWLEDGE & DATA ENG'G 25, no. 7 (May 21, 2013) (Proposing a pre-processing discrimination prevention framework to prevent direct discrimination, indirect discrimination, or both, with the objective of a fair tradeoff between discrimination removal and data quality).
[37] Moritz Hardt, Katrina Ligett, & Frank McSherry, *A Simple and Practical Algorithm for Differentially Private Data Release*, http://www.moritzhardt.com/papers/mwem.pdf.
[38] Citron, *supra* note 13; Barocas & Selbst, *supra* note 9.

or inherent discrimination, such as whether a relevant model accounts for biases, and closely the dataset mirrors the population being measured. [39]

Ultimately, preliminary research is exactly that—preliminary. It does not answer all the tough questions raised by the use of big data, and how automated decision-making challenges existing legal frameworks designed to protect privacy and civil liberties. While understanding the mechanics of algorithmic decision-making is fundamentally necessary to prevent violations of privacy and civil liberties from simply being ignored, it is only the first step towards preventing them. At the very least, it is a start.

[39] FED. TRADE COMM'N,, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; ("How representative is your data set?...Does your data model account for biases?...How accurate are your predictions based on big data?...Does your reliance on big data raise ethical or fairness concerns?").

ASYLUM SEEKERS IN THE UK GAIN CYBER-ADVOCATE

Deena Dulgerian*

CITE AS: 1 GEO. L. TECH. REV. 160 (2016)
http://bit.ly/2fGq9jf

INTRODUCTION

> "We are not a law firm or a substitute for an attorney or law firm. We cannot provide any kind of advice, explanation, opinion, or recommendation about possible legal rights, remedies, defenses, options, selection of forms or strategies."[1]

When machines take the place of persons in providing certain services, what is considered a marketable skill for the human service provider changes. With many fearing inevitable doom, even the value of highly skilled, white collar professionals is called into question.

Some in the legal field believe this fear to be the fatal flaw in the legal profession's general attitude towards technology, that it hampers the potential of the industry in the United States.[2] Legal Zoom's disclaimer above provides an appropriate reminder of the limits of machine-based services. It illustrates how the industry of online legal assistance will create efficiency in the provision of legal services, but as a supplement to, not a replacement of, attorneys.

Joshua Browder, founder and creator of donotpay.co.uk, is not out to turn the legal world upside down, merely to turn it right side up. The DoNotPay ("DNP") website is powered by software to help individuals appeal parking tickets at a quicker pace, without further assistance.

---

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; University of California Los Angeles, B.A. 2012.

[1] LEGAL ZOOM, http://bit.ly/2dElOzP (last visited Oct. 9, 2016).

[2] Ed Sohn, *alt.legal: If We Build It, Will They Come? The Problem of Legal Tech Adoption*, ABOVE THE LAW (Sept. 14, 2016, 7:25 PM), http://abovethelaw.com/2016/09/alt-legal-if-we-build-it-will-they-come-the-problem-of-legal-tech-adoption/?rf=1.

DNP is accessible to users in the United Kingdom, New York, and Seattle. Since Fall 2015, it has successfully overturned $4 million worth of tickets.[3] While anyone can use the website, it is an especially valuable service for individuals who cannot navigate, or afford to navigate, the arduous and frustrating bureaucracy of their local parking enforcement. Browder has replicated DNP's framework to create software that assists individuals in seeking housing aid and assistance in the United Kingdom; travelers in receiving compensation for delayed flights; customers in requesting credit for bank overage charges; and HIV-positive individuals in retaining a digital ledger of their disclosure to a partner for legal purposes.[4]

The technology behind DNP has been in use for years, but it is the idea behind what Browder calls an "asylum bot" that sets him apart from other coding engineers and start-ups. A bot refers to certain type of software that automates tasks such as placing orders, making reservations, or filling out forms.[5] The most commonly used bots function in the form of a chat bot which mimics human-to-human conversation to complete such tasks.[6] The asylum software would assist individuals seeking asylum in the United Kingdom to fill out their asylum applications.[7] The asylum software is currently in production and was set for a controlled trial run in September 2016.[8] Its potential demonstrates a possible future of bots and software in the legal field. In order to understand that future, however, it is important to understand the technological and legal background that makes this software useful.

THE TECHNOLOGY BEHIND THE DNP

In their simplest forms, software similar to DNP is used to provide answers to frequently asked questions and services, such as ordering pizza through Domino's Pizza bot "Dom" via a request in text form. An example in the legal world is Bloomberg Law's Draft Analyzer tool, Exemplify.[9]

---

[3] *This robot lawyer could help you get your parking ticket dismissed*, CBS NEWS (July 21, 2016, 8:05 AM), http://www.cbsnews.com/news/donotpay-bot-lawyer-helps-dismiss-parking-tickets-joshua-browder/.

[4] Telephone Interview with Joshua Browder, Founder, DoNotPay (Sept. 16, 2016).

[5] *See* Kurt Wagner, *Bots, explained*, RECODE (Apr. 11, 2016, 5:00 AM), http://www.recode.net/2016/4/11/11586022/what-are-bots.

[6] *See* Amir Shevat, *To bot or not to bot*, VENTURE BEAT (Apr. 29, 2016, 5:05 PM), http://venturebeat.com/2016/04/29/to-bot-or-not-to-bot/.

[7] Telephone Interview with Joshua Browder, *supra* note 4.

[8] *Id*.

[9] *Draft Analyzer*, BLOOMBERG LAW, http://www.bna.com/draft-analyzer/ (last visited Oct. 9, 2016).

Exemplify stores thousands of contracts for various transactions collected from Bloomberg's own database and the Securities and Exchange Commission's (SEC) EDGAR database. EDGAR collects various filings submitted by companies in accordance with SEC requirements.[10] Exemplify allows attorneys not only to compare standard language between law firms, but to add specific terms in templates created from sample contracts.

The technology behind DNP goes beyond the word comparison functionality of the Bloomberg software. Primarily, DNP acts as a legal translator. Individuals add the necessary information, such as where the parking ticket was issued, their driver information, and details of the surrounding area for context. When an individual describes their situation, most do so in plain (and often ambiguous) language. This plain language is then translated by a natural language processor into precise legal terms.[11] For example, DNP has been taught to interpret "I couldn't see the sign" as "the parking sign was not visible to the reasonable driver, and therefore the warning was insufficient," or something similar. With every subsequent answer, the software proceeds down a different plausible path on a decision tree to find the strongest grounding for an appeal.[12] Each of these plausible paths on the decision tree were collected by Browder's team through an analysis of data retrieved via requests through the United State's and United Kingdom's respective Freedom of Information Acts ("FOIA").[13] The most successful rationales, as determined by the FOIA data analysis, are used as the backbone for an appeal. After the information for the appeal is collected, the appeal itself is prepared.

The appeal is then communicated to the parking authority. Due to the fact that DNP and the parking authority were not created by the same individual or company, they likely operate different systems and thus need a "common boundary" to communicate.[14] DNP uses an application program interface ("API") to communicate with the parking authority. An API serves as a middleman between an individual and an application, similar to a waiter in a restaurant who communicates a customer's order to the kitchen. An API (waiter) presents individuals with a list of options (the menu) they can request.

---

[10] *Id.*

[11] Natural language is the everyday spoken and written words humans use. The processing is what an application will do to understand and analyze natural language. *See* Peng Lai "Perry" Li, *Natural Language Processing*, 1 GEO. L. TECH. REV. 98 (2016).

[12] That process can be compared to the quizzes found in lifestyle magazines: "Do you wear white at least once a week? If yes, go to question 4. If no, go to question 10."

[13] Telephone Interview, *supra* note 4.

[14] Michael Patterson, *What Is an API, and Why does It Matter?*, SPROUT SOCIAL (Apr. 3, 2015), http://sproutsocial.com/insights/what-is-an-api/.

The API (waiter) takes down an individuals' request and is the medium by which the order is delivered to the opposing software that processes the information (the kitchen). In this analogy, the kitchen responds by preparing the meal based on the order and the waiter delivers the meal back to the customer. Similarly, an API accepts an individual's request and returns the relevant data or final product (in the case of the DNP, the appeal).[15]

While the technology behind DNP forms the backbone of the asylum software, the issues that the asylum software handles are considerably different. The Syrian refugee crisis in the last few years has changed the demographics of many countries accepting refugees or asylum seekers. The biggest roadblocks in the asylum process are understanding another country's legal system, translating a different language, and affording the necessary legal representation. The asylum software seeks to alleviate these issues. In order to understand its capabilities and scope, it is important to understand the basic and different asylum processes in the United Kingdom and in the United States.

IMMIGRATION LAW IN THE UNITED STATES AND THE UNITED KINGDOM

When a refugee in the United States first applies for asylum, they are scheduled for an interview with an asylum officer who determines whether or not to grant asylum. The officer bases their decision on a 30-60-minute interview that gauges the refugee's credible fear of persecution. If the officer cannot approve asylum at this first stage, the refugee is referred to appear before an immigration judge in the Executive Office for Immigration Review (EOIR). At this stage, a refugee would strongly benefit from an immigration attorney, but many cannot afford one. The fact-finding process under EOIR differs from regular court proceedings, as immigration judges are Article I judges operating under the Department of Justice. This means that the proceedings do not follow the Federal Rules of Evidence and that judges are not bound by case law precedent.[16] The fact-finding process, therefore, depends more on the judge's discretion and not necessarily the legal standing and facts, making the chances of success very slim, even with an attorney.

---

[15] *Id.*

[16] *See* Karen T. Grisez, *The ABCs of Representing Unaccompanied Children in Removal Proceedings*, AM. BAR ASS'N, 30 (2008), http://www.americanbar.org/content/dam/aba/administrative/immigration/UACBasicsImmCtOct2014.authcheckdam.pdf.

In 2015, 69,933 refugees entered the United States.[17] Of the 84,182 applications filed (taking into consideration that refugees have one year to file an application so some of those who filed entered the United States in 2014), the U.S. Citizenship and Immigration Services Asylum Division managed to process only 40,062.[18] Of the 40,062 applications, 15,999 or 39% were granted asylum by the asylum officer and 17,943 were referred to an immigration judge.[19] Of the applications referred to an immigration, usually less than half are successful.[20]

The asylum process in the United Kingdom is somewhat similar. The first step for a refugee is to submit an application. The applicant must meet certain criteria, such as an inability to return to the home country and persecution for an enumerated set of reasons.[21] As long as the applicant meets the criteria and does not pose a national security threat as determined by the Home Office (the equivalent of the Department of State in the U.S.), they are granted asylum and possibly housing and health benefits. If the application is denied, then the refugee proceeds in front of a judge. Although it is unclear how many refugees entered the United Kingdom in 2015, about 25,711[22]–38,900[23] people applied for asylum. Of these, about 35% were granted asylum[24] and

[17] *FY15 Refugee Admissions Statistics*, U.S. DEP'T OF STATE, http://www.state.gov/j/prm/releases/statistics/251285.htm (last visited Oct. 9, 2016).
[18] *Affirmative Asylum Application Statistics and Decisions Annual Report*, DEP'T OF HOMELAND SEC. 3, (2016) https://www.dhs.gov/sites/default/files/publications/U.S.%20Citizenship%20and%20Immigration%20Services%20-%20Affirmative%20Asylum%20Application%20Statistics%20and%20Decisions%20Annual%20Report%20-%20FY%202016.pdf.
[19] *Id.*
[20] In 2014, 48% (8,775) were successful. DEP'T OF HOMELAND SEC., OFFICE OF IMMIGRATION STATISTICS, ANNUAL FLOW REPORT: REFUGEES AND ASYLEES: 2014 (Apr. 2016), https://www.dhs.gov/sites/default/files/publications/Refugees%20%26%20Asylees%20Flow%20Report%202014_508.pdf.
[21] *Claim asylum in the UK*, GOV.UK, https://www.gov.uk/claim-asylum/eligibility (last visited Oct. 9, 2016).
[22] *National Statistics, Asylum*, GOV.UK (Aug. 27, 2015), https://www.gov.uk/government/publications/immigration-statistics-april-to-june-2015/asylum#asylum-appeals.
[23] *Asylum Seekers in Europe* 2, REFUGEE COUNCIL (May 2016), http://www.refugeecouncil.org.uk/assets/0003/7727/Asylum_in_Europe_May_2016.pdf.
[24] *Asylum statistics Annual Trends* 2, REFUGEE COUNCIL (Aug. 2016), http://www.refugeecouncil.org.uk/assets/0003/8738/Asylum_Statistics_Annual_Trends_August_2016.pdf.

about 65% were referred to an immigration judge.[25] Of these appeals, only 30% were successful.[26]

It is important to note that the statistics are impacted by certain realities. Given the dangerous and clandestine ways refugees may enter a country, many go unaccounted for. Additionally, refugees who enter in one year may not file applications in that fiscal year which creates a gap between the number of refugees who enter a country in a year and the number of refugees who apply for asylum in that year. Administrative delays also affect the statistics; applications that are denied or granted may not be representative of refugees who either entered the country that same fiscal year or filed applications that fiscal year.

In the United Kingdom, the asylum software handles the initial application process, with a focus on basic access to justice. Browder and his team claim that refugees are accepted into the United Kingdom and granted asylum in the initial application phase at a higher rate than in the United States.[27] This is one of many possible reasons why a software that streamlines document production and form processing for refugees has a greater capacity to make a difference in the United Kingdom. As long as an individual meets the criteria[28], asylum is granted. As discussed, however, the actual rate at which each country accepts refugees and grants asylum is not divergent enough to attribute the greater feasibility of the asylum software in the United Kingdom, as opposed to the United States, to its asylum process or policies. It is likely that the expected success of the asylum software hinges on a factor external to the legal issues, possibly the United Kingdom's government's and British society's perspective on refugees and asylum.

The current version of the asylum software is designed for Syrian refugees: it translates from Arabic into English, and British charities that work with Syrian refugees assisted in the trial run. Syrian refugees, however, have the highest rate of asylum-approval in the United Kingdom out of the various nationalities that apply; about 86% of Syrians who apply are granted asylum.[29]

---

[25] *National Statistics, Asylum*, *supra* note 20; *see also Migration to the UK: Asylum*, THE MIGRATION OBSERVATORY (July 20, 2016), http://www.migrationobservatory.ox.ac.uk/resources/briefings/migration-to-the-uk-asylum/ (stating that 70-86% of applicants that were rejected filed an appeal and of those, 28% were granted asylum, 65% dismissed, and 7% withdrawn).

[26] *National Statistics, Asylum*, *supra* note 22.

[27] Telephone Interview, *supra* note 4.

[28] *Claim asylum in the UK*, *supra* note 21.

[29] *Compare Asylum statistics Annual Trends*, *supra* note 24 (stating 86%), with *National Statistics, Asylum*, *supra* note 22 (stating 87%). While there are a certain number of applications submitted, not all of them are reviewed. This fact slightly affects the statistic.

This could be due to a combination of the exigent circumstances in Syria and the recent upsurge in placing Syrians in stable homes. The asylum software could also be built to assist individuals from countries such as Pakistan who have a high rate of application but low rate of approval.[30] Of course, each country has its policy reasons for directing attention to one group of immigrants over another; this may require Browder to make certain strategic decisions in creating and making his website accessible in certain countries.

TECHNOLOGY OF THE ASYLUM SOFTWARE

Due to the complexities of immigration law, the asylum software operates under a more complex framework than the DNP software. Whereas the DNP software had to translate layman's English to English legalese, the asylum process involves a more challenging initial step: the translation from Arabic (the language most of the refugees speak) to English, not only literally, but structurally and relationally.[31] Translating the tragic story of a single mother's escape from religious persecution at the hands of a tyrannical ruler is a different feat than translating the basic transcript of how one received a parking ticket. To tackle this, the asylum software will be operating on IBM's Watson platform, which is a question answering computer system.[32] Unlike the natural language processing used in Browder's other software that take natural English and match it with the appropriate legalese, Watson goes above and beyond. It not only translates the Arabic into English, but it also closes the gap of what is lost in translation. Watson is able to understand the context of the Arabic text without being limited to only what is written. It does this by consuming enormous amounts of information and then undergoing manual programming through a series of questions that teach it how to interpret intent and draw inferences, just as a human does.[33]

Watson also incorporates machine learning into its API. Machine learning is a method of pattern recognition and trial-and-error which allows

---

[30] *Asylum statistics Annual Trends*, *supra* note 24, at 3 ("…among countries with relatively large numbers of applicants, Pakistan…had well above average refusal rates."); *see also National Statistics, Asylum*, *supra* note 22.

[31] *Id.*

[32] Recall when Ken Jennings, the Jeopardy! contestant who won 74 games in a row but was defeated after losing to a computer—that was Watson.

[33] Johnathan Cohn, *The Robot Will See You Now*, THE ATLANTIC (Mar. 2013), http://www.theatlantic.com/magazine/archive/2013/03/the-robot-will-see-you-now/309216/ (discussing Watson's capabilities to process up to 60 million pages of text per second of natural language).

computers to gain understanding without information being manually programmed by a human. This method, called feature selection, describes when a software algorithm (a set of instructions) parses data and selects only the information that is relevant to creating the final product.[34] Each time Watson learns new information from an asylum seeker's application, such as the name of a town the applicant is from or fled to, or the dates of bombings that displaced multiple families, it stores that information because it is relevant to building an asylum application.[35] Watson can then refer to that information when it needs to understand the details of a subsequent application. The more stories and (successful) applications Watson ingests, the more relevant, stronger, and quicker its subsequent responses and applications will be.

LEGAL TECHNOLOGY IN THE UNITED STATES

Browder's software and other technology that streamlines administrative legal tasks have been a source of fear for many attorneys.[36] While our society is accustomed to machine-led labor, it has mostly been in the context of manufacturing and customer service.[37] Attorneys, however, develop creative arguments and engage with other legal practitioners such as judges. This makes an attorney's role more interactive, less formulaic, and thus more necessary in a complex adversarial proceeding. Bureaucratic processes, however, such as parking tickets, reimbursements, and now initial applications for asylum in the United Kingdom, are less reliant on creative legal arguments and more about the logistics of meeting certain criteria. Browder's software alleviates an administrative legal task that is a burden for a majority of individuals whose only brush with the law is minimal in scope but impactful to

---

[34] *See* Jason Brownlee, *An Introduction to Feature Selection*, MACHINE LEARNING MASTERY (Oct. 6, 2014), http://machinelearningmastery.com/an-introduction-to-feature-selection/.

[35] Rob Schapire, *COS 511: Theoretical Machine Learning- Lecture #1*, PRINCETON (2008), http://www.cs.princeton.edu/courses/archive/spr08/cos511/scribe_notes/0204.pdf ("So in general, machine learning is about learning to do better in the future based on what was experienced in the past.").

[36] *Joshua Browder on Bots That Fight Bureaucracy* (Sept. 15, 2016), https://soundcloud.com/oreilly-radar/joshua-browder-on-bots-that-fight-bureaucracy; *see also How to Kill an Hour: How Not to Pay Parking Tickets!! w/ Joshua Browder* (Sept. 15, 2015) (downloaded using iTunes).

[37] Alex Debecker, *Chatbots are revolutionizing customer support*, VENTURE BEAT (Sept. 5, 2016, 12:10 PM), http://venturebeat.com/2016/09/05/the-chatbot-revolution-in-customer-support/; *see also* Michael Schneider, *Bots, Messenger and the future of customer service*, TECHCRUNCH (May 7, 2016), https://techcrunch.com/2016/05/07/bots-messenger-and-the-future-of-customer-service/.

their lives. The technology does not threaten the crux of the legal profession and does not decrease the value of human legal representation.

Some argue, however, that even alleviating a burden requires regulation and compliance with the same Model Rules of Professional Conduct that govern attorneys. Fixed, an application ("app") in the United States that worked similarly to Browder's DNP software, was suspected of violating ethics rules in 2015.[38] The app, which appealed parking tickets, was met with criticisms that the humans behind it—non-attorneys who were experts in parking regulations—were operating as attorneys, a violation of the law. These experts served as a set of analytical eyes and reviewed the substance of an appeal letter before it was mailed in.[39]

For areas of the law that require little legal expertise, such as traffic violations, DNP is sufficient. An attorney's skills, however, are more of a necessity for issues and areas of the law that truly require knowledge, insight, and guile. For example, because immigration judges in the United States are not bound by precedent, their discretionary decisions are more easily influenced by argumentative orations and appeals to emotions. With a decrease in the amount of applicants granted asylum after their initial interview and an increase in the amount of referrals to immigration courts, the importance of an attorney in the courtroom is only expected to increase.[40] The courtroom presentation of computer-made appeal is akin to reading *Macbeth* in English class, whereas zealous human advocacy is akin to watching Ian McKellen play Macbeth at the Royal Shakespeare Company.[41]

Technology that streamlines bureaucratic processes and molds to the idiosyncrasies of the applicable law should be viewed as alleviating a burden rather than an existential threat. Attorneys may take advantage of the software for small profit.[42] For example, adopting such software into an immigration

---

[38] Mark Wilson, *New App Fights Parking Tickets for You, but It's 'Not an Attorney,'* FIND LAW (July 28, 2014, 5:57 AM), http://blogs.findlaw.com/technologist/2014/07/new-app-fights-parking-tickets-for-you-but-its-not-an-attorney.html; *see also* Martha Neil, *Law firm with tech expertise has acquired 'Fixed' ticket-fighting app,* ABA J. (Jun. 15, 2016, 4:48 PM), http://www.abajournal.com/news/article/law_firm_acquired_fixed_ticket_fighting_app.

[39] Heather Kelly, *New app helps you fight parking tickets,* CNN (Feb. 22, 2014, 2:22 PM), http://www.cnn.com/2014/02/20/tech/mobile/fixed-app-parking-tickets/.

[40] *Annual Report 2014*, DEP'T OF HOMELAND SEC., viii (2014), https://www.dhs.gov/sites/default/files/publications/cisomb-annual-report-2014.pdf.

[41] Patrick Foster, *Sir Ian McKellen: Don't bother reading Shakespeare*, THE TEL. (Oct. 27, 2015, 12:01 AM), http://www.telegraph.co.uk/news/celebritynews/11956151/Sir-Ian-McKellen-Dont-bother-reading-Shakespeare.html.

[42] Samuel Gibbs, *Chatbot lawyer overturns 160,000 parking tickets in London and New York*, THE GUARDIAN (June 16, 2016, 6:07 AM),

firm's website could offer asylum services at a reduced price because there would be minimal maintenance and labor costs. Whether incorporating software into firm practice establishes an attorney-client privilege would depend on how involved humans would be on the backend of the software (i.e., are attorneys reviewing each form before it is sent or merely maintaining or updating the software).

The pushback against Fixed demonstrates the obstacles that developers of legal technology face. By changing the narrative from "my job is at risk" to "this helps me do my job," the legal profession can ensure a better working relationship with the technology industry, and reduce the access to justice gap that prevents needy and indigent individuals from receiving legal redress. Whether the asylum software launches in the United States remains to be seen, but it is likely that software such as DNP will soon become commonplace in the legal field.

https://www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york; *see also* Telephone Interview, *supra* note 4.

HEALTHCARE BEGINS A MOBILE REVOLUTION

Michelle M. Ovanesian*

CITE AS: 1 GEO. L. TECH. REV. 170 (2016)
http://bit.ly/2gFASwA

Healthcare is in the midst of a mobile revolution, and it will only be a matter of time before mobile healthcare applications ("apps") change how we deliver, consume, measure, and pay for healthcare.[1] The rapid pace of innovation and broad applicability of mobile healthcare applications have fueled this revolution. The healthcare mobile app market, currently estimated to be worth $4 billion, is expected to increase to $26 billion by 2017.[2]

In doctors' offices and hospitals, smartphones already are replacing stethoscopes and pagers as the most widely-used physician accessory.[3] Some federal agencies even have entire programs focused on the development and promotion of medical apps.[4] For example, the U.S. Department of Defense established a National Center for Telehealth and Technology evaluates mental health technologies for military personnel.[5] The program includes various smartphone apps, such as one that helps physicians diagnose and treat traumatic brain injuries and mental disorders by enabling users to track their emotional experiences over a certain period of time.[6] Ranging from the automation of simple tasks for healthcare providers to patient-specific analysis and diagnosis

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Georgetown University, M.S. (2013); University of California, Berkeley (2011).
[1] Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1190 (2014).
[2] Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals To Protect Health and Fitness Data At Work*, 16 YALE J. HEALTH POL'Y, L. & ETHICS 1, 9 (2016).
[3] Cortez, *supra* note 1, at 1177.
[4] *Id*. at 1214.
[5] *Id*. at 1215.
[6] *See id*.; *see also Smartphone Resiliency Apps*, U.S. ARMY (Feb. 28, 2013), https://www.army.mil/article/97390.

for consumers, mobile healthcare apps present numerous potential benefits and risks to consumers.[78]

Potential benefits include the reduction of medical errors, improvement of quality care, and prevention of more serious episodes of illness.[9] Mobile healthcare apps may also benefit consumers by shifting the locus of effective care away from medical facilities and professionals and toward digitally-empowered patients.[10] However, potential risks may outweigh the benefits and are greater for the poor, uninsured, and underinsured who may use an app lacking in clinical evidence for self-diagnosis and treatment rather than pay for a doctor's visit. The risks can range from relatively benign, such as an app claiming to relieve tooth pain that is actually clinically ineffective, to severe, such as an app storing personal health information that is hacked.

Today, a muddled assortment of different agencies—including the Food and Drug Administration (FDA), the Federal Trade Commission (FTC), and the Federal Communications Commission (FCC)—and regulations are involved in regulating the potential risks that mobile healthcare apps pose.[11] Unfortunately,

---

[7] *See, e.g.*, K Royal & Gretchen A. Johnson, *Cybersecurity And Medical Devices: Reality Bytes*, 32 NO. 8 ACC DOCKET 66, 80 (2014). ("The US Center for Disease Control has a vaccine application (CDC Vaccine Schedules 4) that helps medical professionals determine immunization schedules for their patients. On the other side, for parents or patients, the Children's Hospital of Philadelphia has launched Vaccines on the Go, which appears to be more informational than a tracking tool. However, VaxNation (created by a team of Baylor College of Medicine, University of Texas School of Public Health and Rice University students) is an online vaccination tracker. Once you enter your vaccination history and date of birth, you will see the age appropriate recommendations based on the Centers for Disease Control and Prevention's guidelines. Families can create an account, link to social media accounts and receive reminders.").

[8] Cortez, *supra* note 1, at 1182-83. ("For example, applications now enable clinicians to use their smartphones to view and manipulate medical images, analyze electroencephalograms ("EEGs") or electrocardiograms ("ECGs"), connect to bedside monitors, screen blood samples, or act as wireless remote controls for medical devices. In this latter category, several applications allow users to control FDA-regulated devices. Examples include apps that allow users to inflate and deflate blood pressure cuffs, perform portable ultrasounds, operate insulin pumps, and visually track whether wounds heal or regress. Other apps also display, analyze, or transmit patient data from an FDA-regulated device. For example, one app allows clinicians to use their phones to track patients' vital signs remotely, pulling data "from hundreds of different types of patient monitors." A related app allows obstetricians to monitor patients' contractions, fetal heartbeats, and other realtime waveform data. Yet another allows cardiologists to review and manipulate ECG results and histories.").

[9] Cortez, *supra* note 1, at 1177; Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and The Regulation Of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 436 (2014).

[10] Cortez, *supra* note 1, at 1177.

[11] Flaherty, *supra* note 9, at 436; Cortez, *supra* note 1, at 1179.

most agencies "have adopted a posture of facilitating rather than regulating mobile health."[12]

For example, the FDA recently issued a non-binding guidance document delineating the types of apps that it will and will not regulate.[13] In the guidance document, the FDA clarifies that it will regulate those apps that meet the statutory definition of "device."[14] The term "device" means "an instrument, apparatus, implement, machine, contrivance, implant…..which is….intended to affect the structure or any function of the body of man or other animals."[15]

While some apps clearly do or do not meet the definition of "device," most apps lie in a "gray" area where FDA regulation is uncertain.[16] Thus, apps like Apple's Health App, which allows users to store and track all of their fitness and health data and even asks for information about sexual history and partners, fall into the "gray" area of unregulated apps.

Despite the scores of federal agencies and regulations overseeing mobile healthcare apps, no current law or regulation clearly protects the health data that apps might collect, and there are few restrictions on app developers as to the type of data they can collect and how they can monetize the data collected.[17]

For example, the FCC has the authority to enforce consumer information privacy provisions and establish regulations on consumer proprietary network information ("CPNI") or "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a

---

[12] Cortez, *supra* note 1, at 1211.

[13] *Id*. at 1203-04.

[14] *Id*.

[15] Cortez, *supra* note 1, at 1209-12; J. Wasserman and LaToya C. Sutton, *What's in This Stuff? An Update on FDA's Policies and Enforcement Actions Concerning Novel Ingredients in Food and Dietary Supplements*, FOOD SAFETY MAG. (June 12, 2016), http://www.foodsafetymagazine.com/magazine-archive1/junejuly2016/whate28099s-in-this-stuff-an-update-on-fdae28099s-policies-and-enforcement-actions-concerning-novel-ingredients-in-food-and-dietary-supplements/.

[16] Cortez, *supra* note 1, at 1209-12.

[17] Brown, *supra* note 2, at 24, 34; Flaherty, *supra* note 8, at 424. Some healthcare apps may fall under the Health Insurance Portability and Accountability Act. "To fall under HIPAA's scope, "protected health information" (PHI) must be communicated between covered entities, including "business associates." PHI includes individually identifiable health information, meaning information collected from an individual that either "identifies the individual" or reasonably "can be used to identify the individual." "Covered entities" include health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form. If an entity does not meet the definition of a covered entity or business associate, or does not transmit PHI, it need not comply with HIPAA's requirements."

telecommunications carrier."[18] Although the CPNI regulations seem to protect location information and to prevent telecommunications companies from marketing user information, they to do not apply to third party app developers and "there are no clear rules for the disclosure of this data and often no way for consumers to control the data they reveal" when a consumer uses an app that is separate from the telecommunications carrier.[19]

In addition to a lack of protective federal laws and regulations, many mobile healthcare apps lack transparent privacy policies, and it is unclear whether a consumer will be able to sue a developer for a privacy violation.[20]

As of now, a malicious acquaintance or employer may be able to legally use and indefinitely store, without your consent, the personal health information stored in an app in your phone.[21][22][23]

Smartphones are only becoming more and more commonplace, and the FDA estimates that 500 million smartphone users now use or will soon use at least one health care app.[24] The development of healthcare apps is progressing exponentially, but privacy regulations in this field have been left behind. A robust dialogue about privacy and mobile healthcare apps among universities, civic organizations, and citizens is needed. Additionally, federal interagency

---

[18] Flaherty, *supra* note 8, at 434-35.

[19] *Id.*

[20] Flaherty, *supra* note 8, at 437; Brown *supra* note 2, at 36. "If an app developer were to violate these terms, however, it is not clear that the consumer whose data were sold would have a right of action against either Apple or the developer. Consumers may be incidental beneficiaries of these terms, but it is unlikely that a court would find that they had standing to sue either a developer for failing to follow them or Apple for failing to insist on them."

[21] Brown, *supra* note 2, at 34. "The potential profit from collecting, analyzing, repackaging, and selling health-related data to employers and/or marketers is barely limited by law. As it stands, app and device makers can now access a wide range of users' health-related data without those users' consent."

[22] Flaherty, *supra* note 8, at 437. Analogizing to Fourth Amendment doctrine, one could cogently argue that people do not have a reasonable expectation of privacy if they voluntarily choose to input private, personal information on the Internet or on a smartphone. As the Supreme Court stated in *Katz v. United States*, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Thus there are reduced privacy protections when people input information into apps because they are essentially putting that information out into the public."

[23] *See also Smith v. Maryland*, 442 U.S. 735 (1979). "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

[24] Brown, *supra* note 2, at 9.

cooperation is necessary in order to provide consistent and meaningful regulatory oversight. Finally, at a minimum, app developers should be required to create accessible privacy policies, obtain informed consent to use consumers' information, and inform users of holes and breaches in app cybersecurity.

YOU KNOW IT WHEN YOU SEE IT: PUNISHMENTS FOR AND REGULATION AGAINST REVENGE PORN

Seth Teleky*

CITE AS: 1 GEO. L. TECH. REV. 175 (2016)
http://bit.ly/2gCqhF4

Widespread access to the Internet, multimedia messaging, and a myriad of other advances in communications technology over the past few decades have made it easier than ever to share information, but more difficult than ever to control information. The many positive results of this evolution, however, are marred by the ease with which it has enabled someone to distribute sexually intimate images or videos of another person online in an effort to mentally damage the other person, derail his or her career or relationships, and/or profit from the views of the image. This is commonly known in the law as "nonconsensual pornography" or "revenge porn."[1]

At first glance, revenge porn may seem to already be barred by existing law. The common law torts of intrusion on seclusion and public disclosure of private facts; copyright protections on photographs and videos; and statutes prohibiting the appropriation of another's identity all would appear to present a victim with avenues of redress. However, the fact that these images or videos are frequently recorded consensually and given freely to a partner makes prosecution under these laws difficult. Traditional privacy laws may also have further idiosyncratic loopholes. For example, until 2014, New York state law prohibited broadcasting images of a person engaged in sexual activity taken without that person's consent, but only if certain body parts were clearly identifiable.[2]

In response to this issue, at least thirty-four states and Washington, D.C. have passed laws aimed specifically at criminalizing revenge porn.[3] The fact that only eighteen states had such legislation in April 2015 indicates just how

---

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Tufts University, B.A. 2013.

[1] CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/about (last visited Sept. 30, 2016).

[2] Carrie Goldberg, *New York Does Not Have a Revenge Porn Law*, NYLS INNOVATION CTR. FOR L. & TECH. (Sept. 30, 2016), http://www.nyls.edu/innovation-center-for-law-and-technology/wp-content/uploads/sites/176/2013/07/Panel-3-Pt-1-NEW-YORK-DOES-NOT-HAVE-A-REVENGE-PORN-LAW.pdf.

[3] *Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ (last visited Sept. 30, 2016).

rapidly this area of law is developing.[4] This past September, another anti-revenge porn bill was introduced by a New York City Councilman in response to a similar bill stalling in the state legislature.[5]

These laws generally add a burden that sexual images must not only have been obtained consensually, but also have been distributed with the explicit consent of the subject.[6] Some, however, have attracted surprising opponents. Journalists have expressed concern about being prosecuted for sharing certain images (i.e. of prisoner abuse at Abu Ghraib) in the news media due to overbroad statutory language, and the ACLU sued Arizona over its version for precisely this reason.[7] To more narrowly target perpetrators, several of the laws now require intent to harass or financially profit from the distribution of the images.[8] Some feminist activists nonetheless protest that laws criminalizing revenge porn distract from related or underlying gender-based issues of stalking and domestic violence, which they believe are crimes in more dire need of legislative attention.[9]

Punishing offenders is only one part of the larger problem— jailing the perpetrator does not solve the problem of how to remove pictures once they have been disseminated. This step is crucial to ensuring that victims are able to resume their lives without the fear and embarrassment of having their most intimate moments a few clicks away by anyone who learns their name.

To stop revenge porn and restore victims' rights, social media companies, image-hosting websites, and Internet service providers must take down these images whenever they appear. This has proven to be a difficult tightrope to walk. Facebook employs software called "PhotoDNA" that attempts to recognize nudity and automatically remove it.[10] This software is often overzealous—the corporation's latest public relations snafu was its

---

[4] Claire Landsbaum, *New York City Moves to Crack Down on Revenge Porn*, N.Y. MAG. (Sept. 14, 2016), http://nymag.com/thecut/2016/09/new-york-city-lawmakers-crack-down-on-revenge-porn.html.

[5] *Id.*

[6] *See id*.

[7] Alex Ronan, *Could All These New Revenge-Porn Laws Actually Be a Bad Thing?*, N.Y. MAG., Apr. 16, 2016, http://nymag.com/thecut/2015/04/why-regulating-revenge-porn-is-so-tricky.html.

[8] *Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ (last visited Sept. 30, 2016).

[9] Sarah Jeong, *Revenge Porn Is Bad. Criminalizing It Is Worse.*, WIRED, (Oct. 28, 2013), https://www.wired.com/2013/10/why-criminalizing-revenge-porn-is-a-bad-idea/.

[10] Alfred Ng, *Facebook loses bid to dismiss teen's revenge porn lawsuit*, CNET (Sept. 13, 2016), https://www.cnet.com/news/facebook-loses-argument-to-dismiss-teens-lawsuit-over-revenge-porn/.

takedown of the famous "Napalm Girl" picture of a naked child crying during the Vietnam War that had been posted by the Norwegian Prime Minister.[11]

However, a British judge recently ruled that a case against Facebook for not doing enough to prevent its site being used to disseminate revenge porn could proceed to trial.[12] (Such legal action could not have been brought in an American court, as Section 230 of the Communications Decency Act largely shields Internet publishers from liability for content posted by the individuals who visit their sites.)[13] Though Facebook argues it should not be liable because it removed pornographic images of the minor who brought the suit upon notification of the post (apparently they went undetected by PhotoDNA), the plaintiff alleges it erred by not banning the group the images were posted in—a group explicitly dedicated to shaming women through posting such images—and that she should have had to only notify Facebook about each picture the first time it was posted, rather than each time it was reposted.[14] For the sake of victims everywhere, the court should compel Facebook and, by extent, similar social media companies to take more proactive measures.

---

[11] Mark Scott and Mike Isaac, *Facebook Restores Iconic Vietnam War Photo It Censored for Nudity*, N.Y. TIMES, (Sept. 9, 2016), http://www.nytimes.com/2016/09/10/technology/facebook-vietnam-war-photo-nudity.html.

[12] Colin Daileda, *Could a revenge porn case in Northern Ireland change Facebook across the planet?*, MASHABLE, (Sept. 29, 2016), http://mashable.com/2016/09/28/facebook-revenge-porn-lawsuit-ireland/#Bu194ymiQOqD.

[13] Sarah Jeong, *Revenge Porn Is Bad. Criminalizing It Is Worse.*, WIRED, (Oct. 28, 2013), https://www.wired.com/2013/10/why-criminalizing-revenge-porn-is-a-bad-idea/.

[14] *Id.*; Alfred Ng, *Facebook loses bid to dismiss teen's revenge porn lawsuit*, CNET (Sept. 13, 2016), https://www.cnet.com/news/facebook-loses-argument-to-dismiss-teens-lawsuit-over-revenge-porn/.

UNLOCKING THE BOX: HOW THE FCC IS REVAMPING THE CABLE INDUSTRY

Nicholas Festa*

CITE AS: 1 GEO. L. TECH. REV. 178 (2016)
http://bit.ly/2gdixsq

Despite the spate of articles on the rise of television cord cutting, 76 percent of Americans still subscribe to a multichannel video programming distributor ("MVPD")[1] at home.[2] Nearly all paid television subscribers lease a set-top box (also known as a cable box) from their television provider, at an average cost of $231 per year.[3] It is estimated that the cost of set-top boxes has increased 185 percent in the past 20 years.[4]

In response to these growing costs, Federal Communications Commission ("FCC") Chairman Tom Wheeler proposed a Notice of Proposed Rulemaking ("NPRM") on the issue of set-top box competition in January 2016.[5] The NPRM began in February, and the Commission was scheduled to consider a subsequent Report and Order on September 29, 2016, but this vote was delayed.[6]

The set-top box market in paid television is currently dominated by large-scale distributors, such as Comcast, Verizon, and Time Warner, as

---

* GTLR Staff Member; Georgetown Law, J.D. expected 2018. St. John's University, B.A. 2015.

[1] A television provider that provides a number of TV channels, e.g. satellite TV or cable TV. *Definition of: MPVD*, PCMAG, http://www.pcmag.com/encyclopedia/term/63309/mpvd (last visited Nov. 23, 2016)

[2] John B. Horrigan & Maeve Duggan, *One-in-seven Americans are Television "Cord Cutters,"* PEW RESEARCH CENTER (Dec. 21, 2015), http://www.pewinternet.org/2015/12/21/4-one-in-seven-americans-are-television-cord-cutters/.

[3] Tom Wheeler, *It's Time To Unlock the Set-Top Box*, RECODE (Jan. 27, 2016), http://www.recode.net/2016/1/27/11589108/its-time-to-unlock-the-set-top-box-market.

[4] *Id.*

[5] F.C.C., *F.C.C Chairman Proposal to Unlock the Set-Top Box: Creating Choice and Innovation* (Jan. 27, 2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0127/DOC-337449A1.pdf.

[6] Jon Brodkin, *FCC Changes Cable Box Rules To Please Industry, Gets Blow Back Anyway*, ARS TECHNICA, Sept. 8, 2016, http://arstechnica.com/information-technology/2016/09/fcc-changes-cable-box-rules-to-please-industry-gets-blowback-anyway/; Ian Paul, *The FCC's plan to replace your cable box with apps hits a snag*, PCWORLD (Sep. 30, 2016), http://www.pcworld.com/article/3126103/tech-events-dupe/fcc-delays-voting-on-unlock-the-box-cable-overhaul.html.

consumers are locked into leasing set-top boxes from their television providers in order to receive their multichannel programming.[7] The FCC's NPRM seeks to change this by allowing tech companies to create competing hardware and software to rival the standard set-top box.[8]

Under the initial proposal, the FCC sought to increase competition by requiring MPVDs to allow three flows of information to outside parties under a standard licensing agreement to be created by a third party.[9] The three information flows include: (1) service discovery (information about what programming is available to the consumer, such as the channel listing and video-on-demand lineup, and what is on those channels), (2) entitlements (information about what a device is allowed to do with content, such as record it), and (3) content delivery (the video programming itself, along with information necessary to make the programming accessible to persons with disabilities).[10]

The three flows would allow third parties to manipulate the way the consumer searches and experiences the content that MPVD provides. It would allow companies like Apple, Google, or any other company willing to develop their own hardware or software to produce a new user interface for consumers to watch multichannel content. Currently, devices such as Roku, Apple TV, and Smart TVs can provide consumers with access to digital content, like Netflix, but are preventing from using the content MPVDs provide.[11] Meanwhile, MPVD set-top boxes meanwhile do not equip users with the digital content just mentioned. This prevents consumers from having all their digital content in one place and necessitates multiple devices.

Chairman Wheeler's proposal seeks to allow third parties to use multichannel content so that businesses can compete over consumers to bring them the best hardware and software that allows them to view all their digital content in one place.[12] Set-top boxes are no longer a technological necessity, and facilitate restricted consumer choice without providing the benefits of an integrated digital system.[13]

---

[7] Wheeler, *supra* note 3.
[8] Brodkin, *supra* note 6.
[9] FED. COMM. COMM'N, FCC Rcd. 16-18, 2016, https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-18A1.pdf).
[10] *Id.*
[11] Consumers are sometimes able to access specific channels using the broadcasters' app, however, a paid cable subscription is required.
[12] Wheeler, *supra* note 3.
[13] *Fact Sheet: Chairman Wheeler's Proposal to Increase Consumer Choice & Innovation in the Video Marketplace*, FCC (Nov. 8, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0908/DOC-341152A1.pdf.

MPVDs made a counter-proposal in which they would provide their multichannel cable services via an app, which will be freely given to third-party device creators.[14] This offer has been incorporated into a newly revised FCC proposal.[15] The revised proposal relies on distributors to develop their apps within the next two years which must be compatible with all widely used entertainment devices.[16] The revised proposal serves both industry and FCC interests, as consumers will now have the option to stop leasing set-top boxes and distributors will have control of their content's user interface. The proposal does, however, stipulate that the content provided through the app must be fully integrated with the search function for other content, and should still be able to be recorded.[17]

The revised proposal also specifies a central licensing body that would issue standard licenses for MPVD content to qualifying third parties.[18] MPVDs have raised numerous concerns over this proposal. First, the MPVDs argue that a central licensing body is unnecessary and fails to reflect the reality of licensing in the current marketplace.[19] Licensing agreements are segmented, and programmers do not offer uniform licenses across uses and platforms.[20] Second, the proposal states that MPVD apps should be both HTML5 and non-HTML5.[21] MPVDs argue that licensing terms for HTML5 platforms do not necessarily apply to non-HTML5 platforms and that a decision to create a non-HTML5 platform should be left to the decision of the MPVDs and should not be imposed by the FCC.[22] In fact, MPVDs advocate that a standard license goes against the current licensing practices and would illegally force upon them a compulsory license.[23] Third, the central licensing for non-HTML5 platforms would not allow MPVDs to recover costs.[24] Fourth, the MPVDs state that the proposed compulsory licenses are beyond the scope of the FCC's authority under §629

[14] Brodkin, *supra* note 6.
[15] FED. COMM. COMM'N, *supra* note 9.
[16] *Id.*
[17] Brodkin, *supra* note 6.
[18] FED. COMM. COMM'N, *supra* note 9.
[19] Rick Chessen, Senior Vice President of Law and Regulatory Policy, National Cable & Telecommunications Association, and Stacy Fuller, Vice President of Federal Regulatory, AT&T Services, Inc., Comment Letter on Proposed Rule on the Commercial Availability of Navigation Devices (Sept. 6, 2016), https://ecfsapi.fcc.gov/file/109061991629473/2016-09-06%20As-Filed%20NCTA-AT&T%20Ex%20Parte%20(9-1-16%20FCC%20Mtg.).pdf.
[20] *Id.* at 2.
[21] *Id.*
[22] *Id.* at 3.
[23] *Id.* at 2.
[24] *Id.* at 3.

of the FCCA.[25] Requiring compulsory copyright licenses is under the authority of Congress.[26] This final concern has been supported by a letter from the Copyright Office.[27] The potential copyright issues have also been echoed by Commissioner Rosenworcel.[28]

It remains to be seen whether the FCC will vote on Chairman Wheeler's proposal, or whether further changes will be made taking into considerations concern within the industry, government, and the Commission itself. With the pressure of a change in administration, it is likely that this delay will not be too lengthy.[29]

[25] *Id.* at 4.
[26] *Id.* at 5.
[27] Letter from Maria Pallante, Director, United States Copyright Office, to Rep. Blackburn, Butterfield, Collins, Deutch, United States Congress (Aug. 3, 2016), https://www.eff.org/document/letter-maria-pallante-fcc-re-set-top-boxes.
[28] Cecilia Kang, *A Choice beyond Cable Box Rentals? It May Hinge on a Swing Voter*, N.Y. TIMES (Sept. 25, 2016), http://www.nytimes.com/2016/09/26/technology/a-choice-beyond-cable-box-rentals-it-may-hinge-on-a-swing-voter.html.
[29] *Id.*

SELF-DRIVING CARS: WHOSE FAULT IS IT?

Damon Ferrara*

CITE AS: 1 GEO. L. TECH. REV. 182 (2016)
http://bit.ly/2gtb1Hx

The burgeoning development of automated vehicle technology has been an increasing focus of journalists[1] and scholars[2] since major technology companies such as Google announced plans to develop the systems several years ago.[3] Coupled with the excitement over the technology's potential advantages has come a slew of controversies pertaining to the safety of such technology[4], and the technology's potential to supplant a number of human jobs.[5] Receiving somewhat less attention are the technology's legal idiosyncrasies, including questions regarding accident liability, insurance claims, vehicle and driver licensing, and even the application of existing vehicle laws to autonomous vehicles (self-driving cars appear to be much more observant of speed limits than their human counterparts, causing some to be cited by traffic police for driving too slowly).[6]

Perhaps the most significant legal question relates to vehicle accidents and liabilities: which party is at fault in an accident resulting from the features of self-driving technologies? The vast majority of automobile accidents are caused by driver error, which is an essential attraction of using artificial intelligence in personal vehicles.[7]

---

* GLTR Staff Member; Georgetown Law, J.D. 2018; University of Southern California, B.A. 2008.

[1] *See, e.g.*, Benjamin Zhang, *Autonomous Cars Could Save The US $1.3 Trillion Dollars A Year*, BUS. INSIDER (Sep. 12, 2014), http://www.businessinsider.com/morgan-stanley-autonomous-cars-trillion-dollars-2014-9.

[2] *See, e.g.*, James M. Anderson, *Autonomous Vehicle Technology: A Guide for Policymakers*, RAND CORPORATION (2016), http://www.rand.org/pubs/research_reports/RR443-2.html.

[3] Sebastian Thrun, *What we're driving at*, GOOGLE (Oct. 9, 2010), https://googleblog.blogspot.com/2010/10/what-were-driving-at.html.

[4] *See, e.g.*, Bill Howard, *Officials: DVD player found in Tesla Autopilot fatal crash*, EXTREMETECH (July 6, 2016), http://www.extremetech.com/extreme/231202-officials-dvd-player-found-in-tesla-autopilot-fatal-crash.

[5] *See, e.g.*, Matt McFarland, *Is Uber's push for self-driving cars a job killer?*, CNNMONEY (Aug. 19, 2016), http://money.cnn.com/2016/08/19/technology/uber-self-driving-cars-jobs/.

[6] *See, e.g.*, Alexander Smith & Shelby Hansen, *Google Self-Driving Car Gets Pulled Over — For Going Too Slowly*, NBC NEWS (Nov. 13, 2015), http://www.nbcnews.com/tech/tech-news/google-self-driving-car-gets-pulled-over-going-too-slowly-n462671.

[7] Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 SANTA CLARA L. REV. 1321 (2012) (referring to a

Consequently, it has become generally accepted that employing artificial intelligence (especially accident avoidance systems) in automobiles will help reduce traffic accidents in the aggregate.[8] With that in mind, some of the liability for the vehicle's operations (and accidents) will shift from the driver to the vehicle itself to the vehicle manufacturers and distributers.[9] This means that when accidents do occur, the manufacturers will be held liable for a greater proportion of overall accidents than they are currently.

The question of liability is at the center of recent controversies, such as the unfortunate Tesla Motors fatality in Florida last May[10] and the bizarre circumstances under which Uber asked test passengers to sign waivers freeing Uber of liability in the event of injury.[11]

The May 2016 Tesla Motors accident marked the first fatality involving a self-driving car, and some initial media reports seemed to attribute fault to the vehicle immediately, with one article describing the incident as the first known death "*caused* by a self-driving car."[12] Yet Tesla's press release response indicated that fault was not yet determined in the accident, citing both the artificial intelligence and the driver as having failed to notice a tractor-trailer that had pulled in front of the vehicle moments before the collision.[13] The investigation has not formally concluded, but later reports indicated that the driver was using a portable DVD player moments before the accident, leading

National Motor Vehicle Crash Causation Survey in which "NHTSA found that driver factors were the primary cause of the accident in 5096 of 5471 accidents studied, whereas vehicle problems were the primary cause of 130 accidents, and road conditions or weather conditions were the primary cause of 135 accidents.").

[8] *See, e.g., id.*

[9] *See id.*; *see also* Anderson, *supra* note 2.

[10] *See* Bill Vlasic, *Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says*, N.Y. TIMES (June 30, 2016), http://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html?_r=0.

[11] *See* Michael Nunez, *Uber's Self-Driving Car Passengers Were Signing Their Lives Away*, GIZMODO (Sept. 26, 2016), http://gizmodo.com/uber-s-self-driving-car-passengers-were-signing-their-l-1787108328.

[12] Danny Yadron, *Tesla driver dies in first fatal crash while using autopilot mode*, THE GUARDIAN (June 30, 2016), https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.

[13] The press release stated that "neither autopilot nor the driver noticed the white side of the tractor-trailer against a brightly lit sky, so the brake was not applied." The Tesla Team, *A Tragic Loss*, TESLA (June 30, 2016), https://www.tesla.com/blog/tragic-loss.

Tesla some commentators to imply that the driver was perhaps more at fault than the vehicle.[14]

To be clear, Tesla's 2015 Model S is not a fully autonomous vehicle; the Model S is equipped with a system called "Autopilot," which Tesla describes as a "driver assistance system." Autopilot is designed primarily to maintain "a vehicle's position in [a] lane and adjust the vehicle's speed to match surrounding traffic."[15] Still, it is likely that the feature (even if only in name alone) might give the impression that the vehicle can operate itself without human management under specific circumstances, leading many drivers to focus on things other than road conditions.[16] In those situations, tort liability can become a tricky topic; did the driver fail to employ the system properly, or did Tesla market an unreasonably dangerous product?

In that sense, the legal boundaries for semi-autonomous vehicles might be even less certain than fully autonomous vehicles—for semi-autonomous cars, liability seems to be nebulously shared between the driver and the system's manufacturer, rather than being apportioned almost entirely to the vehicle. Tesla, for example, chose to label Autopilot as a "driver assistance" system, and not as an "accident avoidance" feature. Within the list of Autopilot's driver assistance systems are features such as the "Automatic Emergency Breaking" function, which Tesla describes as a "collision avoidance *assist*" feature.[17] Labeling the Autopilot system as an "assist" feature is perhaps one way that Tesla can keep liability focused on the driver and thereby mitigate the potential for lawsuits when the system fails to fully "avoid accidents." In the event of an accident, Tesla might then argue that the system is there only to "assist" the driver, not to drive the car autonomously. Nonetheless, it is difficult to answer the question as to where the feature's responsibilities end, and where the driver's begin.

To make matters worse for Tesla, in September, a Chinese consumer initiated the first-ever lawsuit against the company for the failure of the

---

[14] *See generally*, Bill Howard, *Officials: DVD player found in Tesla Autopilot fatal crash*, EXTREMETECH (July 6, 2016), http://www.extremetech.com/extreme/231202-officials-dvd-player-found-in-tesla-autopilot-fatal-crash.

[15] *See* Bill Howard, *Tesla: We're not going to disable Autopilot (obviously)*, EXTREMETECH (July 13, 2016), http://www.extremetech.com/extreme/231662-tesla-were-not-going-to-disable-autopilot-obviously.

[16] *See id.; see also* Reuters, *Elon Musk Says Tesla's New Autopilot Likely Would Have Prevented Death*, FORTUNE (Sept. 12, 2016), http://fortune.com/2016/09/12/elon-musk-tesla-new-autopilot-death/.

[17] *Model S Software Release Notes v.6.2*, TESLA (2015), https://www.tesla.com/sites/default/files/tesla_model_s_software_6_2.pdf.

Autopilot system as the alleged cause of a traffic fatality.[18] According to the lawsuit documents, the Tesla vehicle crashed into the rear end of a road-sweeping vehicle while under Autopilot control. The documents further allege that "the autopilot programme's slow response failed to accurately gauge the road conditions ahead and provide instructions."[19] Tesla is reportedly still in the process of investigating the incident, which occurred in January in the Chinese Hebei province, but has had little progress in obtaining vehicle data from the plaintiffs.[20]

For its part, the National Highway Traffic Safety Administration (NHTSA) has been reviewing autonomous vehicles' safety features with more scrutiny, asking Tesla for a detailed list of information pertaining to the Model S's Autopilot functions.[21] NHTSA has not made final conclusions with respect to the artificial intelligence system's role in the May 2016 fatality, but the oversight is part of a larger trend towards possible federal oversight of automated vehicles in the future.[22]

Informed regulation in this area could prevent similar accidents before tort litigation would be necessary, but the same regulation might bring about its own slew of legal adjudicatory issues, wherein manufacturers would lobby aggressively against proposed stringent rulemaking by local, state, and federal regulators. California lawmakers have already received strong opposition from industry, leading some companies to characterize the regulatory agencies as being "overly restrictive and stifling innovation."[23]

Still, in cases similar to Tesla's, questions will remain as to whether the systems were being employed properly, and whether, in spite of the driver's actions, the system was responsible for any amount of the liability. If these issues are raised in tort lawsuits, the questions might also depend on whether the manufacturer provided adequate warnings or instructions for proper usage,

---

[18] *See* Brenda Goh & Norihiko Shirouzu, *Chinese man blames Tesla autopilot function for son's crash*, REUTERS (Sept. 15, 2016), http://www.reuters.com/article/us-tesla-crash-idUSKCN11K232.

[19] *See id.*

[20] *See id.*

[21] *See* Howard, *supra* note 15.

[22] NHTSA released new guidance in September 2016 giving manufacturers guidance for vehicle performance, including a 15-point safety assessment for the design, development, testing, and deployment of automated cars. NAT'L TRANSP. SAFETY ADMIN., DEP'T OF TRAN., DOT HS 812 329, FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY (2016).

[23] *See* Alexandria Sage, *California proposes giving more freedom to test self-driving cars*, REUTERS (Sept. 30, 2016), http://www.reuters.com/article/us-california-selfdriving-idUSKCN1212W6.

whether or not those warnings would be heeded or understood by the average consumer, whether the risk of the dangers was justified given possible alternative designs, and what a reasonable consumer would expect from such a vehicle or product feature—and given the fact that reasonable expectations regarding autonomous or semi-autonomous vehicles is a fairly unexplored region of law, liability could be quite tricky, indeed.[24]

Tesla, for example, has pointed to abundant warnings about Autopilot's proper use and the driver's continued responsibility to keep the vehicle under their control.[25] In Tesla's press release following the May fatality, the company cautioned that "every time that Autopilot is engaged, the car reminds the driver to 'Always keep your hands on the wheel. Be prepared to take over at any time.'"[26] With Tesla's assertion that the feature is simply an "assist" that requires you to maintain control of your vehicle at all times, one might ask what value the system provides at all? That is, if proper use of Autopilot does not allow the driver to remove their hands from the wheel, nor to cede "control" of their vehicle to Autopilot, is the experience substantially different from that of a non-autonomous vehicle?

Federal courts and products liability experts have long recognized that manufacturers cannot immunize themselves by simply "slapping warning labels" on dangerous products.[27] The Restatement (Third) of Torts likewise provides that "instructions and warnings may be ineffective because users of the product… may be likely to be inattentive, or may be insufficiently motivated to follow the instructions or heed the warnings."[28] If one accepts the notion that an average Autopilot user might not "always keep [their] hands on the wheel," perhaps some courts could find the warnings ineffective, as Tesla users would likely be "insufficiently motivated" to follow the instructions. After all, strict adherence to Tesla's instructions would seem to defeat the attraction of self-driving technology in the first place.

In any event, the battle to determine liability is far from over, highlighted by Tesla's most recent announcement that the Autopilot feature will be temporarily disabled for drivers who "ignore repeated warnings" to take back

---

[24] *See generally* RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY § 2 (AM. LAW INST. 1997).

[25] *See, e.g.*, The Tesla Team, *A Tragic Loss*, TESLA (June 30, 2016), https://www.tesla.com/blog/tragic-loss.

[26] *See id.*

[27] Hood v. Ryobi Am. Corp., 181 F.3d 608, 612 (4th Cir. 1999).

[28] *See* RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 CMT. L & REPORTER'S NOTE.

control of the vehicle.[29] This was considered by some commentators as a response to "widespread concerns that the system lulled users into a false sense of security through its 'hands-off' driving capability."[30] Indeed, on September 30, California regulators introduced draft regulations prohibiting manufacturers from using terms such as "autonomous" and "self-driving" when describing systems that are merely "semi-autonomous."[31] The future of self-driving cars will likely see a mix of more stringent regulations, oversight, statutory measures, and perhaps some high-profile lawsuits—at least until the technology is a little more commonplace, and lawmakers better understand their complexities.

[29] The Tesla Team, *Upgrading Autopilot: Seeing the World in Radar*, TESLA (Sept. 11, 2016), https://www.tesla.com/blog/upgrading-autopilot-seeing-world-radar-0.
[30] *See* REUTERS, *Elon Musk Says Tesla's New Autopilot Likely Would Have Prevented Death*, Fortune, Sept. 12, 2016, http://fortune.com/2016/09/12/elon-musk-tesla-new-autopilot-death/.
[31] *See* Sage, *supra* note 23.

STRONG SIGNALS FROM SPACE: WHAT DOES IT MEAN FOR INTERNATIONAL LAW?

Melissa Keech*

CITE AS: 1 GEO. L. TECH. REV. 188 (2016)
http://bit.ly/2gS4zgD

Astronomers across the globe marveled at news that a Russian radio telescope detected a uniquely strong signal of unknown origin, coming from the direction of a solar system akin to our own.[1] The signal's strength, much greater than noise power generally detected by the Russian satellite, was consistent with something extraterrestrial.[2] As researchers analyze and debate the signal's source, questions as to how the world would react to extraterrestrial contact have naturally arisen.

Radio telescopes, such as the one used here, allow astronomers to study space and the atmosphere.[3] Astronomical objects with changing magnetic fields, such as planets, produce radio waves.[4] Large radio telescopes detect the waves coming from space and analyze the waves' shape, strength, and path traveled to map the universe and study astronomical phenomenon.[5]

Although originally detected in May 2015, researchers first reported this signal at the end of this August.[6] Russia's telescope observed radio waves from the direction of the star HD164595, and witnessed a significant spike in signal intensity.[7] Located roughly ninety-four light years away from Earth, this solar

---

* GLTR Staff Member; Georgetown Law, J.D. expected 2018; Case Western Reserve University, B.S. 2014.

[1] Sam Thielman, *Alien Life, or noise? Russian telescope detects 'strong signal' from sun-like star*, THE GUARDIAN (Aug. 29, 2016), https://www.theguardian.com/science/2016/aug/29/russian-radio-telescope-strong-signal-hd164595-seti.

[2] *Mystery Alien Signal from Hercules Constellation – "Was from a Russian Military Satellite"—Russian News Agency TASS*, DAILY GALAXY (Sept. 5, 2016), http://www.dailygalaxy.com/my_weblog/2016/09/mystery-alien-signal-from-hercules-constellation-was-from-a-russian-military-satellite-russian-news-.html.

[3] National Aeronautics and Space Administration, *Radio Waves*, MISSION: SCIENCE (Sept. 23, 2016), http://missionscience.nasa.gov/ems/05_radiowaves.html.

[4] *Id.*

[5] Diane Fisher Miller, *Basics of Radio Astronomy for the Goldstone-Apple Valley Radio Telescope*, JET PROPULSION LABORATORY – NASA (Apr. 1998), http://www2.jpl.nasa.gov/radioastronomy/radioastronomy_all.pdf.

[6] *Mystery Alien Signal*, *supra* note 2.

[7] *Id.*

system is particularly interesting because it is centered around a star of similar brightness, age, temperature, and size to our sun.[8] We know of only one planet in this system, which is similar in size to Neptune.[9] This planet, however, orbits too close to the star to support life.[10] It is likely, however, that only a highly civilized society, perhaps more sophisticated than here on Earth, could generate such a signal from HD164595.[11] That signal strength would have required one hundred billion watts of energy to blast in all directions, and fifty trillion watts to blast just in the direction of Earth.[12] This is more energy than all the people on Earth combined use at the moment.[13]

Many researchers were hesitant to put any weight on the discovery. As with any research, replication is key. Out of thirty-nine scans that passed over this star, only one produced this strong signal.[14] Experts were also quick to point to alternative sources of the bizarre signal. Because the telescope scanned a large spectrum of space, verifying the particular direction the signal came from can be difficult.[15] Natural celestial events and objects, such as quasars, could have caused a similar signal strength.[16] Further, the signal's frequency was the same band as that allocated to Russian military use.[17] Russia also later announced that the signal originated instead from a Soviet Military satellite that had not been entered into the catalog of celestial bodies.[18]

The question remains how Earth would respond to an authenticated alien signal. The United Nations would likely be the primary authority for

---

[8] Thielman, *supra* note 1.
[9] *Id.*
[10] *Mystery Alien Signal*, *supra* note 2.
[11] Loren Grush, *Astronomers have picked up a strong radio signal from space – but it doesn't mean aliens*, THE VERGE (Aug. 29, 2016), http://www.theverge.com/2016/8/29/12695352/seti-russia-radio-observatory-signal-detected-alien-unlikely; *Alien Hunters detect 'strong signal' from star 95 light years away*, THE TELEGRAPH (Aug. 30, 2016), http://www.telegraph.co.uk/science/2016/08/30/alien-hunters-detect-strong-signal-from-star-95-light-years-away/.
[12] Dave Mosher, *Astronomers have detected an' interesting' and possibly alien radio signal coming from a sun-like star*, BUS. INSIDER (Aug. 29, 2016), http://www.businessinsider.com/alien-signal-seti-hd164595-2016-8.
[13] *Id.*
[14] *Mystery Alien Signal*, *supra* note 2.
[15] Mosher, *supra* note 12.
[16] Grush, *supra* note 11.
[17] Mike Wall, *'Alien' Signal Had Earthly Cause, Russian Scientists Say*, SPACE (Aug. 31, 2016), http://www.space.com/33922-mysterious-seti-signal-earthly-cause.html.
[18] *Mystery Alien Signal*, *supra* note 4.

dictating action, with resources already dedicated to "space law."[19] The United Nations Office of Outer Space Affairs (UNOOSA) is tasked with promoting the peaceful uses of outer space.[20] With laws aimed at ensuring international cooperation in the preservation of space and Earth's environments, sharing of potential discoveries, and regulation of space-related technologies, these laws do not speak directly to procedures in an instance of extraterrestrial contact.[21] However, the existing treaties and principles provide a relevant framework to start shaping this area of the law.

The most significant of the five international treaties that govern the use of space is the "Outer Space Treaty."[22] The treaty requires exploration and use of outer space to be carried out "for the benefit and interest of all countries."[23]. To ensure that space is used peacefully, the treaty specifically prohibits nations' appropriation of celestial bodies through claims of sovereignty, and the use of nuclear weapons in space.[24] Article XI of the treaty requires parties to inform the Secretary-General of the United Nations, the public, and the scientific community of the "nature, conduct, and results" of exploration activities.[25] This provision ensures that the UN would be informed of extraterrestrial contact, and would therefore be able to respond accordingly. Further, the existing provisions ensuring peaceable relations between countries on Earth would prevent violent relations with extraterrestrials. The United States has adopted similar domestic laws, often to ensure compliance with international treaties.[26]

---

[19] *Space Law*, UNITED NATIONS OFFICE OF OUTER SPACE AFFAIRS, http://www.unoosa.org/oosa/en/ourwork/spacelaw/index.html (last visited Sept. 23, 2016).
[20] *About Us*, UNITED NATIONS OFFICE OF OUTER SPACE AFFAIRS, http://www.unoosa.org/oosa/en/aboutus/index.html (last visited Sept. 23, 2016).
[21] *Space Law Treaties and Principles*, UNITED NATIONS OFFICE OF OUTER SPACE AFFAIRS (last visited Sept. 23, 2016), http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.
[22] *See Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, UNITED NATIONS OFFICE OF OUTER SPACE AFFAIRS, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html (last visited Sept. 23, 2016).
[23] *Id.*
[24] *Id.*
[25] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty), art. XI, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.
[26] *Human Activities in Spaces: Issues and Framework of the United States Law Concerning Outer Space*, GLOBAL RESEARCH, http://www.globalresearch.ca/issues-and-framework-of-the-united-states-law-concerning-outer-space/5484590 (last visited October 13, 2016).

The UN General Assembly adopts a yearly resolution entitled "International cooperation in the Peaceful Uses of Outer Space."[27] The Committee on the Peaceful Uses of Outer Space and its legal subcommittee review space research and legal problems that arise, and can thus adapt to rapid advances in space technology that could lead to these legal questions.[28] While these protocols wouldn't be legally binding, they would at least provide helpful guidance.[29]

One last useful guide for conduct in the event of extraterrestrial contact is the SETI Institute's "Protocols for an ETI Signal Detection." The SETI institute is a nonprofit organization dedicated to scientific research on the "origin and nature of life."[30] As part of its mission, SETI explores life in the universe.[31] The protocol is perhaps one of the only authorities concerning activities after the detection of extraterrestrial intelligence.[32] The protocol calls for verification of the signal, informing various parties including the UN, other researchers, and public media, and constant monitoring of the source.[33] While is protocol is not law and is targeted toward researchers, it could provide further groundwork for developing legal protocols.

While Russia's discovery seems to be of terrestrial origin, researchers like the SETI institute and astronomers across the globe continue to scan the skies for signs of life. Should these signals become verified in the future, it seems "space law" should expand to include "interstellar law." As our technology advances, our law should be prepared to respond to the new scientific findings.

---

[27] *Space Law: Resolutions*, UNITED NATIONS OFFICE OF OUTER SPACE AFFAIRS, http://www.unoosa.org/oosa/en/ourwork/spacelaw/resolutions.html (last visited Sept. 23, 2016).
[28] *Committee on the Peaceful Uses of Outer Space*, UNITED NATIONS OFFICE OF OUTER SPACE AFFAIRS, http://www.unoosa.org/oosa/en/ourwork/copuos/index.html (last visited Sept. 23, 2016).
[29] *Space Law: Resolutions*, *supra* note 26.
[30] *Our Mission*, SETI INSTITUTE, http://www.seti.org/about-us (last visited Sept. 23, 2016).
[31] *The Center for SETI Research*, SETI INSTITUTE, http://www.seti.org/node/61 (last visited Sept. 23, 2016).
[32] *Protocols for an ETI Signal Detection*, SETI INSTITUTE, http://www.seti.org/post-detection.html (last visited Sept. 23, 2016).
[33] *Id.*