# Table of Contents

## Articles
- Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids ................................................................. 273
- The Law and Legality of Smart Contracts ................................................................. 305

## Student Note
- Protecting Privacy in our Financial Transactions: An Alternative Method to Thinking about our Privacy in the Digital Era ............................................ 342

## Case Comments
- Bitcoin: Reacting to Money with Non-Money Attributes ........................................ 371
- Back and Forth: An Analysis of the Business Method Exception to Patentability ... 388
- U.S. v. Sarao: The Flash Crash and a new effort to prosecute market manipulation and deceptive trading practices ......................................................... 396

## Literature Review
- Privacy, Tax Evasion, and the Development of Cryptocurrencies .............................. 401

## Technology Explainers
- Smart Contracts: A Smart Way to Automate Performance ........................................ 417
- Machine Learning and Fintech .................................................................................. 428

## Legal News & Developments
- Fintech Meets the Telephone Consumer Protection Act ......................................... 446
- This Little Piggy Went to Wall Street: Privacy Law When a Toy Becomes Your Child’s Banker......................................................................................... 458
- Fintech and Trump Tech: How the New Administration is Shaping the Technology World Demands ................................................................. 477
- Insurtech: An Industry Ripe for Disruption ................................................................. 491
- Tribal Sovereignty and FinTech Regulations: The Future of Co-Regulating in Indian Country ................................................................................. 503
ARTICLES

SMART AFTER ALL: BLOCKCHAIN, SMART CONTRACTS, PARAMETRIC INSURANCE, AND SMART ENERGY GRIDS

Alan Cohn, Travis West, & Chelsea Parker*

https://perma.cc/65YT-PRTC

ABSTRACT

Blockchain technology—the technology behind Bitcoin—is a secure and resilient mechanism for conducting peer-to-peer electronic transfer of anything of value, with a resulting immutable transaction record. While blockchain is best known for payments and digital currency, one of the blockchain’s “killer apps” will be blockchain-based smart contracts. Blockchain-based smart contracts can be used to automate and execute “if-then” contractual relationships by coding these relationships onto the blockchain in order to automatically trigger their secure execution. The potential use cases are limitless; blockchain-based smart contracts can be used for everything from automobile leases, to voting, to recording of land titles.

A threshold question for the wide-scale use of blockchain-based smart contracts is whether such smart contracts are legally enforceable. This Article argues that existing laws, specifically the federal Electronic Signatures in Global and National Commerce Act (“ESIGN”) and state laws modeled on the Uniform Electronic Transaction Act (“UETA”), render blockchain-based smart contracts enforceable and therefore immediately usable.

With the enforceability of blockchain-based smart contracts established, this Article examines potential applications in the insurance and energy industries, in order to demonstrate the utility of such contracts. In the insurance industry, blockchain-based smart contracts can enable the automation of simple life insurance policies, thus reducing costs of administration, and provide a platform for new insurance products such as

*Alan Cohn is Of Counsel at Steptoe & Johnson LLP and Adjunct Professor, Georgetown University Law Center; he is also an advisor to several blockchain technology companies. Travis West is an Associate at Steptoe & Johnson LLP, Harvard Law, J.D. 2016, and Chelsea Parker is a Project Assistant at Steptoe & Johnson LLP, Princeton University, B.A., 2014. Cohn is co-chair, and West and Parker are members, of Steptoe’s Blockchain and Digital Currency Practice. © 2017, Alan Cohn, Travis West, & Chelsea Parker.
blockchain-based parametric insurance contracts. Within the energy industry, blockchain-based smart contracts can further enable the adoption of microgrids and technology such as smart meters, which can expand accessibility to different models of electric power distribution and provide resilience against accidental or deliberate disruption. In this way, blockchain-based smart contracts have the potential to both streamline and increase the efficiency of existing processes and open new models of service delivery.

ABSTRACT

INTRODUCTION

PART I: WHAT IS A BLOCKCHAIN AND WHAT IS A SMART CONTRACT? 
Blockchain Defined ................................................................. 277
Blockchain-Based Smart Contracts ........................................... 280

PART II: SMART CONTRACTS, UETA, AND ESIGN 
UETA and ESIGN ......................................................................... 286
How Do UETA and ESIGN Apply to Blockchain-Based Smart Contracts .... 288

PART III: SMART CONTRACTS, PARAMETRIC INSURANCE, AND THE SMART GRID
Insurance ...................................................................................... 290
Smart Contracts and the Energy Industry .................................... 297

CONCLUSION .................................................................................. 303

INTRODUCTION

Before 2016, blockchain technology was known, if at all, as the technical underpinnings of virtual currency. However, in the past year, blockchain technology has come into its own. It is now seen as a groundbreaking advance that can both reduce frictional costs in existing transactional systems and enable new, previously-unworkable models of social and commercial engagement.¹

A “blockchain,” as the name implies, is in its simplest terms a “chain” of previously-validated “blocks” of transactions that constitutes an immutable digital ledger and the distributed, resilient foundation for transfers of value. However, the newfound attention to blockchain has come with an increase in the attendant hype. Blockchain technology threatens to become the “next big

thing” and all sorts of blockchain-based projects are being proposed. For instance, the Republic of Georgia has committed to using the Bitcoin network to validate property-related government transactions, and a private company in San Francisco has developed new pharmaceutical packaging technology that uses blockchain to reveal whether a package has been opened.

These and other projects have led many observers to ask whether a simple cloud-based database could accomplish the same task, while others have asked whether there are actually realistic and beneficial uses for blockchain technology beyond simply underpinning a digital currency.

While centrally-administered cloud-based databases can accomplish many tasks, the crucial benefit of blockchain is the ability of the technology to enable transactions to occur in an environment where the parties do not trust each other and do not want to rely upon an intermediary. Blockchains are ideal for applications where transactions are transparent and no single user controls the rules of transaction; by contrast, a centrally-administered cloud database places a single entity in control of the rules of the platform, while also creating a central store of data that can be hacked or corrupted. For instance, in places where land records are poorly kept or changed because of corruption, a cloud-based database run by a central government would not provide the requisite trust that an immutable blockchain system would.

---

4 Luther Martin, Blockchain vs. Relational Database: Which is Right for your Application, TECHBEACON (Sept. 23, 2016), https://techbeacon.com/blockchain-relational-database-which-right-for-your-application [https://perma.cc/HQV9-7WLV].
food, speed and trust can be improved by using a blockchain-based tracking system.\(^8\)

If blockchain can enable high-value transactions in low-trust environments, a logical next step is to use blockchain to automate certain aspects of those transactions. Indeed, current blockchain scripting language enables the programming of “if-then” statements in order to automate transactions on a blockchain. By doing this, the value being digitally represented on the blockchain—often thought of as a “token,” like a digital coin—can be transformed instead into an instantiation of an agreement between parties that a transaction of value automatically take place upon the occurrence of a previously agreed-upon event or events.

Some have humorously noted that a “smart contract” is neither smart nor a contract, because it simply executes previously-written code, which itself was constructed to represent an actual contractual agreement.\(^9\) Nevertheless, the promise of automating existing and new processes while also eliminating the middle person, smart contracts may emerge as one of the blockchain’s “killer apps.”\(^10\)

But can blockchain-based smart contracts be recognized under law as currently conceived, and in what instance would this represent both a viable and a valuable usage? This Article examines these questions in turn. Part I of this article provides a practitioner’s background on blockchain technology and blockchain-based smart contracts. Part II sets out the argument advanced by digitization experts that existing laws, specifically the federal Electronic Signatures in Global and National Commerce Act (“ESIGN”) and state laws modeled on the Uniform Electronic Transaction Act (“UETA”), provide sufficient legal foundation for blockchain-based smart contracts to be enforced under current law. Part III of this Article describes potential uses within the insurance and energy industries where blockchain-based smart contracts could be implemented under the legal framework of ESIGN and state UETA-based laws.

---


\(^10\) Marvin, supra note 1.
PART I: WHAT IS A BLOCKCHAIN AND WHAT IS A SMART CONTRACT?

As noted above, a “blockchain,” can be understood as a “chain” of previously-validated “blocks” of transactions that constitutes an immutable digital ledger and the distributed, resilient foundation for transfers of value. Underpinning that simple description, however, is a sophisticated digital protocol that includes complex cryptographic algorithms, public and private encryption keys, and a transaction validation process that results in a high-integrity ledger of transactions. Similarly, a “smart contract” can be understood as a digital instantiation of an existing contract. However, this is not the only definition of a smart contract, and indeed, blockchain technology enables different types of smart contracts. This Part I explains these concepts in turn.

Blockchain Defined

“Blockchain” can mean—depending on who you ask—an append-only database, an underlying technological protocol, or a virtual currency system. For the purposes of this Article, we use the term “blockchain” or “blockchain technology” to refer to a distributed, decentralized ledger that, when combined with a digital transaction validation process, allows for peer-to-peer electronic transfer of an asset without the need for an intermediary, such as a bank.11 Blockchains replace centralized recordkeeping by having every participant in a blockchain-based process maintain an append-only copy.12 Every participant can write to and view the ledger, but no participant can change the rules of administration.13 This distributed ledger is synchronized in real time by a community of individuals (through their computers, or banks of computers) validating transactions.14 This synchronization of recordkeeping prevents users from posting invalid transactions to the blockchain, such as trying to spend a resource that user has already spent, since the invalid transaction (e.g.

11 Bernard Marr, A Complete Beginner’s Guide to Blockchain, FORBES (Jan. 24, 2017), http://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#36e42ce666a6 [https://perma.cc/6NVB-W8YB]. Although blockchains are much more general, this Article will only focus on their applicability to smart contracts due to the intense interest in smart contracts.
13 See Greenspan, supra note 6.
14 See VIGNA & CASEY, supra note 12.
a double-spend of a single asset) would be detected by the rest of the community by comparison to their copies of the ledger.\(^\text{15}\) The validation of individual transactions is performed using different types of digital mechanisms—for example, the Bitcoin blockchain uses a proof-of-work algorithm\(^\text{16}\)—and solutions to the proofs are verified by the community.\(^\text{17}\)

As the previous paragraph implies, blockchain technology relies on a variety of digital processes to maintain the integrity of the system, including sophisticated cryptographic algorithms. Cryptography is the science behind protecting and securing information, typically in an insecure environment. Within the blockchain ecosystem, cryptography can be used to protect the identity of participants, keep transactions private, and confirm the authenticity of the transactions. A transaction is signed with a cryptographic key by the participants, which ensures that each participant validated it and prevents a third-party from impersonating one of the participants. The transaction is then encrypted in such a way that the digital signatures of the participants and the contents are all signed, so that no one can change any part without causing others on the blockchain to reject the transaction. Multiple transactions are added onto a block, which references the previous block via its cryptographic signature.\(^\text{18}\)

The keys that are used to sign transactions are normally implemented using asymmetric encryption. In asymmetric encryption, each user generates a pair of keys that are linked through complex algorithms: one is a private key that the user keeps secret; and the other is a public key that, as the name implies, is publically available.\(^\text{19}\) If a second user wants to share information

\(^{15}\) See Marr, supra note 11.


\(^{19}\) See Panayotis Vryonis, Explaining Public Key Cryptography to Non-Geeks, MEDIUM (Aug. 27, 2013), https://medium.com/@vryanexplaining-public-key-cryptography-to-non-geeks-f0994b3c2d5#2tkqtmuti [https://perma.cc/IZW3-8NHK]. The following discussion about asymmetric encryption is drawn from this article.
with the first user, the second user can sign a document with the first user’s public key, which will encrypt it in such a way as to ensure that only the first user’s private key can decrypt it. Conversely, the first user can sign a document using their private key. That document will only be able to be decrypted by the corresponding public key, which establishes that the encrypted document was signed by the first user.

Being distributed and open, the blockchain enables high-trust transactions without the need for an intermediary or third party since many parties are verifying each transaction. The Bitcoin blockchain, for example, ensures that transactions are validated by incentivizing validators with a small financial reward that is unrelated to the underlying transaction. For popular public blockchains such as the Bitcoin blockchain and Ethereum, transactions are public, and identity is based on the user’s public authentication key. By distributing copies of the ledger, the system is resilient and resistant to corruption or attacks on single or groups of nodes. These characteristics enable blockchain to incorporate both security and resilience by design.

Blockchains can also be private or “permissioned.” Permissioned blockchains are administered by a single entity, although other technical attributes common to open or permissionless blockchains remain the same. As the name applies, permissioned blockchains can be configured to restrict access or permissions to only approved users. Permissioned blockchains give administrators the right to both control access and require a higher degree of authentication. Private blockchains are instantiations of similar technology in a fully private space, such as a private server or cloud-based environment.

Blockchain technology has made noteworthy progress in the past year, from large banks and governments experimenting with the new technology, to newly formed consortia facilitating industry-wide exploration. Over forty percent of senior executives at U.S. organizations with over $500 million in

---

20 VIGNA & CASEY, supra note 12.

21 A node is a computer connected to the blockchain network. Each node, which can represent an individual or entity, maintains a copy of the blockchain.


23 Id.

annual revenue believe blockchain will disrupt their industry.\textsuperscript{25} While the financial services industry was one of the first industries predicted to be disrupted by blockchain, a range of industries, from life sciences and healthcare, to technology and media, are showing significant interest.\textsuperscript{26} For example, over forty-two percent of senior executives at U.S. organizations in the consumer products and manufacturing industry with over $500 million in annual revenue are planning to invest $5 million or more in the next calendar year.\textsuperscript{27} These investments are not just speculative, with twenty-one percent of the executives stating that they have already brought blockchain-based applications into production.\textsuperscript{28}

Despite the technical differences between open, private, and permissioned blockchains, for the purposes of this Article, we will use the term “blockchain” or “blockchain technology” to refer to the technology generally, as each of these types of blockchains presents similar opportunities and challenges from a smart contracts perspective.

\textit{Blockchain-Based Smart Contracts}

Smart contracts as a concept are not intrinsically linked to blockchain. “Smart contract” is often used interchangeably with a broad range of terms, from “smart legal contract” to “digital contract” to “smart contract code.”\textsuperscript{29} Generally, the definitions include some type of automated, self-executing transaction.\textsuperscript{30}

A smart contract has multiple benefits over traditional contracts.\textsuperscript{31} The digital nature of the contract ensures that there is a final version of the contract written in a detailed method that will be executed precisely by computers.


\textsuperscript{26} Id.

\textsuperscript{27} Id.

\textsuperscript{28} Id.


\textsuperscript{30} See, e.g., id.

when necessary. Unlike a paper contract, which can be destroyed or exist in multiple versions, a smart contract will by necessity be saved and executed only according to its encoded instructions. By forcing the contract to be translated into computer code, a smart contract lessens the parol evidence problem, in part because a computer cannot consider any external evidence and can only run the code that it is given. It will be difficult for a party to argue that there were agreed upon but un-incorporated issues if that party signed and verified that the contract had been accurately translated into computer code. Even if the parties dispute the terms later, the smart contract itself becomes a powerful form of evidence that demonstrates what the parties thought they were agreeing to.32

Smart contracts are most efficient for contracts that can be reduced to simple “if-then” statements, as their terms are easy to convert to computer code and can be executed automatically. For instance, a life insurance contract can be coded as an “if-then” statement by specifying that if the policyholder dies, then payment to the beneficiaries commences. For similar contracts, given the option of a smart contract, it may no longer be efficient to have a person in charge of administering and executing these contracts.

For the purpose of this Article, a blockchain-based smart contract is a contract between two or more parties that is stored and digitally executed on the blockchain using code.33 While human involvement is needed to define the contract and input the code, the actual execution of the contract is automated based on a defined parameter, such as an event or price.34

Blockchain-based smart contracts have the potential to impact a range of industries35 and some are even calling 2017 “The Year of Smart Contracts” for blockchain.36 Blockchain-based smart contracts can be used not only to


34 Id.


 automate existing processes, but also to create new industries and reach new markets. By providing a digital platform for coding “if-then” statements, providing a secure and resilient environment for value transactions, and preserving a detailed and immutable transaction history, the blockchain provides an ideal platform for smart contracts. Blockchain technology allows users to write an agreement into code in the exacting detail required by both a court and a computer to faithfully execute only terms agreed to by the contracting parties.37

For the purposes of blockchain-based smart contracts, every action on a blockchain can be configured to require the participants to sign off on the transaction using their private cryptographic key.38 This helps to create the record of transaction and verifies the identities of the parties involved in case of later disputes. Once a consensus is reached that a transaction is valid, the transaction is added as a block of multiple other transactions to the chain of previous blocks of transactions (hence, “blockchain”).39 These blocks are then part of the ledger and cannot be removed or changed, giving the chain both transparency and immutability.40 For instance, if a party later wants to edit or cancel a transaction, rather than removing that block from the blockchain, a new transaction will be formed and the underlying asset will be returned in that transaction.

Another essential element of blockchain-based smart contracts is the ability of the blockchain protocol, as a digital system, to monitor for events that would trigger the embedded “if-then” statement. Having every node—each of which verifies the correctness of the blockchain simultaneously—

38 See Berger, supra note 18.
39 Consensus can be achieved in multiple ways. Bitcoin relies on proof of work for validation. However, an alternative system could be set up so that once the participants in a transaction, or a certain percentage of the participants, reach consensus, the rest of the chain will recognize it.
40 Of course, for some transactions, transparency would not be a goal. A blockchain can be set up so that only the participants (and regulators) would be able to inspect the actual details of the transaction. To the rest of the chain, it would appear as a block was added but the details were kept encrypted. Cf. Cliff Moyce, How Blockchain Can Revolutionize Regulatory Compliance, CORPORATE COMPLIANCE INSIGHTS (Aug. 10, 2016), http://www.corporatecomplianceinsights.com/blockchain-regulatory-compliance/ [https://perma.cc/LSQ7-RX9D].
monitor external sources for the defined parameter is complicated, and entails certain risks. While there are a few possible solutions, oracles are a common solution. Oracles are one or more external digital agents or sources trusted by the blockchain participants.\(^{41}\) The oracle monitors the external parameters designed within the smart contract, and gives direction or approval to execute the contract if those parameters are met.\(^{42}\) An oracle can be configured to work with numerous blockchains, external sources, and any necessary entity involved with automating the execution of the smart contract.\(^{43}\) Using an oracle or other triggering mechanisms, smart contracts will only execute upon the occurrence of agreed-upon events, based on agreed-upon sources of information. In this way, smart contracts have the potential to simplify administration of a range of commercial contracts.

Although blockchain technology is being explored in many areas, its usage in smart contracts has been among the most prominent.\(^{44}\) The Ethereum blockchain was among the most popular blockchain implementations of smart contracts, due to its scripting language that could be used to write the contracts.\(^{45}\) The native ability to generate smart contracts has led to a proliferation of startups using Ethereum, ranging from gambling contracts to energy contracts.\(^{46}\) Ethereum also has its own native currency, Ether.\(^{47}\)

---


Companies are also emerging to build enterprise-grade applications on the Bitcoin blockchain. Similarly, as with other open-source environments, third party companies are developing a range of applications for the Bitcoin and Ethereum blockchains and others, including applications focused on identity, device authentication, and transaction analysis.

Recognizing the potential benefits of blockchain-based smart contracts, industry leaders have already started experimenting with new applications. $116 million was invested in smart contract venture capital-related deals in the first quarter of 2016 alone. Governments and regulatory agencies are also experimenting with blockchain-based smart contracts. The state of Delaware created the Delaware Blockchain Initiative and is exploring the use of blockchain-based smart contracts to increase recordkeeping efficiency and reduce costs.

PART II: SMART CONTRACTS, UETA, AND ESIGN

With companies and industries continuing to explore new blockchain-based smart contract applications, it is important to establish the enforceability

---

48 The value of Ether collapsed when a bug was found in its most popular implementation, the Distributed Autonomous Organization or “DAO,” which nearly allowed a hacker to steal millions of dollars’ worth of Ether. Jonathan Ore, How a $64M Hack Changed the Fate of Ethereum, Bitcoin’s Closest Competitor, CBC NEWS (Aug. 28, 2016), http://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009 [https://perma.cc/HA2N-H2YK]. However, Ethereum remains a popular platform for smart contract development.


of blockchain-based smart contracts. Technical details aside, questions have been raised as to whether a contract on the blockchain is binding and enforceable. Vermont, for instance, has made multiple attempts to pass a law that would make blockchain evidence self-authenticating, and has finally succeeded in enacting one. Arizona recently passed a law clarifying that signatures obtained through blockchain technology are valid electronic signatures. It is not clear that Arizona was responding to any perceived problem with the enforceability of signatures obtained through blockchain technology; instead, the bill appeared to be a way for the state to signal that it is open to blockchain companies.

Even if these contracts can be efficiently translated into computer code onto the blockchain, they will not help anyone if they are not legally enforceable. Contract law is a complicated area of law, with principles dating back to medieval England. Disputes often arise about the interpretation of terms. For parties who agree upon a contract and then convert it to computer code, a dispute about a term in the original contract may now be compounded by a disagreement about its manner of implementation in computer code.

In this Part II, we argue that current laws, such as UETA and ESIGN, already allow for smart contracts to be enforced. Part II describes the evolution and application of state laws modeled on UETA as well as the federal ESIGN. Part II also describes how blockchain-based smart contracts fit under these authorities. Based on this examination, we conclude that blockchain-based smart contracts are enforceable under UETA and ESIGN.


55 See VT. STAT. ANN. tit. 12, § 1913 (West 2016).


UETA and ESIGN

A. Development of UETA and ESIGN

In the early days of the internet, states enacted a patchwork of laws designed to balance the needs of online commerce with protections of consumers and businesses. In response to the often-contradictory state laws, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") drafted UETA to provide a model law to harmonize the rules governing electronic commerce transactions.\(^61\) Currently, forty-seven states, the District of Columbia, and the U.S. Virgin Islands have enacted a form of UETA.\(^62\)

Despite the UETA’s purpose of providing a standard national code governing electronic commerce transactions, states inconsistently implemented UETA by changing several provisions to protect consumers or reflect their own state laws.\(^63\) Businesses, again facing the challenge of needing to comply with multiple inconsistent state laws, pushed for a new law to standardize the equivalence between electronic signatures and other forms of signatures on a national level.\(^64\)

Congress responded by passing ESIGN, which, while mirroring UETA in many ways diverged in some provisions, including consumer consent requirements.\(^65\) However, Congress included a pre-emption provision that gives states the option between ESIGN compliance or UETA adoption.\(^66\) Congress specified that states could preempt ESIGN with their own laws, so


\(^63\) For example, California was the first state to implement UETA, but it added several pro-consumer exceptions. See Kristin Burford, Uniform Adult Guardianship and Protective Proceedings Jurisdiction Act: E-SIGN, CAL. L. REFORM COMM’N (Mar. 28, 2013), http://www.clrc.ca.gov/pub/2013/MM13-14.pdf [https://perma.cc/B8DJ-QNG5].

\(^64\) Robert A. Wittie & Jane K. Winn, Electronic Records and Signatures under the Federal E-Sign Legislation and the UETA, 56 BUS. LAW. 293, 294 (2000); see also 146 Cong. Rec. S. 5217 (statement of Sen. McCain) (“A majority of States have enacted electronic authentication laws, but no two of these laws are the same. This inconsistency deters businesses and consumers from using electronic signature technologies to authorize contracts or transactions.”).

\(^65\) Id.

long as those laws were either UETA or did not conflict with ESIGN.\(^{67}\) This reflected the desire that states either follow ESIGN or adopt UETA and displace ESIGN.\(^{68}\) In this way, the preemption provision ensures that either ESIGN or UETA governs electronic transactions.

### B. Common Provisions of UETA and ESIGN

UETA and ESIGN share several features. First, both guarantee that a signature or record will not be held legally ineffective because it is in electronic form.\(^{69}\) Second, both clarify that any law that requires a record to be in writing will be satisfied by an electronic record.\(^{70}\) Finally, an electronic signature is held to be the equivalent of a written signature for any law that requires a signature.\(^{71}\) Collectively, these provisions ensure that electronic records and signatures carry the same legal authority as physical documents and signatures.

These provisions also recognize the notion that consent can be granted by electronic means. UETA requires that both parties agree to “conduct transactions by electronic means,” which can be “determined from the context and surrounding circumstances, including the parties’ conduct.”\(^{72}\) ESIGN and UETA also have sections relating to the retention and accessibility of any electronic records.\(^{73}\) Both acts require that an electronic record be producible and must accurately reflect the final form that the parties agreed upon.\(^{74}\)

Overall, the effect of UETA and ESIGN is to allow digital signatures to have the same effect as a physical signature. Congress wanted to allow businesses to benefit from the efficiency of transmitting and signing documents electronically and to free businesses from being required to keep a warehouse full of contracts.\(^{75}\) Although it is difficult to imagine now, the

\(^{67}\) Id.

\(^{68}\) See Wittie & Winn, supra note 64, at 295.

\(^{69}\) 15 U.S.C.A. § 7001; UETA § 7(a).

\(^{70}\) Id.

\(^{71}\) Id.

\(^{72}\) UETA § 5(b).

\(^{73}\) Id. at § 12; 15 U.S.C.A. § 7001(e).

\(^{74}\) U.S.C.A. § 7001(e); UETA § 12(a)(1)-(2).

\(^{75}\) 146 Cong. Rec. S. 5217-18 (statement of Sen. McCain) (“It would ensure that consistent rules for validating electronic signatures and transactions apply throughout the country. Thus providing industry with the legal certainty needed to grow electronic commerce. It empowers businesses to replace expensive warehouses full of awkward and irreplaceable paper records with electronic records that are easily searched or duplicated.”).
Congressional Record is replete with the concern that electronic signatures would somehow be less valid than physical signatures unless Congress acted. The courts have interpreted both the UETA and ESIGN in a way to help facilitate digital transactions, which has allowed the digital economy to grow. Indeed, UETA and ESIGN have allowed credit card applications, loan applications, and other transactions to be performed online while still being enforceable.

How Do UETA and ESIGN Apply to Blockchain-Based Smart Contracts

The key to the applicability of UETA and ESIGN to blockchain-based smart contracts is the cryptographic key with which blockchain-based smart contracts are signed and acknowledged. Simply put, asymmetric key encryption falls squarely within the both the language and intent of ESIGN and UETA as an “electronic signature.”

As noted above, one way for a party to express agreement with the terms of a blockchain-based smart contract is to provide its digital signature utilizing a cryptographic key. This signature, expressed using asymmetric key encryption, is similar to the initial digital signatures that early forms of UETA envisioned. UETA defined “electronic signature” as “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” An electronic signature therefore has two components: the signature, in whatever form it is, and the intent to sign.

Courts have interpreted the requirement for the signature and the intent to sign broadly. For example, courts have found that typing “Thanks” plus the sender’s name in an email constitutes a signature. The court in that case noted that the plaintiff manually typed her name, as opposed to having a default signature automatically attached by her email program. This is a low bar to set to allow UETA to enforce the contract.

By contrast, parties using blockchain-based smart contracts would negotiate terms and then each party would need to use their cryptographic

76 Id. at S. 5219. (statement of Sen. Leahy) (“The AARP found that of consumers over the age of 45, half of them worry that electronic contracts will give them less protection than paper contracts. That is what we want to avoid.”).
77 UETA § 2(8). The definition of “electronic signature” under ESIGN is essentially the same. 15 U.S.C. § 7006(5).
79 Id.
key, unique to them, to sign off on the contract. The cryptographic key would be either a “symbol or process attached to or logically associated with a record,” and the deliberate signing off would demonstrate each party’s “intent to sign the record.” Regardless of the specific contract terms, the fact that a blockchain-based smart contract can require the participants to sign the contract through the cryptographic key should assure courts that a blockchain-based smart contract is a legally-binding agreement under UETA and ESIGN.

Moreover, a blockchain-based smart contract can prevent some of those factual challenges because the cryptographic nature of the signature for a blockchain-based smart contract can more effectively establish a person’s identity. In a case arising out of Louisiana, a court upheld the applicability of Louisiana’s version of UETA to automobile insurance contracts but held that a genuine issue of fact existed over whether the plaintiff had actually signed the insurance waiver.80 The insurance company insisted that she had, but she pointed out that the waiver was signed four days after she met with the insurance agent to apply for insurance.81 Due to this conflict, the case needed to go back to the trial court for further proceedings. This is not an uncommon issue, as similar cases have arisen in other jurisdictions.82 These kinds of disputes often boil down to which side can muster enough evidence that the proper person signed the contract or create enough doubt to go to trial, where a jury could be swayed by other concerns.

A blockchain-based smart contract, by contrast, needs to be signed by each party using a cryptographic key that only each party has access to. This cryptographic key is a much more reliable identifier, as it is nearly impossible for someone to forge the key, as it would require cryptographic hacking that is only available to nation-state actors. A third party can see that signature and immediately know who signed it, preventing many disputes about the authenticity of a signature. A party may argue that its cryptographic key was stolen, but unlike in cases where someone’s bitcoin wallet key is stolen to transfer funds, the benefits of stealing the key for an insurance contract or other type of blockchain-based smart contracts are much less obvious. In the case of an insurance contract, the beneficiary could not be changed without needing a new smart contract and the smart contract would ensure that the premium is being paid, which lessens the chance a party could enter into a

80 Bonck v. White, 2012-1522 (La. App. 4th Cir. Apr. 24, 2013); 115 So. 3d 651, 655.
81 Id.
fraudulent contract. Instead, the cryptographic signing would function much like having witnesses observe the signing of a will. It would create a high barrier to overcome and reduce costs of enforcement, as fewer parties would be willing to go to court to contest that they signed a contract, as the evidence would be difficult to overcome.

PART III: SMART CONTRACTS, PARAMETRIC INSURANCE, AND THE SMART GRID

Blockchain-based smart contracts have the potential to benefit the insurance and energy sectors by streamlining current activities and opening new markets for products. Both the insurance and energy sectors can take advantage of blockchain to digitize and streamline administration of existing processes and utilize the technology to offer new products and services where transparency, trust, and simplicity offer value. In the insurance industry, many of the most common forms of contracts can be reduced to simple “if-then” statements and digitized as blockchain-based smart contracts. Digitizing the administration of existing policies would reduce the cost of administering these products; using basic parameters for policy payout could leverage blockchain-based smart contracts’ ability to easily administer “if-then” transactional relationships. In the energy industry, blockchain-based smart contracts can enable smart grids, microgrids, and other types of innovative grid management technologies by both providing the mechanism for automating value transmission and the means to streamline transaction administration. Blockchain’s trust environment for transactions can also open new markets for innovative methods of service provision and payment for service. As such, both the insurance and energy industries provide real-world use cases to demonstrate the value of blockchain-based smart contract technology.

Insurance

Basic insurance contracts can often be boiled down to an agreement to make payment upon the occurrence of a discrete event. However, administration of even apparently straightforward insurance policies can become complex. Claims adjusters are needed to assess a claim and its validity. If parties later disagree about the interpretation of the terms, or the parties relied on representations outside of the policy, disagreements can arise.
Parties are often mistrustful of one another even in the most cordial customer-service environment because of the potential for fraud, abuse, or denial of claims. In either event, insurance companies incur costs administering even the simplest of contracts, and those costs are often passed along to consumers in the form of higher premiums.

Blockchain-based smart contracts can avoid many of these problems. They can be structured to reflect the basic “if-then” relationship of many basic insurance policies. Through the use of event monitoring functions, such as oracles, payments can be automatically triggered based on objective validation of specified events. Construction of blockchain-based smart contracts requires the parties to precisely define the terms of the policy so that those terms can be executed by a digital protocol, since the protocol can be programmed to execute only explicit policy terms. Moreover, by overcoming challenges of trust and providing transparency, new types of policies for different or underserved populations can be structured and utilized.

A. Efficiency Gains in Current Insurance Contracts: Life Insurance and Final Expense Policies

Some of the simplest “if-then” types of insurance policies are individual life insurance and final expense policies. Life insurance contracts pay out upon the policyholder’s death. Although this process is normally easy for the survivors to carry out, usually requiring the presentation of a death certificate or other proof of loss and a beneficiary form, problems can arise in multiple ways. For example, the policyholder may hold multiple life insurance policies, the beneficiary may not know about the policy, or the beneficiary may misplace the paperwork for the policy. As a result, inefficiencies and increased administration costs can arise without any malfeasance or ill-will from any party.

Blockchain-based smart contracts can remedy many of these problems. For example, rather than maintaining only a written insurance contract, a blockchain-based smart contract is digitally instantiated and recorded to the blockchain’s immutable ledger. Rather than relying upon the policyholder to retain the policy (making the policy subject to loss through misplacement or destruction by fire, flood, or similar occurrences), the policy would be

---

recorded on the blockchain and its terms would be available at any time for the insurer, the policyholder, and the beneficiary to review. Rather than relying upon a beneficiary to notify the insurance company, a blockchain-based smart contract can be constructed to rely on oracles set to monitor specific sources of information about individual deaths. The transparency of the blockchain and the fact that its rules are not administered by any single participant in the process can allow purchasers to rely on digital instantiation and administration.

Digitization has already enabled portions of this process. The United States government maintains the Social Security Death Master File, which tracks when a person with a Social Security number dies.84 Although this is not a perfect record and has in many instances been subject to legitimate criticism for its accuracy,85 an oracle could monitor this file for policyholders, and upon the death of a policyholder the oracle could trigger the potential execution of the blockchain-based smart contract. Currently, the Master File is only updated once a week and a person’s death must be reported to the Social Security Administration for it to be filed.86 For that reason, oracles could also monitor other digitally-available sources of information, such as social media, in order to provide further assurances before the final execution of the contract.87 Indeed, some organizations are already experimenting with peer-to-peer unemployment insurance smart contracts based on LinkedIn data.88

A similar application for blockchain-based smart contracts in insurance is final expenses insurance. Final expenses insurance is a form of insurance where a fixed sum is paid out upon a person’s death to help cover

84 SOC. SEC. DEATH MASTER FILE, https://www.ssdmf.com/FolderID/1/SessionID/%7BA19D1475-03BF-4688-9934-27CFB0BE9234%7D/PageVars/Library/InfoManage/Guide.htm (last visited Apr. 16, 2017) [https://perma.cc/5LFC-LNZL].
86 Id.
funeral costs.\textsuperscript{89} For some cultures, it is essential to have a proper funeral or perform funeral traditions.\textsuperscript{90} However, families are often unable to pay for an unexpected funeral or even the funeral of an elderly family member. A blockchain-based smart contract could be set up using the same sources as a life insurance smart contract and perform the same function. Indeed, contracts could even be purchased by family members in other countries, with agreed-upon oracles and specified mechanisms of digital payment, such as direct payment to funeral providers, rather than reliance upon local reporting and paper checks.

B. New Models of Insurance: Parametric Insurance

Life insurance and final expense insurance are good examples of simple “if-then” arrangements that can be digitized into blockchain-based smart contracts in relatively straightforward ways. But could other types of insurance that are currently reliant on more subjective factors be restructured into products with more firmly defined parameters, enabling their digitization and administration through blockchain’s transparent processes? Parametric insurance policies offer such potential. By pairing parametric insurance with blockchain-based smart contracts, insurers can reinvent the manner in which classes of insurance are offered.

Parametric insurance is a form of insurance where the payouts are determined not through a claims adjuster surveying the damage, but based on objective measures, such as the magnitude of a weather event.\textsuperscript{91} It is most often used for insurance for natural catastrophes, such as tornadoes or hurricanes, where individualized policies based on specific damage would be difficult and costly to administer but a standardized payout based on proxies, such as the severity of the storm, would suffice.\textsuperscript{92} Parametric insurance is


\textsuperscript{90} Kate Torgovnick May, Death is Not the End: Fascinating Funeral Traditions Around the Globe, TED (Oct. 1, 2013), http://ideas.ted.com/11-fascinating-funeral-traditions-from-around-the-globe/ [https://perma.cc/M42H-V628].


\textsuperscript{92} Melody Schreiber, A Super-Nerdy Insurance Plan Could Save Poor Countries from Damaged Caused by Climate Change, Quartz (Nov. 18, 2016), https://qz.com/840570/a-
preferable to other forms of insurance when a quick payout is necessary, such as when a country suffers a hurricane and needs to quickly obtain money to begin rebuilding and pay emergency workers.\textsuperscript{93} Parametric insurance can lower the time of payment from months to two weeks, which can help jumpstart the rebuilding process.\textsuperscript{94}

The key to parametric insurance is finding objective indicators that can serve as an effective proxy for the type of loss being covered. The benefit to doing so is that once effective proxies are identified, policies that would need to be adjusted qualitatively could instead be reduced to simpler “if-then” statements. For example, by relying upon objective markers, such as storm intensity, wind speed, or amount of rain, there is no need for individualized adjustment of claims. After a hurricane damages an area, an oracle can pull data from a third-party site, such as the National Weather Service, to determine objective measures, such as the strength of the storm, and then make a payment based on that data. While individual losses may be greater or less than the specified payment amount, the insurer gains certainty in loss forecasting and the policyholder gains speed in payment. Both parties benefit from the automation of the process and the reduction in frictional costs.

Parameterizing current forms of insurance based on proxies for loss and coding these policies onto blockchain-based smart contracts can fundamentally alter insurance offerings by (1) lowering transactional costs of simple policies to allow for lower-premium policies to be profitably administered and (2) opening new markets for insurance products since locally-based claims adjustors or other local trusted agents would no longer be necessary to effectively administer the policy. Although some costs are difficult to manage, studies have found that for property and casualty insurance, management and contract administration is the largest driver of cost variance.\textsuperscript{95} Indeed, for property and casualty insurance, one study concluded that over eighty percent of the cost variance was attributed to management factors, not to the underlying product.\textsuperscript{96} It is estimated that

\begin{ex}
\textsuperscript{93} Id.
\textsuperscript{94} Id.
\textsuperscript{96} Id.
\end{ex}
improving IT efforts alone could reduce costs by twenty to forty percent, with business complexity and performance management being other large drivers of cost variance.97

Moving to parametric blockchain-based smart contracts has the benefit of addressing IT improvement, business complexity, and performance management, while gaining transparency and trust. Blockchain technology can be implemented without having to discard current IT systems, as a blockchain-based platform can be added on top of an existing IT system and, indeed, is commercially available through several cloud services providers.98 Parameterizing current policy structures drastically reduces business complexity, and its standardization of payouts and parameters allows for much more bounded modeling of potential loss events and amounts. Finally, blockchain-based smart contracts can be administered through oracles and monitored in real-time through analytic software examining the permanent blockchain record of transactions and loss occurrences, creating incentives both for parameterization and for reducing such policies to blockchain-based smart contracts. Fewer local agents would be necessary, and the use of oracles could replace the need to rely on the reports of adjusters on the ground.

As a result of the reduction in frictional costs, policies that were previously unprofitable because of low margins—due to the low premiums or high administration costs—could become profitable areas for new products. For example, companies could profitably insure extremely low premium and low payout events through no-fault parametric policies, where the payouts are determined based on readings from sensors installed in the cars about damage to the car, pattern of driving before the incident, violation of local traffic laws, or other factors.99 Homeowners could have parametric insurance for incidents such as fires in their homes where a smart fire alarm and smart home sensors could identify the source of a fire, the resulting damage, and potentially its cause.

Moreover, the agricultural industry lends itself to the use of parametric, blockchain-based smart contract insurance. Touting the numerous potential benefits of parametric insurance to improve the welfare of smallholder farmers, increase resilience, and eliminate the need to verify

97 Id.
losses, numerous organizations have piloted index insurance programs all over the world, particularly in developing countries. However, the ability to reach smallholder farmers to make sure they can access and understand the insurance contracts currently limits scalability. Rural areas with poor infrastructure may be hard to reach with traditional methods.

The ability to market and administer blockchain-based smart contract-enabled parametric insurance policies solely through internet-connected smartphones can aid in reaching underserved populations. For example, a smartphone-based system, potentially modeled after Kenya’s M-Pesa, could be a good solution. M-Pesa is a mobile payment system that allows people to send and receive money using their cellphone. Since 2007, the technology has taken off with at least one individual in ninety-six percent of Kenyan households using it. Indeed, seventy-five percent of the unbanked population in Kenya uses M-Pesa. Elsewhere in Africa, BitPesa is using the Bitcoin blockchain to bring the M-Pesa model to other African countries and to cross-border transactions.

In sum, parametric, blockchain-based smart contracts represent not only an opportunity to digitize existing insurance products to realize efficiencies, but also open potentially untapped markets for insurance products using the benefits of newly-developed technology.

C. Smart Contracts, Insurance, UETA, and ESIGN

As noted above, we argue that blockchain-based smart contracts are enforceable under UETA and ESIGN. Specifically with respect to insurance contracts, however, these types of digital contracts are also the exact types of contracts that Congress wanted to protect under ESIGN. Insurance contracts

---


101 Id.


103 Id.

104 Id.

are specifically included in the statute.106 ESIGN, as part of its consumer protection provisions, prohibits the cancellation of life insurance policies through electronic means.107 This protection reflects the special status of life insurance as providing for one’s family after death, which has led states to protect life insurance proceeds in other ways.108 UETA does not have a similar protection, but many states have implemented similar exemptions.109 These limitations restrict the kinds of smart contracts that can be created for insurance products.

In order to take advantage of UETA and ESIGN, a blockchain-based smart contract for life insurance would not be able to cancel a policyholder’s policy upon non-payment of the premium. Instead, the cancellation notice would need to be sent via physical form. Cancellation of blockchain-based smart contract-driven life insurance policies for non-payment may be an area for further development of legal guidance under UETA and ESIGN. In addition, smart contracts need to be worded carefully to ensure that policyholders do not use them as a substitute for a will, as ESIGN and UETA would not ensure that they are valid.

Smart Contracts and the Energy Industry

The energy industry is actively examining new models and mechanisms for delivering service to customers. Likewise, customers themselves are looking for new ways to purchase energy and to understand the origins of the energy they purchase. Blockchain-based smart contracts can help accelerate two developments in the energy industry: (1) smart meters; and (2) microgrids. Blockchain-based smart contracts can provide a new, more secure basis for smart meters and, in fact, can take advantage of blockchain’s currency foundations to automate payments as well. Blockchain-based smart contracts are already enabling microgrids, and these initial efforts can point the way to broader adoption. Blockchain-based smart contracts can provide the tool to give both utilities and customers the levels of efficiency

109 See, e.g., N.C. GEN. STAT. § 66-313(e)(3).
and effectiveness that both strive for, while delivering both the consumer protections and individual choice that stakeholders often advocate.

A. Smart Meters

Retail energy provides power to customers through energy lines. The electric utility tracks a customer’s power consumption through a meter installed at the customer’s home. At the end of the billing cycle, a customer is sent a bill for their past month’s consumption.

Although this process is well understood by all parties involved, it has several drawbacks. First, by receiving a bill only once a month, it is difficult for customers to obtain immediate feedback on their energy usage. On a hot day, a customer may know that their usage will be higher, but they would not have a way of knowing exactly how much more energy they used that day compared to a regular day. For instance, they may know that keeping the house at 73 degrees will be expensive but not how much more expensive relative to keeping it at 75 degrees, which limits the ability of a household to adjust its usage on a less-than-monthly basis. If a homeowner wants to balance their comfort with keeping heating and cooling costs down, having access to this more granular level of detail will enable them make the best decision. Second, the process relies on customers being able to provide forms of identification and credit, which may be difficult for certain populations, like students and households without bank accounts. Many utilities require either a Social Security number or two forms of identification, including one with a photo.110 Even if the potential customers do have those forms of identification, they may lack access to banks or credit cards that a utility requires.111

In response, some utility companies have begun to use smart meters, which are electrical meters that wirelessly send meter readings to the utility company. This allows the company to provide a more accurate and up-to-date bill while also freeing the company from needing to send inspectors out every month to read the meters.112

111 Id.
Smart meters can go a step further, however, to allow customers to pay as they go rather than rely on monthly assessments and the credit requirements. For example, Arizona’s Salt River Project Agricultural Improvement and Power District (‘‘SRP’’) implemented a pay as you go smart meter system, M-Power, which is currently one of the largest pre-paid energy programs in the United States. Under M-Power, SRP installs smart meters in customers’ homes and allows them to use pre-paid smart cards to purchase energy. These cards can be re-loaded at pay centers across the Phoenix metro area, which includes centers that are open 24 hours a day. This system gives customers more control and flexibility over their energy bill, which is particularly beneficial for those with tight budgets, such as lower-income families or students. Customers are also more aware of their energy usage, resulting in a twelve percent reduction in electricity use of M-Power customers. With high satisfaction ratings, SRP’s customer base has also expanded from those needing more flexibility than a monthly electricity bill to include customers interested in measuring their energy use or wanting to reduce their energy use.

Blockchain-based smart contracts could build further on the pay-as-you-go smart meter concept. For example, blockchain-based smart contracts can resolve some security concerns and allow for quicker payments. A recent report noted that smart-meters are woefully insecure, using outdated encryption protocols that can be easily brute-forced. Some customers are also unable to reload their payment cards without visiting a separate payment machine, which can pose a problem if their energy runs out in the middle of the night and no pay centers are open. Finally, some consumers have protested that smart meters inaccurately measure their consumption and overcharge

115 See Neenan, supra note 113.
116 Id.
117 Id.
118 Id.
them. By contrast, blockchain-based device authentication tools can augment the security of smart meters on a blockchain-based system.

Blockchain-based smart contracts can also enhance payment processes for smart meters. Instead of relying upon payment cards that must be reloaded at a separate location, with blockchain-based smart contracts paired with smart meters, customers can arrange payments on their phones using blockchain-based smart contracts that execute when their remaining electrical power drops below a certain amount of time left. This makes it easier for customers to pay than the current system, which often requires going to a separate physical location to add to one’s balance. Blockchain-based smart contracts could also be structured so that when an external weather reporting site indicates that the next week will be particularly cold or hot, the contract would automatically add more money to the consumer’s balance to account for the expected higher usage. For some users, the assurance of knowing that they will not need to frantically add to their balance during the middle of a snowstorm or heat wave is worth paying earlier than necessary. The consumer would also benefit from having multiple smart contracts execute during what would have been a traditional monthly billing cycle. The consumer would have more immediate feedback about their energy usage and could adjust in real-time or based on pre-programmed parameters if necessary.

As noted above, blockchain technology also offers benefits of greater transparency for all participants, as well as a greater sense that rules cannot be changed unilaterally. As a result, a blockchain solution can address questions concerning overbilling. With a blockchain-based system, consumers would have direct access to an immutable record of their usage, which could be compared to historical usage or the average usage of neighbors. A user who suspects they were either overcharged or perhaps had their smart meter hacked would be able to compare their usage on an extremely granular level to the usage of their neighbors to demonstrate errors. These benefits may allow companies to reach new markets of people looking for more flexibility or who have difficulty with the traditional requirements.


B. Microgrids

Microgrids are another area of innovation in the electric industry. In the United States, the majority of people receive their electricity from coal and natural gas facilities. These facilities generate power at a central location, which is then transmitted over power lines to the end user. Although this is the dominant model for delivering power in the United States, this model presents specific risks.

For example, centralized power production creates a risk that if a plant goes offline, customers will suffer substantial loss of service. Hurricane Sandy demonstrated this problem in dramatic fashion. The hurricane left 7.9 million people without power in the Mid-Atlantic and New England areas in the immediate wake of landfall. Even a month later, one percent of Jersey Central Power & Light customers remained without power. The crippling effects of the storm demonstrated that an electrical grid relying upon a few central power plants could collapse quickly and need a lengthy rebuild. The fact that multiple storms in the previous year had knocked power out to millions of people on the Eastern Seaboard further confirmed that the electrical grid was vulnerable. For these and other reasons, the centralized grid model has been criticized in recent reports as being outdated and in need of serious upgrade.

Microgrids are a potential supplement to centralized grid systems, but may eventually replace them altogether. Rather than rely exclusively upon a power plant that produces electricity for a region, a microgrid allows residents

in the area to better manage local usage and even generate and sell power through solar panels or other alternative energy methods. The residents can use the microgrid to power their own homes or businesses, supplement their power needs from the larger grid—and if they generate extraneous power, residents can sell it either to their neighbors or back to the larger grid. Microgrids provide a backup system in case a storm or terror event disables the centralized grid. In fact, several microgrid participants cited access to a reliable backup as part of the reason that they joined the project. Microgrids may even extend power access to rural and tribal communities.

Blockchain technology is beginning to be deployed in the United States to facilitate microgrids. The most successful example so far is the Park Slope microgrid in Brooklyn, New York, with over 130 buildings participating. Although currently limited in scope, the ultimate goal is to use blockchain-based smart contracts to allow buildings that produce extra energy to sell that energy in an automated fashion to other residents on the microgrid. Blockchain-based smart contracts would be set up in such a way that when one user produces excess energy, it is automatically sold to another user in the neighborhood, which allows the neighborhood to lessen the amount of energy it draws from the central grid. Facilitating the sale of excess energy produced by one building to a building in need of energy helps reduce the overall strain on the grid, thereby preventing brownouts during times of high-energy consumption. The Park Slope microgrid has already led to reduced energy usage, as well as facilitating a better understanding amongst

128 Id.
130 DEP’T OF ENERGY, supra note 126.
132 Id.; see also BROOKLYN MICROGRID, http://www.brooklynmicrogrid.com (last visited Jan. 12, 2017) [https://perma.cc/4JV4-PGF3].
consumers regarding where the energy originates and how it is made.\textsuperscript{134} The emphasis on buying energy as needed forces customers to confront their energy usage and re-evaluate how much they are using.\textsuperscript{135}

Adopting blockchain technology in the energy industry poses its own challenges. Strict industry regulation and monopolies make it difficult to implement new technologies even with their likely benefits. For example, as a political subdivision of the state of Arizona, SRP is under different regulations from the Arizona Corporation Commission (“ACC”) than a standard utility company.\textsuperscript{136} This regulatory freedom allowed SRP to test and implement its pay-as-you-go smart meters. In this way, co-ops are also strong candidates to begin experimenting with and adopting blockchain-based smart contract technology, in a manner that can ultimately benefit the entire industry.

**CONCLUSION**

With all of the hype surrounding blockchain-based smart contracts, it is important to focus on the use cases that are both viable and valuable. Blockchain-based smart contracts should be seen as a legally binding statement under UETA and ESIGN and, therefore, available for innovation now. Moreover, the benefits of blockchain-based smart contracts are clear. Blockchain-based smart contracts provide security and resilience, an immutable transaction history, and the ability to enable micropayments, micro-transactions, and automation in an effective and profitable manner.

The insurance industry could greatly benefit from blockchain-based smart contracts, particularly for contracts that can be easily automated or broken down into “if-then” statements. This would allow the industry to reach new markets while also solving some existing problems. Blockchain-based smart contracts would reduce the need for intermediaries, copious amounts of paperwork, and cases of underpayment while simultaneously increasing efficiency and decreasing payout time. Parametric insurance may prove to be the best application of blockchain-based smart contracts in the insurance


\textsuperscript{135} Id.

industry, leading to lower transactional and administrative costs and reducing
the need for claims adjustors, which will in turn reduce premiums. With 2.5
billion unbanked people in the world, a new payment system using blockchain
could open up a huge new market of potential customers.

Another promising application is in the energy industry. Blockchain-
based smart contracts could increase the efficiency of payment systems and
energy transfer while also improving security and resilience. Customers would
also have more freedom and information on their energy usage and costs using
blockchain-based smart contracts. Microgrids will increase resilience of the
energy system, which may become more essential with severe weather
patterns or potential terrorist attacks. Blockchain-based smart contracts will
also allow people to easily sell or buy more energy depending on their usage
at any given time. With fewer regulatory barriers, co-ops may be the best
starting place for implementing these new applications within the energy
sector, to the overall benefit of the energy industry as it can observe these
experiments and take advantage of the technology as it matures.

In sum, rather than simply a futuristic science project, blockchain-
based smart contracts are real, enforceable under existing law, and able to
offer real benefits across a variety of industries.
THE LAW AND LEGALITY OF SMART CONTRACTS

Max Raskin*

CITE AS: 1 GEO. L. TECH. REV. 305 (2017)
https://perma.cc/673G-3ANE

ABSTRACT
A new technology called “smart contracts” has emerged. What makes these legal agreements innovative is that their execution is made automatic through the use of computers. This Article examines smart contracts from a legal perspective. Specifically, this Article explains smart contracts’ operation and place in existing contract law. It introduces a distinction between strong and weak smart contracts, as defined by the costs of their revocation and modification. The article concludes that smart contracts are simply a new form of preemptive self-help that should not be discouraged by the legislatures or courts. While certain unconscionable examples of strong smart contracts may need to be policed, judges and policymakers should foster a climate that treats smart contracts as another form of more traditional agreements.

ABSTRACT.................................................................305
INTRODUCTION...............................................................306
SMART CONTRACTS: STRONG AND WEAK..................................309
   Definition ..............................................................309
   Contractware ............................................................311
   The Radical History of the Vending Machine ..........................315
   Decentralized Ledgers ..................................................316
   History of the Idea and Some Preliminary Observations ............320
PLACE IN EXISTING CONTRACT LAW ........................................321
   Formation ...............................................................322
   Performance and Modification ........................................326

*At the time of writing, author was a fellow at the NYU Law Institute of Judicial Administration. B.A., New York University; J.D., New York University School of Law. For signaling purposes and for help on the paper, I would like to thank Oren Bar-Gill, Will Baude, Richard Epstein, Dan Evans, Ian Grigg, Andrew Hinkes, Mario Rizzo, Nick Szabo, David Yermack, the Mechanic’s Liens Steering Committee, the NYU Austrian Colloquium, and the NYU Law Classical Liberal Institute. All errors contained herein are my own, except any egregious ones that may exist. In that case, I blame the aforementioned for their laxity in review. Cf. D.C. Makinson, Paradox of the Preface, Analysis 25, 205-207 (1965); see also Robert Bork, The Antitrust Paradox, xvi (1978). © 2017, Max Raskin.
INTRODUCTION

Self-help is nothing new. Whether building walls to stymie trespassers or changing locks to evict squatters, individuals regularly act on their own before invoking the formal legal system. Over the past few years, a group of innovators have begun designing computer technologies that bring self-help to the realm of contracts.\(^1\) They call these new contracts “smart contracts.” Their aim is to allow contracting parties to ensure their agreement is enforced by raising the costs of any breach by a prohibitive amount.

Smart contracts are defined as agreements wherein execution is automated, usually by computers. Such contracts are designed to ensure performance without recourse to the courts. Automation ensures performance, for better or worse, by excising human discretion from contract execution.

One example of a smart contract is the humble vending machine. If the machine is operating properly and money is inserted into the machine, then a contract for sale will be executed automatically. This is a smart contract. Such a contract poses no legal problems if the machine were to dispense soda, but legal questions arise if the machine instead dispenses heroin. Should laws be passed to ban vending machines because they can be used to further illegal ends? Or should their use be regulated \textit{ex post}?\(^2\)

Certain situations will arise that will force the law to deal with smart contracts, and the purpose of this article is to assess their legality and demonstrate that there is little difficulty situating smart contracts within existing contract law. Innovative technology does not necessitate innovative jurisprudence, and traditional legal analysis can help craft simple rules as a framework for this complex phenomenon.\(^2\)

\(^1\) See infra pp. 333. Such technologies are discussed below. They range from options contracts that automatically trigger on certain conditions (“prediction markets”) to fundraising platforms that automatically disburse funds when funding thresholds are met.

\(^2\) Compare Frank H. Easterbrook, \textit{Cyberspace and the Law of the Horse}, 1996 U. Chi. Legal F. 207 (1996) (arguing that the best way to learn and craft the law of a particular field is to
The Article begins with a definition of smart contracts and an explanation of the interplay between legal prose and machines. This analysis will also engage with the existing smart contract research, which is often written from a computer science perspective. The salient features of smart contracts differ between the technical and legal discussions, a fact which is lost in the existing literature. To help clarify, the article will introduce a classification of strong and weak smart contracts. To provide context to the above discussion, a short history of the idea will be included.

Next, the two technological components that have enabled smart contracts will be explained. The first component will be termed “contractware,” which can be defined as the physical or digital instantiations of contract terms onto machines or other property involved in the performance of the contract. By instantiation, we mean taking the terms of the agreement and either writing them into previously existing software or writing them into software that is connected in some way to a machine that implements the contract. Take, for example, the innards of our aforementioned vending machine. A physical device within the machine is encoded with a seller’s offer. The machine will only dispense a soda if the terms of the agreement are met, for instance, by depositing a Krugerrand into the device. In addition to discussing the legal theory behind the vending machine, the contraption’s radical history will also be discussed to remedy the paucity of vending machine literature that exists in legal academia. This history sheds light on the power of the smart contract to protect individual autonomy over state diktat.

---

study general rules), with Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, 113 HARV. L. REV. 501 (1999) (arguing that the nature of cyberspace is unique and can reveal general principles of law); and RICHARD A. EPSTEIN, SIMPLE RULES FOR A COMPLEX WORLD, (Harv. Univ. Press. 1995) (arguing that basic legal principles can and should govern a complex, industrial society).

3 The pieces of property do not need to be tangible; software systems can be embedded with contractware.

4 The term “contractware” has appeared elsewhere to refer to commercial software offerings that facilitate the workflow and writing of traditional contracts.

5 Cf. Orin Kerr, The Influence of Immanuel Kant on Evidentiary Approaches in Eighteenth Century Bulgaria, 18 GREEN BAG 2d 251 (2015); see also Chief Justice of the United States John G. Roberts, Jr., Interview at the Fourth Circuit Court of Appeals Annual Conference (June 25, 2011) (much like how Professor Kerr’s work remedied the paucity of legal literature on the influence of Immanuel Kant on evidentiary approaches in eighteenth century Bulgaria, a paucity that was observed by Chief Justice Roberts).
There is a second technological component this article will discuss: decentralized ledgers, also known as blockchains. These are databases of information that are created by a network with no central authority. For instance, instead of a public recordation system that exists on paper files stored in city hall, a blockchain system would keep a decentralized ledger on the computers of every node running the software. It has become easier to build and enforce secure contracts without recourse to the state through the use of shared, instead of centralized, consensus-establishing mechanisms. The combination of these components—contractware and blockchains—has made smart contracts that are enforced by a decentralized, third-party network possible.

Section 2 of the Article will analyze smart contracts through the lens of existing doctrines in contract law. The section will provide an overview of the classic stages of contract formation and pose a series of observations and questions that are implicated by smart contracts. In particular, this section will discuss consideration, formation, avoidance, performance, breach, and remedy. Section 3 will explore one existing application of smart contracts: automobile starter interrupters. These are devices that are installed in cars by creditors, allowing them to remotely disable the car if a debtor has breached the terms of an agreement. The subject of this section will be how courts and legislatures have dealt with these devices. This is a current instance where courts have passed judgment on the legality of smart contracts, albeit not self-consciously. They were not setting out to rule on legality, but implicitly did so as a collateral matter.

Next, the Article will examine the benefits of smart contracts. Like many technologies, the creators and early adopters of smart contracts are ideologically driven and believe that the invention can radically alter the nature of society and its relationship with the traditional centralized state. Many believe that private enforcement of contracts can reduce the need and extent of monopolized police and legal services provided by the state.

---


7 Id. at 2, 4.

8 Other systems of verification are possible, but blockchains have become a sort of Schelling point. Attention from the media and capital have established this particular technology as the one to work with.

However, the vision of the first movers often gives way to the realities of a conservative world that looks askance at new technologies. There are, however, benefits of smart contracts that do not upend the existing social order, but instead decrease transaction costs by cutting out intermediaries. This allows for industrial society to operate more effectively. These benefits extend to financial transactions, corporate governance, financial products, and a host of other potential applications that have been analyzed by economists.

The final section of the Article discusses both a philosophical and practical set of problems with smart contracts. The benefits of smart contracts must be viewed in light of their inherent limitations. A smart contract asks its parties to tie themselves to the mast like Ulysses and *ex ante* commit to abiding by the terms of the agreement. In certain instances, the state may want to prevent individuals from committing themselves if the terms of the contract are substantively unconscionable.

**SMART CONTRACTS: STRONG AND WEAK**

*Definition*

A smart contract is an agreement whose execution is automated. This automatic execution is often effected through a computer running code that has translated legal prose into an executable program. This program has

10 HOME, THE ODYSSEY, Book XII, 36-54 (A.T. Murray trans.) (c. 800 B.C.E.), http://www.theoi.com/Text/HomerOdyssey12.html [https://perma.cc/WSP5-VGPN] (describing Ulysses’ commands that his troops tie him to the mast of his ship so that he would not be tempted by the Sirens and their alluring voices, which would have resulted in his death).

11 Alternative and broader definitions of smart contracts exist and these may be better for computer science purposes, but for legal purposes, what is relevant is the excision of human control. See, e.g., Christopher D. Clack et al., Smart Contract Templates: Foundations, Design Landscape and Research Directions 2 (Aug. 4, 2016) (unpublished manuscript), http://arxiv.org/pdf/1608.00771v2.pdf [https://perma.cc/8Z5P-QRM9] (“A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution.”). Much of the remainder of this paper will discuss under what conditions smart contracts are legally enforceable, but if they have been executed, then the agreement has been enforced in some sense. The cogs of a vending machine enforce the agreement, even if *ex post* a court finds the sale to be impermissible.

12 “Automation is generally taken to mean being executed by one or more computers.” Clack et al., supra note 11, at 3. For a discussion of this translation process see Tom Hvitved, Contract Formalisation and Modular Implementation of Domain-Specific Languages (Mar. 2,
control over the physical or digital objects needed to effect execution. Examples are a car that has a program installed to prevent ignition if the terms of a debt contract are not met or banking software that automatically transfers money if certain conditions are met. A smart contract does not rely on the state for enforcement, but is a way for contracting parties to ensure performance.

For legal purposes, I will further differentiate between strong and weak smart contracts. Strong smart contracts have prohibitive costs of revocation and modification, while weak smart contracts do not. This means that if a court is able to alter a contract after it has been executed with relative ease, then it will be defined as a weak smart contract. If there is some large cost to altering the contract in a way that it would not make sense for a court to do so, then the contract will be defined as strong.

Numerous alternative definitions of smart contracts have been proposed. In a paper outlining a template for creating standard smart contracts, Clack et al. proposed a broader definition of smart contracts that bifurcates into what they call traditional and non-traditional methods of enforcement. Clack et al. define traditional means of enforcement as those through institutions like arbitration or courts of law – these are weak smart contracts in our classification scheme, because the costs to change or revoke the contract are not high enough to proscribe courts or arbitrators from doing so. They define non-traditional means of enforcement as those through “tamper-proof” technology “with the assumption that in a perfect implementation of the system wrong-performance or non-performance become impossible.” This narrower set of smart contracts is what I deem the strong variety. The reason is that the execution of the contract can be “tampered” with by the courts in the sense that the court can alter the original intentions of the parties.

2012) (unpublished Ph.D. thesis, University of Copenhagen) (on file with author). It is an open area of research as to whether computers can actually affect this execution, but for the purposes of this paper, what poses the most novel legal questions is what happens when human legal prose and execution are subordinate to mechanical execution.

13 See, e.g., Clack et al., supra note 11; Josh Stark, Making Sense of Blockchain Smart Contracts, CoinDesk (June 4, 2016, 18:36 GMT), http://www.coindesk.com/making-sense-smart-contracts/ [https://perma.cc/37QL-6TCN].
14 Clack et al., supra note 11, at 4.
15 Id. An example of a weak smart contract would be an easily revocable money transfer between two large financial institutions where a court could simply order the transfer undone or modified if necessary.
16 Id.
From the perspective of innovators, this bifurcation makes sense because as a practical matter, technology and society are far away from the pure, strong smart contract definition this paper considers. For instance, personal service contracts are not subject to computer control.

Clack et al.’s broad definition does not capture what is unique about smart contracts from a legal perspective. The broad definition that includes instances where courts can interpret and enforce the contract is indistinguishable from a traditional contract law. If a court has power to interpret and then enforce a contract, then it is the smart actor and will abide by previous precedential rules and statutory frameworks. Traditional enforcers who are confronted with contracts that use technology, but ultimately rely on some form of alterable behavior, will be able to award damages, issue injunctions, or enforce criminal penalties to enforce their understanding of the law. For instance, consider a smart contract that requires a party to mow a lawn if funds are dispersed. And suppose the mechanism for enforcing the dispersal of funds was a sensor that measures the lawn’s average grass length. Although one side of the contract could be automatically enforced, because the behavior of the human party is alterable by a court, i.e. a court can excuse performance, the contract will not necessarily execute.

But traditional enforcers who are confronted with strong smart contracts will be helpless ex post. This is the novel situation that a legal definition of smart contracts needs to address. Unlike non-smart contracts whose performance can be stopped by the parties either voluntarily or by court order, once a strong smart contract has been initiated, by definition, it must execute. If, for instance, an individual in our above hypothetical were to install a device in his brain that would cause crippling pain if the lawn was not mowed, there is a case that the contract is in a stronger sense self-enforcing. This is the novel question posed to courts, and so this article will examine this second set of contracts. Much of this article will deal with smart contracts whose execution is contrary to governing law.

*Contractware*

Contracts are most often enforced by the parties to the contract. This is because most contracts do not end in breach and rancor, but rather in performance and completion. Modern industrial society would not be possible if this were not the case.

It is only when there is a dispute over a contract that there is a need for enforcement. Yet resorting to the court system is a resource-intensive
The opportunity to ensure performance ex ante is a preferable situation if the expected value of the costs of litigation outweigh the expected value of the contract. Because litigation can be a resource-intensive undertaking, the rise of contractware qua enforcer could be a welcome possibility.

I will define contractware as the physical instantiation of a computer-decipherable contract. The terms of many contracts can be written in programming languages that are communicated to a machine. The reason for this is that performance and enforcement of a contract essentially boils down to conditional statements, which are foundational to computing.

For example, in a secured auto loan, if a certain amount of money is not received by a certain date, then the car can be repossessed. While many contracts are certainly more complex, at base, conditional statements stand behind all enforcement. Whether interpreting private contracts, statutes, or the Constitution, American courts take a series of inputs, run them through a series of conditionals, and then have an executor to enforce their output. For instance, if a city tried to segregate its schools, a court would run this factual

---


20 Computers take inputs and apply functions to them to derive outputs. John McCarthy, Recursive Functions of Symbolic Expressions and Their Computation by Machine, Part I, 3 COMM. ACM 184 (1960).

21 As a theoretical matter, perhaps not all conditionals in law can be reduced to code, but parties can certainly reduce many conditionals to code, and where they cannot, they should not consider using a smart contract.
input through the conditional of Brown, *viz.* if segregation, *then* enjoin, and have someone enforce the output.\textsuperscript{22}

It is important to mention that the instantiation of the contract need not be in a physical piece of property or hardware, but can instead be in another piece of computer code. For instance, a bank account could include contractware that interacts with the bank’s systems. As an example, such contractware could commit a buyer to send money to escrow once certain external conditions were met. Automatic payment of credit card bills, such as the service offered by Chase, are already in operation.\textsuperscript{23} As a technological matter, until the advent of computers, it was difficult to use contractware. This left a larger role for courts and their agents to enforce contracts. Now, however, with increased digitization and the so-called “Internet of Things,” the feasibility of installing contractware has increased dramatically.\textsuperscript{24}

On the above view, the enforcement of a contract is nothing more than the running of a circumstance through a conditional statement. The central question to ask is: who runs the conditional statement? The most common and least disputed enforcement of a contract comes from the parties themselves. Take the contract, “Max agrees to buy Whiteacre from Richard for 500 Krugerrands.” The conditional can be written “If Max pays Richard 500 Krugerrands, then Richard will sign a piece of paper granting Max legal title to Whiteacre.” In most instances, Max gives Richard 500 Krugerrands and Richard then signs the document granting him Whiteacre. The parties themselves interpreted and enforced the contract.

\textsuperscript{22} Admittedly, equitable doctrines complicate matters and nebulous judicial standards, such as “with all deliberate speed” and “rational basis,” escape formulaic application, likely by design. But outside of the realm of constitutional law, courts tend to value the law “be settled than that it be settled right.” Burnet v. Coronado Oil & Gas Co., 285 U.S. 393, 406 (1932) (Brandeis, J., dissenting).

\textsuperscript{23} Cf. CHASE, ONLINE SERV. AGREEMENT, https://chaseonline.chase.com/Content.aspx?ContentId=COLSA1A_LA (last visited Feb. 6, 2017) [https://perma.cc/76BC-6ZWJ] (“Some Chase Loan and Credit Accounts will allow you to set up automatic payments. Automatic payments differ from repeating payments in that automatic payments are triggered based on the associated billing date and the payment amount may vary each month. Terms and conditions for automatic payments to Chase Loan and Credit Accounts will be presented to you at the time you set up the payments.”).

\textsuperscript{24} For example, even refrigerators can now connect to the Internet. See, e.g., Folasade Osisanwo et al., *Internet Refrigerator – A typical Internet of Things (IoT)*, 3 INT’L CONF. ADVANCES ENG’G SCI. & APPLIED MATHEMATICS 59 (2015), http://iieng.org/images/proceedings_pdf/2602E0315051.pdf [https://perma.cc/R9BB-DYJ9]. Consider a world where HVAC systems are connected to the internet. Smart contracts can be used to ensure payment and services altered if customers are in default.
When things go wrong, however, a third party can be invoked to interpret and enforce the conditional statements. The most familiar example of such a third party is a common-law judge using his legal reasoning combined with his sheriff to physically enforce the output of the conditional statement. At base, the judge is nothing more than a computer who applies a series of rules to a set of facts and then instructs others to enforce his output.\(^{25}\)

But judicial enforcement of contracts is not the only way that contracts can be enforced. Instead of having a judge interpret and enforce the statements, it is possible to have a machine do so. Such a machine would need to have two abilities. First, it must be able to render correct outputs from given factual inputs. Second, its output needs to be reified some way in the real world. The vending machine is the archetypical example of a self-executing smart contract. Vending machines have been defined as “self-contained automatic machines that dispense goods or provide services when coins are inserted.”\(^{26}\) In other words, they complete one side of a contract once unilateral acceptance in the form of money tender has been effected.\(^{27}\)

The contract at its most essential can be written in the following way: “Seller agrees to release one can of Dr. Brown’s Cel-Ray Soda if Buyer inserts one Krugerrand into this vending machine.” The Seller here is not the vending machine, in contradistinction to our Whiteacre property sale, where Richard was the Seller. Instead, the Seller is effectively outsourcing the contract execution, with the vending machine merely acting as his third-party distribution agent and enforcement mechanism. Buyer inserts his Krugerrand, and vending machine performs by releasing one Cel-Ray Soda.

During the transaction, the computer inside of the vending machine is presented with a factual situation, \textit{i.e.} the insertion of a Krugerrand and selection of Cel-Ray as the Buyer’s choice. Next, the vending machine applies


\(^{27}\) This is not to say that contracts cannot be executed without computers. In a world without vending machines, in the vast majority of instances, a seller would give the soda once money has been tendered. But introducing humans into the equation does introduce some uncertainty and cost. By some measures, employee theft accounts for over $40 billion a year in the United States. \textit{See} Anne Fisher, \textit{U.S. retail workers are No. 1 . . . in employee theft}, \textit{FORTUNE} (Jan. 26, 2015), http://fortune.com/2015/01/26/us-retail-worker-theft/ [https://perma.cc/7F86-G8D3]. The courts would be needed to rectify this, but as mentioned, the costs of litigation, especially for these relatively small amounts (they are likely to be small by their very nature) make such litigation prohibitive.
the contractual rules to the instant case, leading to a judgment output, *i.e.* dispensing one Cel-Ray Soda, which is the benefit of the bargain. The computer then directs the physical mechanisms of the vending machine to enforce the contract between the Buyer and the Seller. Had the factual situation been slightly different, for example Buyer inserted a penny, then our computer-judge would have rendered a different output and would have directed the vending machine to a different action, *i.e.* returning the penny without dispensing the Cel-Ray Soda.

One reason for the existence of contractware may be the lowering of costs through the ensuring of performance without recourse to the courts. As we will be shown now, another reason may be the subordination of state authority to individual autonomy. The vending machine demonstrates this clearly in both its utilitarian and utopian purposes.

*The Radical History of the Vending Machine*

The first known reference to a vending machine came in 215 B.C. in *Pneumatika*, a book by the Greek mathematician, Hero. In it, he detailed a machine that dispensed holy water for use in Egyptian temples. The user would put a coin in a particular spot, which would trigger a lever that opened a valve that dispensed the water. Fear of divine retribution would combat the use of fake coins.

Although coin-activated snuff and tobacco boxes were used in England in the 17th century, one of the most conceptually important early uses of vending machines was as a means of evading censors. The British bookseller, Richard Carlile, invented a book-dispensing machine so as to avoid prosecution under the country’s libel and sedition laws. He had been jailed previously and wanted to avoid any future liability, so the idea was to make it impossible for the Crown to prove that any individual bookseller

---

28 The lowering of transaction costs does not mean their abolition. When vending machines malfunction a typical self-help remedy is to pound the machine with a fist in the manner of Fonzie. A manufacturer’s allowance of this remedy may lower the cost of enforcement by avoiding the courts, but it may also increase the risk of illegitimate whacks to the machine. The point here being that so long as self-help is a less costly alternative than judicial recourse, it is a worthwhile alternative.


30 See Segrave, supra note 26, at 4.

31 Id. at 5.

32 See id.
actually sold the blasphemous material. He argued that it was purely a contract between the buyer and the machine with the publisher having no formal involvement.

Here is Carlile’s description of the machine as it appeared in The Republican:

Perhaps it will amuse you to be informed that in the new Temple of Reason my publications are sold by Clockwork!! In the shop is the dial on which is written every publication for sale: the purchaser enters and turns the hand of the dial to the publication he wants, when, on depositing his money, the publication drops down before him.

The Crown, however, was not amused. Use of the device was ineffective and both Carlile and his employee were convicted of selling blasphemous literature through the device. Although unsuccessful in this instance, the vending machine demonstrated its ability both to help achieve political and economic ends. The fact that Carlile flaunted his attempts to evade prosecution would make this an easy case for the court, but this article—discussed below—will deal with the theoretical question of how a court should approach a less flagrant smart contractor. Before moving onto this question, a second technological advancement will be highlighted.

Decentralized Ledgers

As mentioned above, contractware solves the problem of performing contracts by eliminating the human element ex post. From a technical sense, if nothing intervenes to prevent the machine from working, then, by definition, it will ensure performance. Yet a machine owned by one of the parties of a contract does not solve the problem of interpreting or writing the contract. The problem, briefly stated, is that an independent third party must interpret the

33 Id.
35 See SEGRAVE, supra note 26, at 5.
36 Opposition to the Crown’s system of licensure and seditious libel laws were some of the driving forces behind the First Amendment. MICHAEL PAULSEN ET AL., THE CONSTITUTION OF THE UNITED STATES 839-49 (2d ed. 2013).
contract in accord with the intentions of the parties.\textsuperscript{37} This is a problem that public courts often try to solve. Another solution to this problem is blockchain technology.

A blockchain is a decentralized collection of data that is verified by members of a peer-to-peer network.\textsuperscript{38} The concept most famously arose in the context of Bitcoin, where the data collection is a ledger of time-stamped financial transactions.\textsuperscript{39} The Bitcoin blockchain, like all others, is a solution to the double-spend problem, a variation of the above problem of human interpretation and the possibility of judging one’s own case.\textsuperscript{40}

Modern industrial society requires trust. As an example, Americans generally trust that corrupt officials have not doctored the state’s real property records. If a malicious county clerk were to forge a deed, it could cause all sorts of problems for \textit{bona fide} property owners. Although this is not a huge problem in the developed world – indeed, our world is developed \textit{because} this is not a huge problem – in countries with less of a commitment to the rule of law and property rights, property recordation is a problem. Citizens in other countries do not have such trust.\textsuperscript{41}

Another example of faith that is placed in centralized institutions is in the banking system. Americans generally trust our banking institutions to keep an accurate reading of the balance on our checking accounts. While these banks have redundancies in the form of backup servers, they are still centralized institutions and, in some sense, judges in their own cases until brought before a court. If a bank asserts an individual has a balance of $1,000

\textsuperscript{37} This is not to say that courts try to divine out party intent to the exclusion of the text of the contract, but rather contract law is about agreements between autonomous parties whose intentions are the foundation of the agreement.

\textsuperscript{38} For an explanation of the mechanics of a blockchain, see Rainer Böhme et al., \textit{Bitcoin: Economics, Technology, and Governance}, 29 J. ECON. PERSPECTIVES 213, 213-238 (2015).

\textsuperscript{39} See Nakamoto, supra note 6, at 2, 4.

\textsuperscript{40} See Jaap-Henk Hoepman, \textit{Distributed Double Spending Prevention}, ARXIV (2008), https://arxiv.org/pdf/0802.0832.pdf [https://perma.cc/PSX3-MG4D] (describing double spending as “the risk that many copies of the same bitstring are spent at different merchants.”).

and the individual claims a balance of $10,000, then a third party is likely needed to adjudicate the dispute.

This is what blockchains seek to solve: the problem of establishing consensus without the need for a centralized repository of information. Blockchains are decentralized collections of data. The unit of a blockchain is a block, which contains certain information, such as credits and debits or property ownership. A block is verified by a large number of computers in a network, called nodes, and then tacked on to the previously verified blocks. This chain of data blocks is known as a blockchain.42

A well-known blockchain is the Bitcoin blockchain; it encodes data that has a market capitalization of $9 billion as of August 28, 2016.43 The data stored on each block consists of transactions, which are debits and credits to bitcoin accounts. “Murray paid Reuben 10 bitcoins on March 2 at 4 p.m.” is an example of a transaction that would be recorded on the bitcoin blockchain.44 That block of data would then be verified by a large number of nodes and then tacked on to the previous chain, so that the blockchain would be one block longer. As it currently exists, the Bitcoin network has amassed the world’s largest amount of computing power.45

What makes the Bitcoin blockchain novel is that it relies on a decentralized network to verify the data as valid according to a set of shared rules. Information already contained in a verified blockchain cannot be overwritten without reaching consensus with the entire network to propagate the altered information. So, while this is not to say that the invalid data cannot be posted, a strong effort is needed to do so.46 In the case of a single

42 See generally Böhme, supra note 38.
44 The block would not include the proper names “Murray” and “Reuben”, but rather their public addresses. One such public address is: 15KGAfhff1B15nsrhbLYHH9WpHvpCaKPK5.
bookkeeping instrument, all a malicious actor would have to do to credit himself a million dollars would be to gain access to the instrument. The security of the Bitcoin blockchain and other blockchains is beyond the scope of this Article. Although this has been borne out by recent history, it is an assumption of this paper that individuals will trust blockchains.  

The implications for the smart contract are that terms of the contract and the state of facts relating to the performance of the contract can be programmed into a decentralized blockchain that cannot be overridden by any individual malicious or mistaken node. If millions of computers verified that “Murray paid Reuben $100 on March 2 at 4 p.m.” and these computers are disinterested and do not make computational mistakes, then one can assume with an exceptionally large degree of certainty that Murray did, in fact, pay Reuben $100 on March 2nd at 4 p.m.  

The implications are vast. Stock recordation, corporate governance, and auditing have all been proposed as areas where blockchains can increase efficiency. Whether the benefits of adopting blockchains outweigh the costs of doing so is beyond the scope of this article.

The starter interrupter combined with a decentralized ledger offers a powerful example of the combination between these two technologies. Instead of programming the contractware so that its inputs and outputs are determined and executed by the creditor’s software, a car’s contractware can be programmed so that its inputs and outputs are determined and executed by a neutral blockchain. Suppose the relevant term of the contract is that “If Murray does not pay Reuben $100 by March 2nd at 4 p.m., then Murray’s car will be rendered immobile, and Reuben can repossess.” The contractware will search the blockchain for such a transaction, and if it finds it, will allow the car to start. If it does not find such a transaction, it will prevent the car from starting. Neither of the parties must trust the other for the contract to be performed. They must trust the disinterested blockchain, which is capable of enforcing the relevant terms.

---

48 It is possible to nearly instantaneously transfer from U.S. dollars into bitcoins, such that there is an identity between $10 and some amount of bitcoins that would actually be recorded on the blockchain or in the records maintained by the provider of the merchant service.  
The contractware reifies the terms of the contract in such a way that technology can compel performance. The decentralized ledger ensures that such contractware operates in an independent manner, free from the problems of self-help. It therefore makes sense to call it a smart contract because it is able to do more than a traditional contract. It can endogenously enforce an ex ante bargain (contractware) and can also allow neutral, third-party enforcement (decentralized ledger).

History of the Idea and Some Preliminary Observations

Smart contracts have existed long before they were consciously described as such. They are the result of human action, not human design. This means that contracting parties were incentivized to lower costs without consciously heeding the advice of academics. Smart contracts were first described by lawyer and technologist, Nick Szabo, in 1997. Szabo defines smart contracts as contractual clauses embedded into hardware and software in such a way that makes breach more expensive. He provides two examples: vending machines and devices for repossessing automobile-collateral. By decreasing the costs of mediation, self-enforcement, and arbitration, Szabo saw smart contracts as representing a fundamental shift in the world away from paper and towards digital systems, like the banking backed by computers and digital databases. This shift was not to take place immediately, however, as Szabo recognized the value of the “long history” of paper.

---

50 ADAM FERGUSON, AN ESSAY ON THE HISTORY OF CIVIL SOCIETY 305 (5th ed. 1767).
51 Example of smart contracts throughout history abound. See infra pp 309-11. More contemporary uses include subway tokens, bike sharing programs, and E-ZPass.
53 See Szabo, supra note 18. (“The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher.”).
54 Id.
55 Id.
Long before Szabo, however, financial institutions were using computer code to facilitate transactions, like options contracts and bookkeeping. The real breakthrough for smart contracts came with the advent of Bitcoin and the proliferation of blockchain technology. First proposed in 2008, the Bitcoin protocol was a successful experiment in the mass usage of decentralized ledgers, which form an important basis of smart contracts.

The proliferation of decentralized ledgers led to a new discussion of using technology to enforce agreements between individuals without recourse to third parties. New companies and protocols have aggregated the essential code to write smart contracts. This code exists apart from the Bitcoin ecosystem. These new companies are building an ecosystem for experimentation with an implementation of smart contracts. There has been a proliferation of writing about the subject, mostly from a technical or financial perspective.

PLACE IN EXISTING CONTRACT LAW

A contract is a legally enforceable agreement. The novel issue of smart contracts is what happens when an agreement can be enforced not by public law enforcers, but through the terms and mechanisms set forth in the terms of the contract itself. The typical legal action for breach of contract involves an aggrieved party going to a court of law or equity to demand


59 See Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015) (unpublished manuscript), http://ssrn.com/abstract=2580664 [https://perma.cc/2UGR-ZFFF] (describing and analyzing the benefits and drawbacks of decentralized technology, and predicting the rise of a Lex Cryptographia, which they define as “rules administered through self-executing smart contracts and decentralized (autonomous) organizations.”).

60 RESTATEMENT (FIRST) OF CONTRACTS § 1 (1932).
money damages, restitution, or specific performance.\textsuperscript{61} With a smart contract, the aggrieved party will need to go to the court to remedy a contract that has already been executed or is in the process of being performed. This is because, by definition, a strong smart contract is already executed or in the process of being executed by the time the court hears the case. So the remedy must come after the fact to undo or alter the agreement in some way.

The three phases of contract law this section will address are formation, performance, and breach. Each of these phases will be covered to understand how these new contracts can be placed in the context of traditional doctrines and concepts.

\textit{Formation}

The initial stage of a contractual agreement is not markedly different between smart and traditional contracts. This is because before any contractware can operate, two parties must agree to some set of terms that initiates the program.\textsuperscript{62} In the realm of smart contracts, unlike traditional contracts, acceptance comes through performance. An individual can say they will initiate a smart contract, which may be a contract in regular law, but until the program initiates, there is no smart contract. Smart contract code can be posted to a ledger as an offer though. Once an action is taken to initiate acceptance, such as by ceding control over a certain amount of money to the code, the contract is formed.

Just as there is bargained-for consideration in a traditional contract, there is consideration in a smart contract. One of the reasons for have the doctrine of consideration is that courts believe that mutuality of obligation distinguishes a contract from a gift, for which parties do not have the same rights of legal enforcement.\textsuperscript{63} As will be shown below, where a gift induces action, that action can serve as a substitute for consideration.\textsuperscript{64} Smart contracts have the potential to formalize the instances where courts will allow contracts

\textsuperscript{61} Id. at § 326.
\textsuperscript{62} Id. at § 3.
\textsuperscript{63} Val D. Ricks, \textit{In Defense of Mutuality of Obligation: Why "Both Should Be Bound, or Neither"}, 78 NEB. L. REV. 491, 494 (1999) ("Courts have held a promise traded for another promise to be enforceable for well over 400 years, since the early to mid-1500s. Courts currently say that a mutual (or reciprocal, or bargained-for) promise constitutes consideration for a promise, causing it to be enforceable.").
\textsuperscript{64} Id.
to be enforced. This is because the terms of the smart contract are explicitly laid out and each side’s obligations and benefits are immediately apparently.

In a contract, the bargain can be presented unilaterally, like a vending machine, or can be bargained-for as in the terms of a loan agreement. But what happens in a smart contract when there is no consideration? A foundational contracts case will be analyzed through the lens of both traditional and smart contracts.

In *Ricketts v. Scothorn*, a grandfather promised to his granddaughter a sum of money, inducing her to quit her job. The grandfather dies and the executor of the estate refuses to pay her. The granddaughter brought an action against the executor of his estate, claiming that she relied on the grandfather’s promise. The court held that the daughter could recover money damages because she detrimentally relied on the promise of her grandfather.

But imagine a situation where the grandfather wrote into the gift-promise code that he or his estate could retain the right to change his mind or explicitly wrote into the code that he or his estate could not change his mind. This would be done using a smart contract. In this instance, it would be impossible for the grandfather to change his mind if the computer program did not allow for a change. The grandfather then writes the terms of this gift-promise into computer language that is readable by his bank including terms that do not allow for revocation.

An ability to write into the code options to change one’s mind or the mind of one’s assignees would make the doctrine of detrimental reliance less important because recipients of gifts could demand that their gifts come with a promise of finality; thus, the ability to recant the promise becomes a disclosed term of the contract. In *Ricketts*, it is likely that the grandfather would have happily tied his executor to the mast. If the counterparty did not give this additional promise in the code, then the gift recipient would be able to act accordingly; if the counterparty did give the promise, rights are more clearly defined.

Smart contracts solve the problem of gift-promises by giving both the promisor and promisee the ability to encode finality so that parties can organize their behaviors around a mechanical certainty or lack thereof.

---

67 *Id.*
Instead of going to court to ask the state to enforce the contract, the parties can agree to a cheaper enforcement mechanism. This is the method by which smart contracts reduce transaction costs. In the realm of wills and estates, like in \textit{Ricketts}, smart contracts can be of particularly high value because they will bind the hands of the executor to the will of the testator, with little room for deviation.

Some of the most difficult problems of early contract law involved defenses of misunderstanding and mistake.\footnote{See, e.g., E. Allan Farnsworth, "\textit{Meaning} in the Law of Contracts, 76 \textit{Yale L.J.} 939 (1967); E. Allan Farnsworth, \textit{Precontractual Liability and Preliminary Agreements: Fair Dealing and Failed Negotiations}, 87 \textit{Columbia L. Rev.} 217 (1987).} With respect to interpretation, the use of computer code has the potential to minimize future conflicts over terms.\footnote{This potential is not certain, as examples of fraud abound in the world of computer code. We discuss the DAO incident is discussed below, infra p. 336. Much like contracts of adhesion, many lay individuals will not comb through the code of their contract. But like open source software, granting everyone access to potentially review the code is a strong bulwark against fraud. Code can minimize, but not completely erase these problems because humans and their misunderstandings of code could provide a basis for contract rescission.} In \textit{Raffles v. Wichelhaus}, a controversy arose over a cotton shipment contract when two ships named Peerless could both fulfill the terms; one party claimed he intended one ship, the other party, the other.\footnote{\textit{Raffles v. Wichelhaus}, 2 H. & C. 906 (1864).} Such problems are virtually non-existent now, at least in the shipping world, but for similar problems that may exist, the precision of cryptographic identifiers is able to dispatch with such issues.\footnote{David Wu et al, Privacy, Discovery, and Authentication for the Internet of Things (Feb. 28, 2017) (unpublished manuscript), https://crypto.stanford.edu/~dwu4/papers/PrivateIoTFull.pdf [https://perma.cc/PXQ6-ZGMY].} Although ambiguity certainly exists in programming languages, these ambiguities are less than in the real world because of the fact that there are simply fewer terms that a computer can recognize than a human can recognize.\footnote{While computer code is subject to the same human error that written language is, it is much less subject to uncertainty. Two humans may read the same words and ascribe different meaning. Two compatible computers reading the same piece of code will not, although that code may not be the “correct” code that was meant to be written by the programmer; average adults have a vocabulary of between 20,000 and 35,000 words. \textit{See Vocabulary size: Lexical Facts}, \textit{Economist} (May 29, 2013), http://www.economist.com/blogs/johnson/2013/05/vocabulary-size [https://perma.cc/UQV4-3W32]. Because computer programs are written by humans, anything a human can write into code, a human can at least recognize as a word or signifier.}
Ambiguity is celebrated in human language. It is a central feature of literature, poetry, and humor. Ambiguity is anathema to computer language. An ambiguous computer language is a nonsensical concept because the predictability of computers is what gives part of their value; imagine a computer that was asked, “what is 1 and 1” it randomly returned either “two” or “11”. Although it is debatable whether every contract can be translated into machine language, many of them can be.\footnote{See, e.g., Ian Grigg, The Ricardian Contract, IANG, http://iang.org/papers/ricardian_contract.html (last visited Apr. 1, 2017) [https://perma.cc/8PS3-YCLP].} When lawyers or the programmers they hire write contracts in code, there is less of a chance for ambiguity than in natural language if only for the simple fact that artificial language must be complete and predefined, whereas natural language is infinite.\footnote{See Carl A. Gunter, Semantics of Programming Languages: Structures and Techniques, 4 (“Perhaps the most basic characteristic of the distinction is the fact that an artificial language can be fully circumscribed and studied in its entirety.”); John W.L. Ogilvie, Defining Computer Program Parts Under Learned Hand’s Abstractions Test, 91 Mich. L. Rev. 526 (1992), http://digital-law-online.info/misc/ogilvie.htm [https://perma.cc/58SG-HC6U].} That is to say a person can walk around and verbally recite lines of code and people can at least understand what he is saying; a machine cannot understand human language that it is not programmed to understand. All of this is simply to say that the problem of ambiguity is reduced in the smart contract context.

Finally, all of the usual defenses to formation of a contract also apply in the realm of smart contracts, although as will be seen later, enforcing the remedy against a strong smart contract may prove problematic to a court. Take unconscionability and illegality, for instance. If a vending machine were to sell alcohol to minors or sell alcohol in a dry jurisdiction, then the contract could be voided as illegal.\footnote{Modern Cigarette, Inc. v. Town of Orange, 774 A.2d 969, 970–71 (Conn. 2001).} As will be discussed, the remedies will be either \textit{ex post} through legal action or \textit{ex ante} through regulation. In this instance, the illegal contract can either be policed through a prohibition on alcoholic vending machines\footnote{Or a prohibition on filling the vending machines with illegal substances.} or a system of preclearance where a driver’s license scanner or some mechanism are required to ensure compliance with age requirements. Similarly, suppose the vending machine charged $1,000 for a can of Coke and a court were to find this to be substantively unconscionable. The remedies would again either be in damages or in policing the use of such vending machines before the contract could be formed.
Because the possibility of policing and damages exist, the issues of contract formation are largely the same in the traditional and smart contract world. The main difference is in the precision with which terms can be defined and inserted. Ambiguities must be taken care of by a functioning program and there is no “I do not know.” The history of computing shows that programs do not always operate as their designers expect, but when code is executed, the code does operate.\textsuperscript{77} Although the actual output of a smart contract may differ from the intentions of the parties, this system provides a more optimal first approximation. This is because computer code can be predicted according to a set of rules, whereas the ambiguity in human interpretation is less robotic by definition.

\textit{Performance and Modification}

A contract can be performed, modified, or breached. This section addresses performance and modification issues.

The performance phase is made easier with smart contracts as they offer a tool to solve ambiguity problems addressed above. A potential problem here, however, comes with imperfect performance. Courts in the United States do not demand perfect performance for a contract to be recognized and enforced.\textsuperscript{78} The common law doctrine of substantial performance permits a contract to be recognized even if the performance does not fully comport with the express terms laid out.\textsuperscript{79} This is the kind of leeway that a computer program cannot recognize because it involves an outcome that was not contemplated and specified by the parties. Imagine, for instance, a contract for a painting that is contingent on the reasonable personal satisfaction of the buyer. One way parties can deal with this is by baking in a certain degree of discretion into the terms of the contract initially or by simply not using a smart contract if discretion is a necessary part of the contract. However, if the terms were to diverge from what the law recognizes, the law would have to again decide between \textit{ex ante} and \textit{ex post} solutions to the problem.

Most conceptually challenging, however, is how smart contracts will deal with modification. The law recognizes certain excuses that will absolve a

\textsuperscript{77}This is true of human contracts too, at least in the sense that something always happens. But with code these happenings are predetermined and predictable and therefore parties can have certainty to organize around.

\textsuperscript{78}See \textsc{Restatement (Second) of Contracts} § 237 cmt. d (1981).

\textsuperscript{79}Id.
party from performance or require some sort of modification.\textsuperscript{80} Impossibility and impracticability are two such excuses. When a contract becomes illegal after it is formed, then the parties can be excused from performance and there is generally no remedy for an aggrieved party.\textsuperscript{81} This poses a problem for the smart contract.

There needs to be a method by which smart contracts can be updated to incorporate changes that may be required by the evolving legal landscape. Suppose that at the time of contract formation, the time a debtor needs to be in default for the creditor to repossess is 30 days and that after the contract is executed, a legislature changes the law requiring that time period to be 90 days.\textsuperscript{82} There are numerous ways of addressing this situation, ranging from state-backed to purely private. One method could be a system in which the relevant jurisdiction creates a publicly available database and application programming interface (API) of relevant legal provisions. These would be provisions related to the terms of the contract. The smart contract would call these terms and would be able to update those provisions terms in accord with the jurisdiction’s update of the database.\textsuperscript{83}

Another method would be through ex post policing of the parties; this puts the burden on the parties or their agents to update the code. The benefit of this option is that there is no need to rely on the third-party government to create a new infrastructure, while the downside is that the parties themselves can potentially unilaterally change the terms of the contract, which is one of the problems smart contracts try to rectify. This could be obviated by leaving certain terms of the contract modifiable, while restricting others from modification. That payment is necessary could be an immutable term, whereas the length of time a debtor has before he is in default could be modifiable. This suggests that government API’s may have a master override over contract terms, which reflect the application of prevailing law over contracts in certain circumstances.\textsuperscript{84}

Finally, computer programs are regularly written with the option of inserting code later. Only those contracts that would involve some kind of

\textsuperscript{80} See, e.g., \textit{Restatement (First) of Contracts} § 456 (1932).
\textsuperscript{81} See \textit{id.} at § 598.
\textsuperscript{82} Other examples of changing provisions include retroactive protection for veterans against foreclosure. \textit{See, e.g.,} 50 U.S.C.A. § 3958.
\textsuperscript{83} Updating the code of a smart contract is a technically difficult task, but for the purposes of this paper, it will be assumed that it will become possible.
\textsuperscript{84} Further, a similar override can be installed as between federal and state governments, as the software of the Supremacy Clause. \textit{U.S. Const.} art. VI, cl. 2.
irrevocability would force courts’ hands. This is because a court would be tasked with enforcing a law that would override the terms of the contract; there would be conflicting dictates. Party autonomy does not trump all other values in state-based legal systems.

*Enforcement, Breach, and Remedies*

The central problem in the final question of contract law is what happens when the outcomes of the smart contract diverge from the outcomes that the law demands. Above are numerous examples where the technical outcome of the smart contract would not be permitted by a court under existing law, *e.g.* the heroin vending machine.

As a threshold, it is possible that contract law and the actual written contracts would have influence on each other so as to minimize these divergences. Courts are going to be more likely to enforce smart contract terms because the courts will have more certainty as to party intent because the parties explicitly laid out their terms. Smart contracts drafters are going to be more likely to write smart contracts that comport with extant law and write terms that are variable to accommodate future changes in the law. The terms of a lease, for instance, will change to accommodate the property law of the jurisdiction. Additionally, torts could emerge for negligent coding or negligent update that would further ensure smart contracts are drafted in accord with existing legal standards. But what happens when these forces are not enough to overcome the divergence?

It is a good rule of thumb that the entity with more guns wins. Here, governments generally have more guns than private parties and so the state’s courts are in a position of enforcing their law over the private law. Enforcement either occurs before or after the damage has occurred. This damage is not to either of the contracting parties because they are getting, by definition, their bargain.\(^{85}\) Instead, the damage is done to the exogenous laws of the society and not the parties themselves.\(^{86}\) If two parties contract to buy liquor, both are satisfied with the bargain ex ante. If one of those parties is below the drinking age, he is still satisfied with the bargain. The only one ex

\(^{85}\) It may be the case, as with the decentralized autonomous organization, that the parties regret their decisions ex post. But in their agreement, the code was the code they signed on to.

\(^{86}\) Damage may also be done to efficiency—smart contracts prohibit or make more costly efficient breach.
ante not satisfied is the government and the government is in a position to respond to that dissatisfaction in some way.

In the United States and other common law systems, *ex post* enforcement is the preferred system and there are many reasons to believe why this is a system conducive to greater prosperity and vibrancy. In the sections below this article will discuss the merits of these two positions, but here it suffices to say that the two likely categories are regulation/policing and criminal/civil actions. There is a spectrum on which these remedies should be offered. In the United States, it is the exception that the government bans certain objects because their possession is per se problematic for society. Automatic weapons and child pornography both fall into this category. If the government does not take this tack, then it is largely left with ex post enforcement.

Some unenforceable contracts result in criminal prosecutions, while some result in non-enforcement. It is too speculative at this point to see how the governments will respond to smart contracts because these technologies have yet to reach a level that requires a government response. They may not reach this level because individuals may not want to change their current contracting patterns because they are fine with the level of leeway and ambiguity that currently exists. It is unlikely, for example, that individuals will want to implant mini-bombs in themselves to ensure compliance with credit card payment. Because egregious bargains like those using the mini-bomb are unusual, it is likely that responses to unenforceable private contracts will remain in the *ex post* phase and tend towards civil, not criminal enforcement.

It will be helpful to solidify the above discussion in a law that is embryonic, but at least extant: starter interrupters.

**CASE STUDY: STARTER INTERRUPTERS**

The existence of a public court system is the antithesis of private self-help because the parties seek external recourse from a third party. There are reasons for this, including a desire to prevent might from making right. But

---

89 See *Restatement (Second) of Contracts* § 178 (1981).
90 For a discussion of self-help see *infra* p. 333.
91 Cf. Kirby v. Foster, 22 A. 1111, 1112 (R.I. 1891) (“The law does not permit parties to take the settlement of conflicting claims into their own hands.”).
recourse to courts is not without its costs.\textsuperscript{92} Forcing a landlord to go through a lengthy eviction process raises the costs for non-breaching tenants, for example.\textsuperscript{93} The situation is similar to when automobiles are collateral. In an attempt to increase recovery rates for their collateral, automobile lenders have turned to using devices called starter interrupters.\textsuperscript{94}

Starter interrupters are an archetypical example of a smart contract and how the law deals with them is instructive in crafting appropriate legal regimes. A starter interrupter is a device that is installed in an automobile that allows for a remote party to prevent the engine from starting.\textsuperscript{95} It allows a user who controls the starter interrupter to remotely shut off an automobile. These devices often also include global position systems, so that the collateral can be located.\textsuperscript{96} The New York Times reported on an Arizona company, C.A.G. Acceptance Corporation, which offers its automobile loans on a condition that if the debtor is in default, the company reserves the right use the device to prevent the car from starting.\textsuperscript{97} Such devices are estimated to be installed in over two million automobiles.\textsuperscript{98}

There are a number of safeguards to the power of the starter interrupters that companies use to ensure that there are not egregious problems

\textsuperscript{93} \textit{Cf.} Berg v. Wiley, 264 N.W.2d 145, 148 (Minn. 1978) (awarding tenant $31,000 for lost profits and $3540 for lost chattels resulting from a wrongful lockout).
\textsuperscript{94} See Michael Corkery & Jessica Silver-Greenberg, \textit{Miss a Payment? Good Luck Moving That Car}, N.Y. TIMES DEAL BOOK (Sept. 24, 2014), https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_r=0 [https://perma.cc/ZK4J-J96R] (This is not technically a smart contract because the creditor here has discretion, but as the technology proliferates and this becomes automated, the salient features are the same in this nascent state, so it is an appropriate case study.).
\textsuperscript{96} Id.
\textsuperscript{97} Corkery & Silver-Greenberg, supra note 94.
\textsuperscript{98} Id.; see also Sydney Ember, \textit{Morning Agenda: Devices Fuel Subprime Auto Boom}, N.Y. TIMES DEAL BOOK (Sept. 24, 2014), https://dealbook.nytimes.com/2014/09/25/morning-agenda-devices-fuel-subprime-auto-boom/?_php=true&_type=blogs [https://perma.cc/J68M-E6B9]. The analogy to the housing crisis is inapt because the marginal loans given out are based solely on the new ability to repossess or have assurances about collateral. There does not seem to be evidence that lenders are extrapolating the marginal increase in recovery rate to a greater belief in the value of the collateral, for instance. Auto lenders generally do not believe that their collateral will appreciate in value with usage; there are standardized depreciation schedules in contrast with the value of real estate.
with their use. For instance, a starter interrupter cannot disengage a car while it is currently running, which would have the obvious potential of causing accidents. The starter interrupter can be manually overridden with a code in certain instances in cases where life and limb are at stake. The creditor can give a sheet of a number overwrite codes, each of which can only be used once to prevent abusing the leniency for exigent circumstances. These common-sense exceptions to the power of the starter interrupters are included in best practices guidelines for the industry. This would allow the companies to comply with existing law that prevents, for instance, tortious conduct on highways.

The cost of locating and then repossessing automobiles is a significant one and the starter interrupter, a form of contractware, is a powerful tool to drive down these transaction costs. This technology is currently being used and developed by creditors who are able to increase their collection rates by locating their collateral and preventing its misuse.

Some critics view such use by creditors to collect collateral as unfair to those debtors who rely on the collateral for transportation to work. Other critics in response point to the lower interest rates that debtors can afford because of the increased rates of recovery and therefore the systemically lower credit risk. This debate is beyond the scope of this article, but if there is an economic incentive for both creditors and debtors to use these devices, the law will be forced – and indeed has been forced – to determine the legality of their use.

Contract law is generally governed by states, and there is no preempting federal law specifically dealing with starter interrupters, but

101 Corkery & Silver-Greenberg, supra note 94.
103 Atta-Krah, supra note 95, at 1201 (“…federal regulations do not provide any direct guidance relating to the use of SIDs by auto dealers and lenders.”); Consumer Information: Vehicle Repossession, FED. TRADE COMM’N, http://www.consumer.ftc.gov/articles/0144-
there is not much state law applicable to contractware. As one recent survey of the extant law concluded, “generally…SID[s] [starter interrupter devices] may be legal in most states due to the secured party's right to the ‘self-help’ repossession provisions of Uniform Commercial Code (‘UCC”) section 9-609.”104

Section 9-609 of the Uniform Commercial Code, as adopted in various forms by the states, governs self-help of secured creditors. The UCC gives a secured creditor the right to either “take possession of the collateral” or “render equipment unusable” without judicial process so long as the action “proceeds without breach of the peace.”105 A rich case law exists on what constitutes a breach of the peace, and as will be shown below, it will not be difficult to fit starter interrupters into this existing corpus.

California, Colorado, and Connecticut all explicitly affirm the legality of starter interrupters but place certain restrictions on their use.106 The primary concerns of the state legislatures are both that the debtor has notice that the device has been installed and has a right to cure the breach.

The rights of debtors under the Bankruptcy Code add another wrinkle in the straightforward use of starter interrupters. A bankruptcy court in Arkansas ruled that the installation of a starter interrupter, while not per se illegal, violated the Bankruptcy Code’s automatic stay because it prevented the debtor from the normal use of her car.107 The court noted that the creditor could have remedied the situation by “taking action to ensure that Debtor had the correct code to operate her car each month, such as by mailing the correct code to Debtor each month.”108 A line of code written that would honor a court’s grant of an automatic stay motion by allowing the car to operate is another potential remedy.

The automatic stay, like the prohibition on selling alcohol to minors, acts as an external condition that the smart contract must incorporate into its terms if it is to comply with the law. The reason is because an individual

---

104 Atta-Krah, supra note 95, at 1207.
105 U.C.C. § 9-609.
cannot contractually waive his right to file for bankruptcy as a matter of public policy. As seen before, this can either be solved \textit{ex ante} or \textit{ex post}. This situation seems ripe for private solution, as it is not difficult to determine whether a party has filed for bankruptcy, given the public nature of these proceedings. A simple conditional could be written that if bankruptcy has been filed, then the starter interrupt cannot be engaged.

As blockchains currently exist, starter interrupters are operated by the creditor and done so with the use of discretion. But large corporations, like Toyota, have contemplated using blockchains to enforce their contractual arrangements. By invoking a blockchain for third-party verification, this discretion would be lost, but the debtor would be able to ensure that an interested party did not have the unilateral ability to control his collateral. The lower interest rates that come along with the blockchain’s assurances may provide a valuable option to some debtors who view the rigidity as enticing.

\section*{Self-Help and Smart Contracts}
\textit{Private Enforcement and Political Philosophy}

Self-help remedies have been defined as “legally permissible conduct that individuals undertake absent the compulsion of law and without the assistance of a government official in efforts to prevent or remedy a civil wrong.” Automated execution of a contract is a preemptive form of self-help because no recourse to a court is needed for the machine to execute the agreement. A smart contract may not, however, meet the first terms of the definition because of illegal contracts like the vending machine that dispenses heroin or the implanted bomb that explodes when a debtor defaults. These

\footnotesize{109} In re Citadel Properties, Inc., 86 B.R. 275 (Bankr. M.D. Fla. 1988) (“A total prohibition against filing for bankruptcy would be contrary to Constitutional authority as well as public policy.”).
contracts are outliers that must be dealt with, but the background approach the state should take towards smart contracts is a liberal one.\textsuperscript{113}

Smart contracts offer a wider range of assurances to parties who previously had to use other mechanisms to ensure performance. For example, without smart contracts parties are more likely to prefer instantaneous performance or overvalue the reputation of the counterparty. These are good proxies for ensuring performance, but not ironclad and come with their own costs.\textsuperscript{114} Much of the literature on self-help in contract law has dealt with how a party who has been aggrieved can remedy the wrong that has been committed against him.\textsuperscript{115} The advent and proliferation of the smart contract will focus the attention on the harms done to the breaching party, ensuring that party autonomy take a backseat to other norms that society wishes to enforce. In what follows, this Article will examine the potential benefits to non-breaching parties and society at large, and then examine the costs to breaching parties and what limits the state will place on the use of smart contracts.

As with many new technologies, behind bitcoin stood a political ideology skeptical of centralized power and supportive of capitalism and free markets. Although he\textsuperscript{116} never identified himself as such, many describe the creator of bitcoin, Satoshi Nakamoto, as a libertarian. Certainly many of the early adopters of bitcoin were self-described libertarians.\textsuperscript{117} Szabo has been

\textsuperscript{113} See Richard A. Epstein, The Theory and Practice of Self-Help, 1 J.L. ECON. & POL’Y 1, 26 (2005) (“[W]...hat the law should do is to supply a second legal remedy that offers the complete relief (or at least more complete relief) that the self-help remedy could not supply.”).

\textsuperscript{114} Id. at 22-23 (“To be sure, there are risks even in this context. Against these perils, the simplest form of protection is a simultaneous exchange in which each side gets to inspect the goods or services provided by the other before going through with the deal...The situation gets more difficult when the exchange takes place sequentially, that is, when one side performs before the other. But once again these trading systems do not suffer a total meltdown. The potential for long-term gain may be sufficient to induce individuals from taking what is left in the first round.”).

\textsuperscript{115} See, e.g., Mark P. Gergen, A Theory of Self-Help Remedies in Contract, 89 B.U. L. REV. 1397, 1449 (2009) (“The primary goal was to give a general account of the rules that regulate the powers to withhold or refuse performance in response to breach, and the power to threaten to do so to extract concessions, which is normatively appealing and well-grounded in the law's specifics.”).

\textsuperscript{116} Some will object to using “he” as the personal pronoun for Nakamoto when it is not known if Nakamoto is a male, let alone an individual. This article uses “he” for brevity’s sake, fully aware that this footnote defeats this purpose.

\textsuperscript{117} Max Raskin, Meet the Bitcoin Millionaires, BUSINESSWEEK (Apr. 10, 2013),
called libertarian and his writings emphasize alternatives to the state’s enforcement of rights.118 Traditionally, states have been defined as monopoly holders of force with a power to tax.119 Among the most radical visions for smart contracts is that the technology will subject the provision of justice to market forces and break the state’s monopoly over the court system. This is an idea that has been discussed by many libertarians, including Robert Nozick, Murray Rothbard, and David Friedman.120

For many libertarians, the purpose of civil government is to protect private property and enforce natural rights.121 Most fundamental here is the harm principle that an individual should be free to do as he chooses, coterminous with the rights of others.122 This implies a strict adherence to freedom of contract.123 On this view, smart contracts use technology to enforce party autonomy in a more effective manner because they prevent external interference. If contractware progresses to a point where there is truly no need for third-party enforcement, there would be no need for a state and the attendant costs that many libertarians see as unjustifiable.

Smart contracts could be used to encode certain constitutional principles into armaments, such that weapons would not work if certain conditions were not met, e.g. if Congress does not declare war, weapons will

http://www.businessweek.com/articles/2013-04-10/meet-the-bitcoin-millionaires [https://perma.cc/P4LQ-C87Y] (“The surge in a Bitcoin’s value has made millionaires out of people who loaded up on them early on—however briefly. Many of them are self-described libertarians, drawn by the idea of a currency that exists outside the control of governments. Some were so taken with the concept that they launched Bitcoin businesses, such as exchanges where people can buy the coins or exchange them for dollars.”).

118 See, e.g., Nick Szabo, Ten ways to make a political difference, UNENUMERATED BLOG (Aug. 12, 2007, 2:10 PM), http://unenumerated.blogspot.com/2007/08/ten-ways-to-make-difference.html [https://perma.cc/D9Q8-BERY] (Advising those who want to make a political difference to, among other things, “Be prepared to vote with your feet….make your own law…donate to or get involved with the [libertarian/conservative] Institute for Justice…Tell us about your good research and good ideas.”).

119 MAX WEBER, POLITICS AS A VOCATION (1919).


121 JOHN LOCKE, TWO TREATISES OF GOVERNMENT, Chapter VII, § 85 (1689).

122 JOHN STUART MILL, ON LIBERTY, 21–22 (1859).

not function on foreign soil. Although fanciful, applications like this limn the concerns animating many early proponents.124 This speculative and radical vision of smart contracts is not held by all proponents of the technology. Rather, some proponents are primarily focused on the capability of smart contracts to reduce transaction costs. Instead of fundamentally changing the nature of political governance, a new wave of smart contract proponents is concentrating on the idea that their use can make the economy and corporate governance more efficient. I call these individuals the Coaseans because they care about reducing transaction costs.125 One of the main areas to do so is corporate governance within firms, where a number of proposals have been discussed.126 These proposals include improving shareholding voting systems, tracking debt and equity issues, and enabling triple-entry accounting.127

An example of a firm that utilizes smart-contract technology to execute its corporate-governance rules is a decentralized autonomous organization (“DAO”). One way of thinking of a DAO is that it is an organization where the rules of management are predetermined and run on computers.128 One such DAO was formed in 2016.129 The idea was to create an investing entity that would not be controlled by any one individual, but by shareholders voting based on their stakes on a blockchain. This would reduce transaction costs by obviating the need for a management team.130 The entity was funded with $150 million.131 Soon after this money was raised, about $40 million of those funds were diverted from the organization by a “hacker” who

---

124 In the recent novel Seveneves, Neal Stephenson imagines a gun that fires robots as projectiles and can only respond to a certain user—futuristic smart bullets. NEAL STEPHENSON, SEVENEVES 676 (2015).
126 See Yermack, supra note 49.
129 Coy & Kharif, supra note 111.
131 Coy & Kharif, supra note 111.
used the code in an unanticipated way.\textsuperscript{132} Strictly speaking, however, the hacker did not “hack” the code in a malicious way, but rather used the terms of the existing smart contracts to accomplish something others later found objectionable, i.e. the diversion of their money.\textsuperscript{133} Consider this using a legal loophole to effect a result that was clearly within the letter of the law, but not within its spirit.\textsuperscript{134}

Another example of smart contracts enabling novel corporate-governance procedures is the use of prediction contracts. A prediction contract is a binary option contract whose value is contingent on an event’s occurrence.\textsuperscript{135} These contracts are often cited as predictors of presidential elections, where market participants buy and sell contracts in accord with shifting beliefs in a candidate’s probability of being elected.\textsuperscript{136} But, they can also be viewed as a form of smart contract that can be executed on a blockchain without any input from a single third party. In many credit default swaps, for instance, a third party, the International Swaps and Derivatives Association, will determine whether a credit event has been triggered.\textsuperscript{137} With a smart contract using a decentralized blockchain for authorization, a network itself can verify whether an event took place and whether the contract will pay out. This has applications in the realm of corporate governance, where decisions can be automated based on discrepancies between the option price and the stock price, directing a board of directors to take one course of action over another.\textsuperscript{138}

\textsuperscript{133} Id.
\textsuperscript{134} Id.
\textsuperscript{138} Robin Hanson, Markets for Telling CEOs to Step Down, GMU.EDU (Apr. 26, 1996), http://mason.gmu.edu/~rhanson/dumpceo.html [https://perma.cc/Q6QD-4H4G]. These contracts also act as a potential hedge of political or event risk for companies, see also Michael Abramowicz, Predictocracy: Market Mechanisms for Public and Private Decision Making 87.
Limiting Principles

The above has shown the benefits that come from judicial recognition and enforcement of smart contracts. Some of the believers in smart contracts think that these benefits can be appreciated without judicial recognition and enforcement because smart contracts can supplant traditional judicial systems enforced by a centralized state.139 This section of the Article analyzes the positive question of where the outer-bound of a state’s acceptance of smart contracts lies. Three examples along a spectrum will demonstrate the degrees to which states and their judicial systems can approach smart contracts. On the one end of the spectrum is permitting the use of smart contracts use and recognizing them in collateral matters, e.g. recognizing a smart contract when going through the probate process. On the other end of the spectrum is prohibiting the use of smart contracts or banning certain forms of contractware. Similar to the manner in which non-smart contracts cover a variety of different agreements—employment contracts are different from marriage contracts—smart contracts will likely be adapted to cover a wide range of subject matter. The application of a particular contract will likely be relevant to which attitude the courts adopt, much as not all non-smart contracts are the same; employment contracts are different than marriage contracts.

Starter interrupter devices are illustrative of the permissive side of the spectrum. As was shown, courts have recognized these devices as legitimate and allowed companies to use them to repossess vehicles, provided there is no violation to external laws, including the Uniform Commercial Code’s “breach of peace” provision and the Bankruptcy Code.140 How courts treat violations will likely be instructive. Suppose a starter interrupter is placed in a truck that is essential to a business. Instead of merely shutting the car off, this starter interrupter will permanently damage the car’s engine, rendering it unusable, if payments are not received on time. Then, suppose the debtor files for Chapter 11 bankruptcy. The debtor-in-possession or trustee could charge that the use of the starter interrupter is a violation of an automatic stay, as it is an attempt by the creditor to control the property of the estate, even though the control is

140 U.C.C. § 9-609.
automatic and out of the creditor’s hands. The question then put to the court is whether starter interrupter can be used at all if they have such potential.

A second example in the middle of the spectrum, would be a modern version of Williams v. Walker-Thomas Furniture Co. In Williams, the court set forth a standard of unconscionability by asking whether the terms of a particular cross-collateralization contract were “so unfair that enforcement should be withheld.” Imagine, however, that the furniture in that case was installed with contractware that blasted an annoying siren if payment was not received. Further, imagine that this was explicitly agreed to by the debtor ex ante. A court bound by Williams, could easily deem the contract unconscionable. This would leave the court to determine the proper remedy.

The court could award damages to account for the harms caused by the automatic execution of the contract, which damaged the collateral in an unacceptable way. In this instance, such a remedy seems appropriate because the damage is not irreparable. It is likely that what the court would do is create a new breaching the of peace doctrine that creditors and the contractware would have to abide by.

The final, and most egregious, example is contractware installed into humans. Although certainly a dystopian gedankenexperiment, it is worth imagining a scenario where creditors can install devices into the bodies of debtors and have the device force them into slavery or some state of impaired consciousness if they default. Such a scheme would certainly be unconstitutional as a violation of the Thirteenth Amendment even if the debtors supported the scheme as a way of securing lower interest rates. This is not the interesting question, however. What is worth analyzing is how a court would deal with such installation. Despite consent by each party, the court would likely nullify the contract. But will the court prevent the installation of the contractware into the body? Much more likely than judicial intervention is a legislative solution. States can and have banned objects that are not per se violative of rights, but pose an unacceptable risk to the morals of the community. This can be a legitimate exercise of the police power of the state, such as, for instance, when the government bans the private possession of bazookas.

143 Cf. Ashcroft v. Free Speech Coal., 535 U.S. 234, 251 (2002) (The case reaffirmed that where the speech is neither obscene nor the product of sexual abuse, it does not fall outside the protection of the First Amendment.).
What the above illustrates is that smart contracts exist in preexisting legal structures that do not unequivocally value party autonomy with respect to the formation and performance of contracts. The central question, however, is whether the state can use prior restraint to prevent the formation of contracts that have the potential to become contrary to public policy, but are not necessarily contrary to public policy themselves.

The likely answer is yes. It is hard to imagine a state sitting idly by while devices are installed to self-enforce contracts that are contrary to the state’s own interests and policies. Although, the proposition is not black-and-white. When dealing with any question of prior restraint, the magnitude of the mischief must be weighed against the likelihood of its occurrence. The Supreme Court’s First Amendment jurisprudence provides a useful model; in that realm, the Court has erred on the side of respecting autonomy and policing ex post. In this instance, contractware ought not be analyzed in toto, but discrete devices and software applications should be evaluated. This evaluation should be based upon the rights implications, as opposed to the particular functions of the contractware device. So, while devices that prevent the usage of personal property could be allowed, implants that enforce unconstitutional contracts or contracts that are unconscionable or void against public policy would not be permitted.

These are questions for judges to decide on a case-by-case basis. Common law principles ought to form the background of such analysis.

CONCLUSION

The creators of smart contracts have invited society to a party they are throwing. They say that this party has better food, booze, and music than the party being thrown down the street. But the other party has all of the people, even if the amenities are not as good. Whether society shows up to this new party is an open question. This is because legacy systems exist for a reason. By definition, they work. Both switching costs and uncertainty stand as barriers to the adoption of any new technology. Yet if the value of the new technology is overwhelming, such a change is more likely to occur.

One way of reducing uncertainty is by situating the new in the old. While there may be many barriers to the adoption of smart contracts, legal

146 Lichtman, supra note 92, at 257 (arguing that private self-help mechanisms should be analyzed on a case-by-case basis).
uncertainty need not be one of them. Courts need not upend extant jurisprudence to accommodate smart contracts.
Mobile banking, digital payments, peer-to-peer lending, and e-commerce are no longer ideas drawn from science fiction. The rise of the internet has disrupted our notion of financial payments; we can now shop, invest, and manage our payments online. The emerging industry of financial technology ("fintech") deepens and broadens the range of financial services that customers can use over the internet, whether through a desktop computer, laptop, or smartphone. Fintech participants include start-ups and other companies that use technology to conduct the fundamental functions provided

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Wesleyan University, B.A. 2012. © 2017, Dina Moussa.
by financial services, impacting how consumers store, save, borrow, invest, move, pay, and protect money. Examples of fintech products include the ability for individuals with checking accounts to use Apple Pay, a payment platform linking their debit and credit cards to their Apple devices. Android users can use Android Pay, a similar app, which links users’ financial information to their devices. To make a payment with either of these, users simply hold their device near a payment reader. Drivers can pay tolls by simply having E-Z Pass devices on their vehicles while driving through toll gates. The E-ZPass system allows drivers to purchase small electronic transponders, which correspond to their pre-paid accounts. When drivers travel a toll-paying road, the antennas at the tolls will read the transponders and debit the accounts for the appropriate amount.

Fintech has also attracted attention beyond Silicon Valley. Governments and policy-makers are also invested in its progress and success. Fintech’s proponents also promise that fintech will make financial services cheaper, more readily available, and more efficient. For example, the World Bank Group, through its Universal Financial Access 2020 initiative, aims to ensure that communities who have poor access to mainstream financial services normally offered by retail banks, have access to traditional financial platforms, like checking accounts, by 2020. Once previously unbanked individuals have something as simple as a checking account, the fintech movement aims to dramatically expand and ease their abilities to make payments.

---


As new technologies emerge and the global economy expands, individuals will continue to rely on the use of cryptocurrency, data analytics, and online transactions. Every action one takes on a fintech platform leaves what computer programmers and app developers call “digital breadcrumbs.” Digital breadcrumbs refer to all the recorded information we share while shopping, investing, or browsing online: purchasing histories, visited websites, and IP addresses, are all stored. Fintech companies store customer information as a matter of course, and often use the information to improve their products or offer new ones. Because companies store this information, and the government can subpoena much of this information, the government in turn will have increased access to our whereabouts, spending habits, and behaviors as individuals increasingly rely on new technology allowing the government access to more sensitive information.

The Fourth Amendment protects individuals from unwarranted searches and seizures conducted by the government. However, under the third-party doctrine, the Fourth Amendment does not afford protection for information turned over to third parties, as individuals surrender a reasonable expectation of privacy in that information by entrusting it to someone else. Depending on the type of data requested, the government is often not required to obtain a particularized warrant or subpoena when requesting user information that was given to a third party. These parties can legally provide their users’ information, which can be used as evidence in a criminal proceeding. While the Supreme Court strives to uphold Fourth Amendment

---


6 See Miklos Dietz et al., supra note 1.

7 See United States v. Miller, 425 U.S. 435, 440 (1976) (noting that individuals have no reasonable expectation of privacy in their bank records because they are business records created and kept by the bank).

8 There are some statutory legal protections on information provided to a third party, such as the Stored Communications Act, which prohibits disclosure of customer information under some circumstances and permits it in others. Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2711 (1986). The Gramm-Leach-Bliley Act, codified in 15 U.S.C. §§ 6801-6810 (1999), also protects customer information and requires financial institutions to provide their information-sharing practices to their customers. However, the Act is an insufficient protection given that it only applies to "financial institutions" and it is not clear whether these new fintech platforms are "financial institutions" as defined by the statute.
values of protecting individuals and their right to privacy, it has not reconciled the current third-party doctrine with the new practical realities imposed by the digital age.\(^9\)

Skeptics argue there is no reason to worry about government searches of our digital footprints because existing Fourth Amendment doctrine prevents the government from unfairly accessing digital breadcrumbs.\(^10\) However, this Note will argue that financial data handed over by users to these third parties is not sufficiently protected under the Fourth Amendment, and that Fourth Amendment jurisprudence has not kept up with technological developments that have made an individual’s financial information increasingly accessible.

First, this Note will explain that financial information in particular requires Fourth Amendment protection in order to sufficiently safeguard individual privacy, as the fintech industry expands and our economy increasingly relies on digital payment methods. It will then argue that current jurisprudence is insufficient to protect an individual’s privacy in his or her financial information given the evolution of modern technology, and that the Supreme Court has made compelling arguments as to why the third-party doctrine is outdated and should not be applied to financial data. This Note will also provide an overview of other existing privacy protections that are insufficient for protecting financial privacy. It will then suggest a solution to protecting the privacy of an individual’s financial information by proposing a new jurisprudential framework that better reconciles the fintech revolution with existing Fourth Amendment values by distinguishing between sensitive and intrusive data. It will conclude with a hypothetical, illustrating how the framework may be used to better uphold Fourth Amendment values in the digital age.

As the automation of the global economy grows and online payment practices proliferate, the Supreme Court will need to adapt the current legal structure to adequately protect Fourth Amendment values governing financial information. If the Court does not, its jurisprudence will abandon many core Fourth Amendment values in the face of technological innovation.

---

\(^9\) The Court has tried to reconcile the third party doctrine with new technologies, such as GPS, but it is not clear whether its application can accommodate future cases with different technologies. See, e.g., United States v. Jones, 565 U.S. 400, 412 (2012).

\(^10\) Jennifer Granick, American Spies: Modern Surveillance, Why You Should Care, and What to Do About It 220 (Cambridge Univ. Press, 2017) (arguing that the third party doctrine does not apply to network providers).
OUR FINANCIAL INFORMATION REQUIRE PRIVACY PROTECTION

Fintech has increased the digitalization of financial transactions making financial data more accessible and easier to store for longer periods of time. Detailed and sensitive user data can now often be stored indefinitely in one or several centralized locations, generally only protected by privacy policies instituted by the company holding the data. Mobile payments, peer-to-peer lending, virtual investing, and connected devices now allow instant transactions through the internet and apps rather than by bank clerks and investment brokers. The internet and new technological products are establishing new norms in banking and lending, which allow individuals to conduct financial transactions more independently. These new norms also allow individuals to have one app to conduct all of their financial transactions—which was previously unheard of. As convenient payment and investment methods become cheaper and more readily available, many of us will use them. For example, many people already prefer to use credit or debit cards rather than cash; many banks and investment companies are slowly eliminating bank branches, and encouraging users to do their banking online.  

The global market trend is toward increasingly digital financial transactions.

As fintech proliferates, users will centralize their transactions and financial information. Unlike transactions conducted with cash or, to a lesser degree, checks and credit cards, fintech transactions create a holistic digital fingerprint of an individual, which is kept indefinitely by the company processing the transaction. Before the digitization of financial transactions, individuals used cash or personal checks, which allowed individuals to purchase items or services without revealing much about the purchases or


services themselves. Historically, paper receipts and checkbooks were used to prove that particular transactions took place. If an individual used a personal check to make a purchase, the bank had the check recipient’s name, which revealed some information about the purchase (the date and the store name) but not as much as what a digital transaction reveals. The individual also had the option to include more details in his or her checkbook surrounding the actual purchase, like the time, location, and the item or service purchased.\footnote{An individual’s checkbook is an effect protected under the Fourth Amendment.} A purchaser could discard the receipt or keep it with his or her financial records. Now, with the increased digitization of financial transactions, financial platforms and apps have immense storage capacity to keep an individual’s digital records indefinitely, without allowing users the ability to delete the information.\footnote{The Privacy Act of 1974, 5 U.S.C. § 552a, was enacted to protect the privacy rights of individuals by reducing the federal government’s ability to have a centralized computer database with all their information.} While users may believe they have simply moved the functions of their checkbooks to the cloud, the legal impacts are profound. While checkbooks are considered a protected “effect” under the Fourth Amendment,\footnote{Wilson, 36 F.3d 1298, 1306.} online records maintained by a third party may have no such protection depending on the type of data they contain.\footnote{See United States v. Miller, 425 U.S. 435, 440 (1976) (noting that individuals have no reasonable expectation of privacy in their bank records because they are business records created and kept by the bank); see also Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2711 (1986).}

These platforms store an immense amount of data, calling into question what, if any, privacy protections their consumers hold. For instance, with the centralization of large amounts of financial and transaction information, law enforcement no longer needs to investigate and search for individual’s separate bank accounts: this data may now plausibly be stored by a single company along with credit card and transaction information. Mint, a web-based personal financial management service, allows users to input information about their bank accounts, physical location, shopping preferences, household budget, investments, and debts and loans. Since all this information is stored by Mint online, law enforcement no longer needs to spend time and energy searching for and obtaining access to different services, greatly reducing individual privacy protections from the government in a way
that could not be the case if this information were stored in the physical realm.\textsuperscript{17}

Online financial transactions can also reveal much about a person from the transaction’s date, time, item purchased (including its image) and its cost. These records create a story explaining where and when an individual was present, and whom was in that particular vicinity when that purchase was made. Additionally, an individual’s purchases can reveal a lot about his or her preferences, needs, and lifestyle.

Even social media can store, track, and reveal users’ preferences, interests, and movements. If an individual uses Facebook’s platform to make purchases or engage in financial transactions with his or her Facebook friends or through Facebook’s apps (like buying a product or service from a friend, making a purchase for a Facebook-hosted game, or making a donation on Facebook), the platform collects and retains information about the transaction. This information includes the user’s payment information and the individual’s name, billing, shipping and contact details.\textsuperscript{18} Users may not expect this information to be revealed to anyone, including the government.

Even when individuals are not using fintech services, their financial and transaction data may be held by third parties, with or without the individual’s knowledge. Many companies now also require individuals to submit a credit report for anything from employment to residential applications. To avoid credit report costs, individuals now use services such as Credit Karma, to generate free updated credit scores and reports from national credit bureaus like TransUnion.\textsuperscript{19} To sign up, individuals must create a user profile, which includes personally identifiable information. Although these services do not acquire payment information, they look into a user’s credit history from multiple sources, including his or her banks, credit card companies, collection agencies, and the government.\textsuperscript{20} This information

\textsuperscript{17}The Supreme Court has noted diminishing privacy protections due to the ease of accessing digital personal information. \textit{See, e.g.}, \textit{United States v. Jones}, 565 U.S. 400, 412 (2012) (Sotomayor, J., concurring that the mosaic theory, whereby government can obtain a lot of information easily, changes the relationship between the government and citizens).


\textsuperscript{20}While the Fair Credit Reporting Act, 15 U.S.C. § 1681, provides privacy and notice rights for consumers, such as the right to know what information is contained in their credit reports, it does not prevent third parties from obtaining such information without their consent.
reveals the individual’s spending habits, payment history, and yearly income. This type of data can identify certain life events or categorize an individual based on his or her credit history.

When the Bill of Rights was added to the Constitution in 1791, it is unlikely (to say the least) that its drafters envisioned a world where the government would have nearly unlimited access to citizens’ financial information through a blanket rule called the third-party doctrine. In the Fourth Amendment, the Founders codified what they believed was essential to individual liberty: protection from unlawful government intrusion, barring particularized warrants and probable cause. In 2017, hardly anyone goes a day without passing information through a third party, leaving that information vulnerable to exactly the type of warrantless intrusion the Fourth Amendment was written to protect against. As the fintech movement continues, financial data is more accessible to law enforcement because it can be centrally stored and kept for longer periods of time without giving users the ability to delete their records.

**CURRENT FOURTH AMENDMENT JURISPRUDENCE IS INSUFFICIENT TO PROTECT AN INDIVIDUAL’S PRIVACY IN HIS OR HER FINANCIAL INFORMATION**

A Fourth Amendment search takes place when the government violates a person’s subjective expectation of privacy through an examination of “persons, places [or] effects,” when that subjective expectation is one that society recognizes as objectively reasonable. The third party doctrine, established by *United States v. Miller*21 and *Smith v. Maryland*,22 removes Fourth Amendment protection for information handed over by individuals to third parties. The Court reasoned that turning over information to another party undermines any reasonable expectation of privacy, such that the government’s accessing of such information is not a search. While once a sensible accommodation of the underlying technological landscape, the third-party doctrine is no longer a reasonable approach to individual privacy, given current and upcoming technological developments. Historically, the third-party doctrine concerned targeted and limited government investigations

21 See 425 U.S. 435 (1976) (holding that individuals have no reasonable expectation of privacy in their bank records because they are business records created and kept by the bank).
22 See 442 U.S. 735 (1979) (holding that when an individual dials telephone numbers, he or she has no reasonable expectation of privacy in his or data because it was handed over to a telephone provider, a third party.).
directed at specific individuals for which the government could show grounds for suspicion.\textsuperscript{23} Neither of these cases from the 1970s addressed our current reality in which digital data storage contains almost all of our private information.

More recently, the Supreme Court has recognized the need to update the third-party doctrine. It has opened up exceptions to the third-party doctrine in order to update it for the digital age, such as in a recent opinion banning government search of information stored on an arrestee’s cell phone without a warrant.\textsuperscript{24} But the fundamental problems with the third-party doctrine remain, and cannot be dealt with by anything less than abandoning the doctrine and replacing it with a more modern and nuanced approach to privacy in the digital age.\textsuperscript{25}

\textit{Overview of the Third-Party Doctrine}

The leading case discussing privacy rights in information given to third parties is \textit{Smith v. Maryland}, where the Supreme Court held that the defendant who voluntarily provided his data to a phone company had no reasonable expectation of privacy in the information.\textsuperscript{26} The Court dismissed the Fourth Amendment claim against the government for using a pen register, with the phone company’s authorization, to track the numbers dialed by the defendant.\textsuperscript{27}

The Court held that when an individual dials numbers on a phone, he willingly uses a telephone company’s service in order to make the call and understands that using the service includes providing certain information to the company.\textsuperscript{28} Therefore, when an individual dials these numbers, he has no reasonable expectation of privacy in his data because he handed it over to the telephone provider, a third party.\textsuperscript{29} Individuals should reasonably know that companies have the capability and incentive to make permanent records of the numbers that their customers dial.\textsuperscript{30} The \textit{Smith} Court reasoned that if an individual takes the risk of “revealing his affairs to another, that . . .
information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose." Since Smith, the third-party doctrine applies not just to telephone numbers, but to any information handed over to third parties, such as purchase history, invoices, and online banking transactions.

Similarly, in United States v. Miller, the police connected the defendant to a bootlegging conspiracy by subpoenaing his bank for checks written from his business account. The Court held that checks are not confidential because they are a business instrument, rather than a private document. Additionally, the Court noted that bank customers have no reasonable expectation of privacy in their bank records because they voluntarily hand over this data to third parties and the bank employees are able to view these documents.

In addition, under the current third-party doctrine, when individuals use fintech (e.g., sending payments online, investing online, banking through their bank’s website, or lending money to a friend) and download the corresponding apps that allow them to conduct these transactions, individuals will have no reasonable expectation of privacy in this data. From financial transactions between friends using Venmo to a bank record tracking the whereabouts of an individual at all times through their debit card use, some fintech apps and methods used to facilitate these virtual transactions may allow companies and the government to access a variety of personal data, which may be voluntarily handed over by the third parties to the government without a warrant. In many cases, courts may conclude that individuals voluntarily used these devices and apps and willingly chose to disclose to third parties the data collected, analyzed, stored, and synced by these apps. Therefore, in some situations where the government requests this information

31 Id. at 744.
33 Id. at 440.
34 Id. at 442.
36 There are some statutory legal protections on information provided to a third party, such as the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712. The SCA permits voluntary disclosure, requires disclosure, and prohibits disclosure of customer information in varying circumstances. See, e.g., 18 U.S.C. §§ 2701 (defining “offense,” and establishing punishments and exceptions for the purposes of the SCA), 2702 (“Voluntary Disclosure of Customer Communications or Records”), 2703 (“Required Disclosure of Customer Communications or Records”), 2711 (defining relevant terms for purposes of the SCA).
from a third party, courts may hold that this is not an unlawful search under the Fourth Amendment, and the evidence may be admissible against an individual in a criminal proceeding. This depends on the specific type of financial data at issue and whether other statutory protections apply to its disclosure.

*The Third-Party Doctrine, as Developed in Smith and Miller, No Longer Adequately Protects Core Fourth Amendment Values*

Although well-reasoned for their times, the holdings in *Smith* and *Miller* simply do not provide relevant guidance for today’s highly networked world. Nearly all of the vast volumes of information that individuals generate about themselves is filtered through a third party, which robs those holdings of their original logic. The way information was created and used in 1970’s America is enormously different from how it is created and used today. As the financial industry becomes digitized, the financial data of individuals will be increasingly gathered and stored electronically by the third parties that run these financial apps and platforms. An individual’s privacy in this data may be vulnerable and at risk depending on the type of financial data he or she is handing over.\(^{37}\)

In *Smith*, the police requested a list of the defendant’s dialed phone numbers from his telephone company in order to determine his whereabouts during the robbery.\(^ {38}\) The police were led to the defendant because a witness had written down his license plate number when his vehicle was spotted during the robbery. Here, the police had two justifications to collect the defendant’s data: (1) the date of the robbery; and (2) “particularized suspicion” that the defendant was the robber because he was spotted fleeing the scene shortly after the crime.

*Smith* is obsolete today because the volume and sensitivity of the information gathered in *Smith* is significantly less than the data that is and will be collected by banks and apps. The *Smith* investigation had a set duration, and collected only three days’ worth of numbers. However, the certain financial data collection from banks and apps will be endless and easier to analyze if the information is not protected under other statutory or regulatory

\(^{37}\) However, the Stored Communications Act prohibits disclosure of customer information under some circumstances and permits it in others. See, e.g. 18 U.S.C. §§ 2701, 2702, 2703, 2711.

\(^{38}\) See *Smith*, 442 U.S. at 737.
schemes. The government will have the ability to gather a tremendous volume of financial data that may be stored indefinitely and acquired at any time without cause or justification. Mass surveillance increases the number of targets available to track at any given time and decreases the cost of tracking to zero as data is collected and stored in the course of our day.39 Because the facts in Smith and society’s current reliance on technology are no longer analogous, Smith and the third-party doctrine should no longer be used to analyze whether individuals have a reasonable expectation of privacy in the financial data they hand over to third parties.

Similarly, Miller is inapplicable today because the amount of data that banks, and other financial and investment companies acquire from their customers can be sorted and analyzed to create a full profile of an individual and his or her behaviors and patterns. For example, companies now use algorithms and computer models to analyze massive pools of information to make inferences about a user’s health, personality traits, and even mood in real time, in order to help the companies predict, and ultimately influence, the user’s next purchase.40 In the aggregate, law enforcement could learn this information as well as a user’s private thoughts and interests from this data or a company’s analysis of the user and his or her preferences.

Additionally, Miller’s holding is too archaic to apply to today’s fintech landscape because banking practices and the financial industry have changed since the Supreme Court decided the case in 1978. Bank tellers, financial advisors, and brokers are being replaced by apps, online banking websites, and financial planning services. These individuals who once played essential roles in processing our checks, transferring our money, and investing in our retirements are no longer acting as intermediaries to facilitate our transactions. Individuals are now capable of engaging in these transactions—transferring funds, sending virtual checks, peer-to-peer lending—instantly and on their own without stepping foot outside their homes. Because the intermediary component (the tellers, the brokers, the financial planners) has been eliminated from these transactions, we should no longer consider financial

records and transactions as business records belonging to the banks or the apps used to engage in these transactions.

When the Supreme Court issued the *Miller* and *Smith* holdings, it was both unanticipated and unforeseeable that technology would reach the level of sophistication and accessibility that it has today. We are now able to lend money and make payments at the click of a button, refinance debts online, and have robot investors execute our investment choices. Technology is now an inherent part of society, and the amount of data that is passed through third parties is “so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression,” thus increasing an individual’s reasonable expectation of privacy in this data. Additionally, some of the data handed over by individuals to third parties is not “voluntary.” For example, the use of some banking apps, like Charles Schwab’s online app, is mandatory—the company only has eleven physical bank locations, which are all in California and Nevada. Most individuals perform their transactions through the Charles Schwab online app. Similarly, when individuals purchase apps, like the Charles Schwab app, they are required to accept the terms and conditions before receiving that product or service. Individuals are forced to sign these contracts in order to receive these apps. Courts apply traditional contract law to determine whether users had reasonable notice and provided consent to a service’s privacy policy. However, practically

---

46 See Schwab Mobile Deposits, CHARLES SCHWAB, http://www.schwab.com/public/schwab/investing/pricing_services/mobile/schwab_mobile_deposit (last visited Mar. 27, 2017) [https://perma.cc/SK9W-Y48N] (many across the country use Charles Schwab. However, the company only has banking branches in California and Nevada meaning its users are required to use the online app for financial transactions).
47 Alison S. Brehm & Cathy D. Lee, From the Chair: “Click Here to Accept the Terms of Service,” 31 AM. BAR ASS’N. COMM’N LAWYER 1 (Jan. 2015),
speaking, the terms and conditions usually are not enough to provide actual notice of what data the app collects about the individuals, or what the companies can do with that information. These agreements are generally way too long and wordy. Individuals also do not have any bargaining power and cannot negotiate the terms of service with the financial company or platform. Lastly, individuals may not have viable alternatives to using a particular financial service or product because it may be the most popular or most of their friends and family members use a particular platform. Users may be forced to agree to these terms and conditions without fully understanding the agreements. The volume of information individuals generate and necessarily ‘hand over’ to third parties makes the underlying logic of Smith and Miller inapplicable in the digital age.

The Supreme Court Has Made Compelling Arguments for Why the Third-Party Doctrine is Outdated and Should Not Be Applicable to an Individual’s Financial Data

Recently, the Court provided several strong arguments for why an individual’s right to privacy in the emerging digital age should not be limited by the third-party doctrine. In Riley v. California, the Court unanimously concluded that the government must obtain a warrant to search a cell phone confiscated during an individual’s arrest because arrestees have a reasonable expectation of privacy in the digital information stored on their cell phones.48 Writing for the Court, Chief Justice Roberts explained that “cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee’s person.”49 He listed several factors explaining why searching a cell phone implicates individual privacy to a degree that is categorically distinct from searching other closed containers; their “immense storage capacity” which can hold and transfer “millions of pages of text, thousands of pictures, or hundreds of videos” and the quantity of information individuals store on these devices.50 The Court acknowledged ninety percent of Americans carry cell phones and “use them to keep a digital record of nearly every aspect of their lives.” Some of this personal information includes


49 Id. at 2479.
50 Id.
where and when they travel, whom they spoke to and what they said, and what
they were thinking about as they searched a question on their phone.\textsuperscript{51}

Through its discussion of cell phones, the Court stressed the
importance of protecting an individual’s right to privacy in the digital era. It
acknowledged that possible “intrusion[s] on privacy [are] not physically
limited in the same way when it comes to cell phones” and other digitally
stored information.\textsuperscript{52} The storage capacity of cell phones has several
interrelated consequences for privacy. First, cell phones collect many distinct
types of information from a single location. This information combined can
reveal much more than any isolated record.\textsuperscript{53} Second, their capacities allow
“even just one type of information to convey far more than previously
possible.” Many details about an individual's private life can be “reconstructed
through a thousand photographs labeled with dates, locations, and
descriptions.” This would not have been the case if an individual had a single
photograph or two of loved ones stored in his or her wallet.\textsuperscript{54} Third, the
phone’s metadata can date back to the purchase of the phone or earlier. The
Court compared this capability to an example predating cell phones: a person
may carry a slip of paper in his pocket reminding him to call an individual.
However, he would not carry a record of all his communications with this
individual for the past several weeks, months, or years.\textsuperscript{55}

Similarly, the most compelling argument that the Court gave in
protecting the digital data of individuals was the “element of pervasiveness
that characterizes cell phones but does not exist with physical records.”\textsuperscript{56} The
Court noted prior to the Internet age, individuals did not carry a collection of
their sensitive personal information with them “as they went about their
day.”\textsuperscript{57} It also noted that certain types of data are also qualitatively different. It
acknowledged internet searches and browsing histories can reveal an
individual's private interests, concerns, worries, thoughts, or feelings. Coupled
with a search for disease symptoms, they can reveal an individual's sensitive

\textsuperscript{51} Id.
\textsuperscript{52} Id. at 2489.
\textsuperscript{53} Riley v. California, 134 S. Ct. 2473, 2489 (2014). For example, if law enforcement accesses
a cell phone containing an address, a note, a prescription, a bank statement, and a video, they
can gather a lot more information about an individual than having one of these in isolation.
\textsuperscript{54} Id.
\textsuperscript{55} Id.
\textsuperscript{56} Id. at 2490.
\textsuperscript{57} Id.
medical information or symptoms they may be experiencing. Additionally, the Court acknowledged information contained on a cell phone can also reveal a person’s whereabouts and current location. It can even be used to “reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.”

The Court also discussed another example of why the digital data of individuals requires additional protections: society’s pervasive use of apps. The average smartphone user installs and uses thirty-three apps. These apps offer a range of convenient tools for managing detailed information about all aspects of a person’s life—such as drug recovery addictions, pregnancy, budgeting, hobbies, dating, and buying and selling just about anything and the records of such transactions may be accessible on the phone indefinitely. Together, this information “reveal[s] a montage of the user's life” and “not only contains in digital form many sensitive records previously found in the home” but “also contains a broad array of private information never found in a home in any form—unless the phone is [there].” The Court acknowledged the flaw in comparing a cell phone to a digital container because the information may not only be stored on the device itself, like information stored on clouds or remote servers but left us with no clear guidance on how to analyze the reasonable expectation of privacy in our data.

The Court’s decision in *Riley* was consistent with its view in *United States v. Jones* where the government attached a Global Positioning System (“GPS”) tracking device to the defendant’s vehicle to monitor the vehicle's movements on public streets. The Court used the reasonable expectation of privacy test and held that the government’s actions constituted a search under the Fourth Amendment and were an invasion of the defendant’s privacy. Specifically, the Court determined that when the Government engages in physical intrusion of a constitutionally protected area or effect in order to obtain information, that intrusion constitutes a violation of the Fourth Amendment. Here, the officers encroached on the defendant's vehicle, which

---

59 Id.
60 Id.
61 Id.
62 Id.
63 Id.
65 Id. at 407.
the Court considered a protected space and effect, in order to monitor the vehicle’s movements.\footnote{Id. at 412.}

In \textit{Jones}, the Court noted that “achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but [that] the present case [did not] not require [them] to answer that question.”\footnote{Id.} Nonetheless, the Court noted that “situations involving merely the transmission of electronic signals without trespass would remain subject to \textit{Katz} analysis and would likely need to be resolved at a later time.”\footnote{Id. at 411.}

Justice Alito and Justice Sotomayor agreed with the Court’s holding but took it a step further in their concurrences alluding to additional privacy concerns as technologies become more sophisticated. Justice Alito’s concurrence noted that advancements in technology are making it easier for the Government to monitor criminal activity and that the “‘[t]raditional surveillance’ of \textit{Jones} for a 4-week period ‘would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.’”\footnote{United States v. Jones, 565 U.S. 400, 412 (2012) (quoting Alito, J., concurring at 429).} He added that while short-term monitoring of an individual’s movements on public streets accords with expectations of privacy, longer term GPS monitoring in investigations impinges on expectations of privacy.\footnote{Id. at 430 (Alito, J., concurring).} He acknowledged that he could not answer the question of when short term surveillance became long term surveillance.

Justice Sotomayor took Justice Alito’s concurrence a step further and cautioned about the implications of wireless surveillance and its effects on privacy, including questions about the constitutionality of warrantless short-term GPS surveillance.\footnote{Id. at 413-9 (Sotomayor, J., concurring).} She argued that even short-term GPS monitoring could reveal an individual's every movement, divulging a great deal about a person's daily actions, interests, and private destinations.\footnote{Id. at 415.}

Additionally, new technologies have made individuals especially vulnerable to government surveillance. As new technologies develop, surveillance will become cheaper and easier than it has ever been before, which facilitates greater surveillance.\footnote{United States v. Jones, 565 U.S. 400, 428-29 (2012) (Alito, J. concurring).} Under the current third-party doctrine,
law enforcement can simply ask a cooperative third party, such as a cell phone provider, for cell tower information to determine the vicinity and movements of a suspect. Judge Richard Allen Posner\textsuperscript{74} made a similar point discussing the implications of mass surveillance, GPS, and advances in technology:

The new technologies enable, as the old (because of expense) do not, wholesale surveillance . . . It would be premature to rule that such a program of mass surveillance [of public movements] could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation’s roads.\textsuperscript{75}

Given that the Court has acknowledged society’s pervasive reliance on technology, particularly cell phones as a means of storing personal information, there is a strong argument to be made that the third-party doctrine should be revisited given that many of our financial transactions are done through apps and stored in cyberspace. Individuals now use fintech (e.g., send payments, shop, invest, bank through their bank’s website, or lend money to a friend—all online) and download the corresponding apps that allow them to conduct these transactions.

Through the pervasive use of fintech platforms, individuals will generate millions of data points through their financial transactions ranging from the bank records tracking the whereabouts of individuals at all times through their debit card use to the apps that store transaction information, such as purchases, dates, and times. The information generated through the use of these technologies reveals many intricate details pushing in favor of reevaluating the third-party doctrine as it applies to financial transactions.

**OTHER PRIVACY PROTECTIONS ARE INSUFFICIENT FOR FINANCIAL PRIVACY**

Besides case law lagging behind technological advancement, the existing statutory protections for financial information are insufficient to protect an individual’s privacy in an age of pervasive data collection. The Right to Financial Privacy Act of 1978 (“RFPA”) protects the confidentiality of personal financial records by attempting to create a statutory Fourth

\textsuperscript{74} Former Chief Judge of the United States Court of Appeals for the Seventh Circuit from August 1, 1993–August 1, 2000.

\textsuperscript{75} United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).
Amendment protection for bank records.\(^{76}\) The RFPA requires the government to provide an individual with notice and an opportunity to object before his or her bank or other financial institution discloses an individual’s financial information to the government for law enforcement purposes.\(^{77}\)

The RFPA was enacted as a response to \textit{Miller}, and was meant to protect against unwarranted and unrestricted government access.\(^{78}\) However, the RFPA contains several exceptions that the government can use to sidestep the statute’s safeguards. These exceptions are (1) disclosures that do not identify a particular customer; (2) disclosures that benefit the financial institution, including its security interests, government loans, and other disclosures relevant to possible violations of the law; (3) disclosures in connection with supervisory investigations and proceedings; (4) disclosures under the tax privacy provisions; (5) disclosures pursuant to other federal statutes or rules, administrative or judicial proceedings, and legitimate functions of supervisory agencies; and (6) emergency disclosures and disclosure to federal agencies charged with foreign intelligence or counter intelligence or other national security protective functions.\(^{79}\) As a result of these exceptions, there are hardly powerful restrictions on the government’s ability to obtain an individual’s financial records.\(^{80}\)

To fintech users, the most jarring of these exceptions is disclosures in accordance with any federal statute. This exception allows banks and other financial institutions to disclose its users’ financial data under the Bank Secrecy Act.\(^{81}\) This Act, initially at issue in \textit{Miller}, allowed the Court to justify its holding that individuals have no reasonable expectation of privacy in their bank information because their banks and other financial institutions are required to keep records under this federal statute. Other glaring issues under the RFPA include the exception allowing the disclosure of this data

\(^{76}\) 12 U.S.C. §§ 3401-3422.


\(^{78}\) Id.


\(^{80}\) See Michael W. Price, \textit{Rethinking Privacy: Fourth Amendment “Papers” and the Third-Party Doctrine}, 8 J. Nat’l Sec. L. & Pol’y 247, 265 (2015) (explaining how congressional alarm over the implications of the third party doctrine has resulted in legislation affording privacy to some categories of third-party records yet these efforts have been undermined by changing technologies).

\(^{81}\) \textit{Fed. Reserve Bd.}, supra note 77.
when foreign intelligence investigations are at issue. This exception has the potential to be applied indefinitely without a way to limit its reach.

A SOLUTION TO PROTECTING THE PRIVACY OF AN INDIVIDUAL’S FINANCIAL INFORMATION

The Court should consider modifying—but not abandoning—the third-party doctrine to better reconcile the privacy interests that individuals have in their financial information and metadata today. Specifically, the current third-party doctrine does not separate situations where the government obtains information that is intrusive or sensitive.

I. Intrusive: This category describes situations where the government encroaches on an individual’s physical space or goes through a third party to acquire an individual’s data. An example of this category of data is if the government receives access to an individual’s financial records from his/her bank without his/her consent; and

II. Sensitive: Several scholars disagree as to the nuances of the definition of sensitive information but most agree that the definition describes information that can be used to enable privacy or security harm when placed in the wrong hands. Presumably, this category involves information that individuals would not knowingly broadcast to the world and would not want others to see because of the harm it may cause if the information is spread. The category includes inherently sensitive information and inerentially sensitive information.

a. Inherently sensitive information: describes “information that causes concrete harm merely by being known to another”, such as information we often regard as embarrassing, humiliating or abasing, like health information.

---

82 See generally Paul Ohm, Sensitive Information, 88 S. Cal. L. Rev. 1125 (2015) (concluding that different categories of sensitive information need more protection than others depending on the privacy harms they bring individuals, and devising a taxonomy for information of varying sensitivity). Since there is considerable debate as to how sensitive information is defined, I use Professor Ohm’s definitions because they are in line with the type of information intended to be protected under the Fourth Amendment. However, in my proposed framework, I do not distinguish between the two types of sensitive information he defines because I leave it up to the courts to determine whether a distinction is warranted depending on the factual situations at issue.

83 Id. at 1170.

84 Id.
b. **Inferentially sensitive information:** describes information “connected to harm through at least one inferential or predictive step” like past criminal conduct, “not only for the inherent shame sometimes associated with criminal activity but also for the possibility of future danger or recidivism.” An example of this type of data is data from an offender’s Amazon account, including all of his or her search and purchase history, that law enforcement uses in a sentencing memorandum to predict his or her rate of recidivism.

Under this model, data is divided into four groups: 1) sensitive, intrusive; 2) non-sensitive, intrusive; 3) non-sensitive, non-intrusive; and 4) sensitive, non-intrusive. This would allow judges to classify which category the data falls into. This section will explain each of the categories under the following diagram and provide examples of each of these groups of data.

**Figure I: Categories of Data**

<table>
<thead>
<tr>
<th>Intrusive</th>
<th>Non-Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive</td>
<td>Non-Sensitive</td>
</tr>
<tr>
<td>Non-Intrusive</td>
<td></td>
</tr>
</tbody>
</table>

A. **Intrusive, Sensitive Data**

The top left-hand corner represents sensitive and intrusive data. The “sensitive” aspect of this category involves information that individuals do not knowingly broadcast to the world and would not want others to see because of its potential to cause privacy or security harm when placed in the wrong hands. The “intrusive” component of this category involves law enforcement impeding into an individual’s physical or digital space to obtain this information.

---

85 Id.
86 Id.
An example of intrusive, sensitive data is personal financial records on Angie’s computer, including mortgage paperwork citing her earning potential, debt, and bank statements that tell a story of where she has traveled and what she purchased over time, that law enforcement obtained without her consent. In this category, law enforcement accessed Angie’s digital space, without consent, to acquire information (the financial records) that Angie did not want the world to see. In the wrong hands, the release of Angie’s financial records can lead to identity theft, fraud, and embarrassment. Angie did her best to store this information in a place where she would not expect anyone to have access to unless the intruder broke into her home or personal computer, which are Angie’s “home” and “effects” respectively for purposes of the Fourth Amendment.

Test

In situations like these, the courts should use the tangible invasion of privacy standard reaffirmed in Jones to determine whether the government committed a digital trespass to acquire private information. This means the court must assess whether there was a tangible invasion of privacy to acquire the data at issue. In the example above, after applying the Jones test, a court would hold that law enforcement committed a digital trespass to acquire Angie’s financial records because they accessed Angie’s computer without a warrant or her consent.

B. Intrusive, Non-Sensitive Data

The top right-hand corner is intrusive, non-sensitive data. This is data that individuals voluntarily broadcast to the world but which can still be obtained by law enforcement hacking into an individual’s physical or digital space or effects. Intrusive, non-sensitive data includes Nora’s past or present locations from her Fitbit® GPS tracker, which law enforcement obtains on the app, through a third party without a warrant. Because law enforcement went through a third party, and did not have a warrant, to obtain this data and intruded in Nora’s digital space to obtain this information, the data was collected in an intrusive manner. The information itself was not private

87 Fitbits are wireless, activity trackers that measure number of steps walked, heart rate, sleep quality, steps climbed, and other personal metrics involved in fitness. Who We Are, FITBIT, https://www.fitbit.com/about (last visited Apr. 1, 2017) [https://perma.cc/MJF6-5BEV].
because Nora was recording it for her personal use but, at the same time, she was protecting this data in her digital space.

Test

When law enforcement invades an individual’s digital space or effects, the test should be the tangible invasion of privacy standard reaffirmed in Jones in order to determine whether law enforcement had probable cause or a warrant to enter, or trespassed into an individual’s space. In the example above, after applying the Jones holding, a court would hold that law enforcement trespassed into Nora’s digital space because it accessed her password-protected Fitbit account to obtain her past and present location information without a warrant or her consent.

C. Non-Sensitive, Non-Intrusive Data

The bottom right-hand corner is non-intrusive, non-sensitive data: data that individuals voluntarily reveal to the world or would not mind sharing. To acquire this type of data, law enforcement need not hack into a website, app, or personal device. Non-private, non-intrusive data is a list of all timestamps from Leith’s Venmo payments which are displayed on his public Facebook profile. Law enforcement neither hacked into Facebook nor went through a third party without a warrant to obtain this information, and they did not collect data that was meant to be private. The individual voluntarily posted this information for the public to access and see.

Test

When law enforcement obtains data that is neither sensitive nor obtained in an intrusive way, the court should use the third-party doctrine as it exists to evaluate whether law enforcement conducted an unreasonable search. In the example above, a court would hold that law enforcement was rightfully permitted under the third-party doctrine to obtain the time stamps, including the financial payment information, from Leith’s public Facebook posts because Leith posted the information publicly and did nothing to protect it. Additionally, law enforcement did not impede on Leith’s digital space or personal effects. A government agent merely viewed Leith’s public profile.

D. Sensitive, Non-Intrusive Data
Sensitive, non-intrusive data is the most difficult category to analyze. In these situations, law enforcement collects sensitive information but does so in a non-intrusive, non-trespassory manner. This could arise if law enforcement used a public library computer to view the search history of a previous patron.

This scenario is the most challenging because law enforcement does not commit a trespass: the tangible invasion of privacy standard reaffirmed in Jones would not apply. The Court would have to use the Katz test to determine whether an individual had a subjective expectation of privacy in the sensitive data he or she accessed and whether there was an objective expectation of privacy in the individual’s data. When applying the test, the Court should consider the following factors:

1. Whether this information is considered “personal” (meaning, whether a reasonable person would feel that law enforcement intruded on his or her personal privacy such that he or she would be embarrassed, uncomfortable, or vulnerable should this data be revealed to the public);
2. Whether the government used readily-available mechanisms to access the information (i.e. was there a technology used to access information on the computer or did the government simply look at the readily available search history); and
3. What type of analysis could be conducted on that data.

The first factor upholds the longstanding notion that an individual has a right to intellectual privacy, both under the Fourth Amendment’s protection of privacy interests, and the First Amendment’s protection of free expression and association. The second factor allows the courts to balance whether the government had other means to obtain the information that it did. This can help the courts determine whether the government could have obtained a search warrant, used technology unavailable to the public or obtained the

89 The Court has supported the concept that an individual not only has the ability to think freely, but also express him or herself freely from government interference. See Stanley v. Georgia 394 U.S. 557 (1969) (holding that law enforcement exceeded the scope of a warrant to search the defendant's home by viewing a defendant's videos and that protecting the individual's intellectual privacy rights under the First Amendment were more important in this case than prosecuting the defendant for a crime outside the scope of the warrant).
information simply due to the individual’s negligence. The third factor allows the courts to determine how much information the data reveals about the individual and whether a narrow or broad analysis can be conducted on this data. This will help the courts balance an individual’s privacy interests with the government’s interests.

Overview

The Court should use this data classification system to carve out additional Fourth Amendment protections to an individual’s right to privacy in the digital age. By classifying data using a sensitive/intrusive distinction, the Court will be able to reconcile the existing tangible invasion of privacy standard reaffirmed in Jones, the reasonable expectation of privacy test, and the third-party doctrine. This data classification system will be better suited to protect individuals and their financial communications and transactions passing through certain spaces or transmitted through certain activities. The third-party doctrine will no longer have a blanket application and will restrict law enforcement’s ability to obtain data passed through to third parties. This restriction will protect certain types of data—data containing private communications by payment and retail platforms, other financial platforms, and apps—and consider any precautions individuals took to protect this information.

The following is an example demonstrating how the proposed classification system would apply to analyze whether the government’s conduct constitutes an unreasonable search of an individual’s financial data.

A. Example: Amazon iCloud Hack

Assume the Amazon iCloud hacked. The Amazon iCloud platform contains all of the financial information, purchase history, and past searches of its users, all of which is stolen by hackers. The information particularly at issue is information acquired by Echo assisting individuals in their financial transactions, including purchasing personal items and gifts for family members and friends. Assume, law enforcement is able to track down this information. Based on the current third-party doctrine, there would be no expectation of privacy in this data because users consented to the terms and conditions of Amazon and gave their information to the company via the data platform. They also consented to bringing Amazon Echo into their homes.
However, under this Note’s new framework, the data would first be classified by the criteria explained above.

First, a court must determine whether the government was intrusive when collecting this data. Because law enforcement did not obtain this information by hacking into the Amazon iCloud directly or accessing an individual’s Echo device, it inadvertently received the information directly from a third party (the hackers who put it online). Arguably, it found this information once the platform was hacked so arguably, no intrusion occurred. Since this data is non-intrusive, we move from row 1 to row 2.

The court must now move on to the question of whether the data acquired was sensitive or non-sensitive. A reasonable person likely would not want to reveal the information contained in his or her Amazon Echo search or browsing and purchase history, which is why these accounts are password-protected. This information can also be considered sensitive because it may be embarrassing (depending on which products an individual is browsing), could be inherently shameful, could reveal private information about an individual’s life or preferences, and could also lead to future recidivism. A court could move away from classifying the data from non-sensitive to the sensitive category.

Because law enforcement accessed an Amazon user’s information without the user’s consent, and did so to obtain sensitive information, the Court could apply the non-intrusive-sensitive standard. Considering the Amazon Echo device was in an intimate location, the individual’s home, a reasonable person is likely to feel that the government intruded on his or her personal privacy by snooping around as to his or her thoughts and needs by viewing their browsing history and purchase history, organized by the data and time of these actions. Furthermore, a reasonable person in their home would be embarrassed if the government obtained information regarding the intimate and confidential details of their actions in the privacy and comfort of their own homes. With this information and the quantity of data, the government will have information as to an individual's discussions, behaviors, habits, and location. A court would rule that this information is extremely personal and an individual has a reasonable expectation of privacy in this data, particularly because of the data’s contents, quantity, and the place it was collected from. Therefore, the government conducted an unreasonable search by obtaining this information from the third party.

In this example, this classification system reaffirms core Fourth Amendment values by upholding *Katz*’s reasonable expectation of privacy standard and examining the totality of circumstances surrounding the data.
This includes the type of data obtained, the place from which the information was acquired, and an individual's attempt to protect access to the information. Here, the analysis hinges on what information is revealed and how law enforcement obtained access to this information.

B. Addressing Counter-Arguments

Critics may argue that this classification system does not adequately balance law enforcement’s interests and an individual’s right to privacy because it creates too high a bar for government investigation. However, this classification system does not eliminate the current third-party doctrine. It merely limits its applicability to particular types of financial data and considers the realities of digital spaces used to store data. The classification system also considers the existing Katz and Jones doctrines and their applications to an individual’s digital effects in the modern age.

Several administrability arguments can be made against the imposition of this classification system, such as the increased burden on the government to obtain warrants and the lack of flexibility in obtaining information from third parties. Law enforcement currently uses the third-party doctrine as a general warrant, allowing the government access to certain financial information passed through to third parties. However, a core value of the Fourth Amendment is to ensure that the government does not have sweeping authority to collect a citizen’s information or property, which is what is currently done under the third-party doctrine. When the Founding Fathers added the Bill of Rights to the Constitution in 1791, the country codified what society believed was essential to an individual’s liberty: the notion that individuals should be protected from unlawful government intrusions without particularized warrants and probable cause. This Amendment was created to protect American citizens from the type of government invasions rampant under King George that allowed British soldiers to invade the colonists’ homes in search of anti-monarchists. The classification system above takes the Founders’ values into account by considering the nature of the financial information and whether the data can be used to harm the individual and considers where the government obtained the information to determine whether it encroached on an individual’s physical or digital space.

Critics may also argue that this classification system itself is too flexible, less predictable, and prone to judicial abuse. However, this test is

---

narrower than the reasonable expectation of privacy test in that it groups data into particular categories and puts the government on notice as to what categories a court will use to determine whether an unreasonable search has occurred. This system will be more responsive to a defendant’s individual circumstances and will be more likely to promote fairness to the parties—unlike the current third-party doctrine, which allows the government to obtain an individual’s information, which he or she voluntarily hands over to third parties, without a warrant.

Finally, critics may argue that well-informed consumers can choose a company or service with better privacy policies if they do not agree with a company’s terms of service. However, even if individuals agree to a company’s terms of service, individuals expect that companies will keep their financial information in their password-protected accounts private and will not reveal it to the government without a warrant. Consumer expectations of this privacy have come to the spotlight since the Snowden and San Bernardino incidents.91 Today, creating a password-protected account to store information is comparable to storing papers in a lock box where only the owner has the key.92 In this scenario, the government is required to obtain a warrant to compel an individual to hand over the key. The government should be required to acquire a particularized warrant to obtain the information stored in a password-protected digital account in the same way they are required to obtain the key to a physical lock box.

CONCLUSION

As fintech platforms increase, it will fall to the Supreme Court to ensure that Fourth Amendment jurisprudence continues to uphold society’s values of an individual’s financial privacy in the digital age. The current

92 See People v. Snipe, 841 N.Y.S.2d 763, 770-772 (N.Y. Sup. Ct. 2007) (holding that the defendant’s mother had no authority to consent to the defendant’s closet, containing a lock, because the defendant did not provide his mother with a key.) This is similar to how a third party cannot consent on behalf of its user to provide the contents of a password-protected account The difference is he had not entrusted the care of the contents of the box to his mother. She still probably could not just guess passwords until she got it right or reset it or whatever. See also David D. Thomas, Dangerously Sidestepping the Fourth Amendment: How Courts Are Allowing Third-Party Consent to Bypass Warrants for Searching Password-Protected Computer, 57 CLEV. ST. L. REV. 279 (2009).
doctrines are ill-equipped to incorporate the modern Fourth Amendment values of protecting an individual’s privacy in their financial data with today’s fintech landscape. Given the pervasiveness and reliance on digital financial services and apps, the financial privacy of individuals is at risk. It is time for the Supreme Court, and the broader legal community, to revise Fourth Amendment jurisprudence for the modern digital age.
INTRODUCTION

Since the release of Bitcoin in 2009, the cryptocurrency has grown in prominence and public acceptance.\(^1\) By seemingly providing a layer of anonymity in transactions, Bitcoin has also become the public face of virtual currencies in illicit online dealings: Bitcoin has been associated with several high-profile criminal cases involving major drug website shutdowns, notably the Silk Road marketplace.\(^2\) However, few cases have addressed how existing statutes and regulations should apply to this new technology. The foundations upon which Bitcoin is built were only made possible by modern technology. As such, Bitcoin defies traditional categorization: its effectiveness as a reliable method of buying and selling goods has led some to embrace it as a


monetary device, while its novelty, decentralization, and volatility has left some courts hesitant to designate it as money.

This tension is visible in the different ways that courts and various agencies treat virtual currencies. For instance, the U.S. Securities and Exchange Commission (“SEC”) regulates Bitcoin as money in legal actions while Internal Revenue Service (“IRS”) official guidance designates it as property. FinCEN laid out guidelines in 2013, regulating “convertible virtual currencies” similar to money under to money transmission services, but noting key differences such as the ability to create currency. In United States v. Faiella, the Southern District of New York followed in the footsteps of SEC v. Shavers, determining that Bitcoin is money and applying federal money transmitting statutes accordingly while a Florida state court shied away from dubbing Bitcoin money, and instead have asked legislatures to redefine old statutes to better account for the new technology.

This comment addresses why the court in Faiella was correct in determining that Bitcoin is money and applying legal standards of money to Bitcoin transactions. In doing so, the comment explores the function, purpose, and attributes of Bitcoin, compares those attributes to those of traditional money, and observes various standards applied by courts grappling with the new concepts introduced by Bitcoin and other virtual currencies. Finally, the comment observes the increasingly complex implications of virtual currencies, and discusses how courts and legislatures may need to react.

STATUTORY BACKGROUND AND PROCEDURAL HISTORY

Silk Road was an online marketplace that exclusively allowed users to anonymously buy and sell goods and services. Robert Faiella, known online as “BTCKing,” operated an exchange for buyers to anonymously purchase

---

bitcoins and have them deposited into a Silk Road account. Faiella’s service allowed buyers to deposit traditional currency into a bank account controlled by Faiella, and Faiella would then deposit a corresponding amount of Bitcoin directly into the user’s Silk Road account.

In 2013, the Federal Bureau of Investigation ("FBI") shut down Silk Road and prosecuted the prominent individuals associated with the website’s operation. Though Faiella was not associated with the operation of the site, his prominent role facilitating transactions by transforming USD into Bitcoin placed him in the crosshairs, and Faiella was indicted for conspiracy to commit money laundering and failing to properly license his business as a money transmitting service in violation of 18 U.S.C. § 1960, which forbids operating an “unlicensed money transmitting business.” This comment focuses on the charge of operating an unlicensed money transmitting business. Faiella asked the court to dismiss that charge on three grounds: first, that Bitcoin does not qualify as “money” or “funds;” second, operating a Bitcoin exchange did not constitute “transmitting” money; and third, that Faiella is not a “money transmitter” as defined in § 1960.

The court explained that the legislative history of § 1960 shows it was intended to apply broadly to “nonbank financial institutions” that could “convert street currency into monetary instruments” used in drug and other illicit transactions by “any and all means.” The court stressed that “any and all means” indicated that Congress intended prosecutors to read the statute broadly “to keep pace with . . . evolving threats.” Using this language to emphasize that the statute is to be interpreted broadly, the court ultimately concludes that Bitcoin can be considered money and its use should be regulated under the money transmitter statute.

---

9 Id. at 546.
10 Id.
11 See, e.g., United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (denying a motion to dismiss in the government’s prosecution of Silk Road creator and operator).
13 Id.
14 Id. at 545-46.
15 Id.
16 Id.
TECHNOLOGICAL HISTORY

Bitcoin

Bitcoin was first introduced through a whitepaper penned under the pseudonym Satoshi Nakamoto in 2008, and was subsequently launched in 2009. Bitcoin operates through blockchain technology, a distributed system for performing, validating, and recording transactions. As set out in the Satoshi whitepaper, Bitcoin is meant to be a “purely peer-to-peer version of electronic cash [to] allow online payments to be sent directly from one party to another without going through a financial institution.” Since Bitcoin relies on non-reversible transactions permanently recorded in a public blockchain, users rely on the entire Bitcoin network to validate that each bitcoin is real and truly belongs to the buyer: that is, that the bitcoin was not already spent elsewhere.

The Bitcoin blockchain is similar to a public ledger that contains each and every transaction since the inception of Bitcoin. If the whole blockchain is a ledger, then each “block” in the chain is a page of transactions that have been verified together by the network. Once a block has been added to the blockchain, it is practically impossible to change. Consequently, each

---

19 Blockchain technology is a type of distributed ledger technology, which uses a distributed set of nodes, all running compatible software, that share and verify information based on pre-defined rules. Transactions and records are verified by the nodes and grouped into a “block,” which is connected to the block before it, creating a chain of blocks, or “blockchain.” Blockchain features vary widely based on how each system is designed and operated.
20 The Bitcoin blockchain uses a permissionless distributed network to verify Bitcoin transaction based on agreed-upon principles. This blockchain stores every transaction in a publicly-available ledger, one block at a time. A Bitcoin block is a group of transactions that have been verified by the network and which a node of the network has encoded by finding a rare number based on hash technology. Each block is “chained” to the block before it, so that every verified transaction can be traced back to the inception of Bitcoin’s blockchain. See generally Nakamoto, supra note 17.
21 Id.
22 Id. at 2.
23 If a single malicious actor controls more than 51% of the computing power of the blockchain, it may be able to approve false transactions at a faster rate than the rest of the network. Id. at 6-8. However, since the value of Bitcoin is based on trusting the network
bitcoin’s history can be traced back to its creation. Buyers and sellers can rely on this chain of authentication to verify that the bitcoins they receive actually belong to the person claiming to own them, and have not been spent already. This mechanism allows bitcoin users to avoid third-party financial institutions, such as banks, since transactions are verified and approved by the blockchain network. 24 Instead, the computers running the Bitcoin software communicate with each other to verify that a transaction is valid according to agreed-upon criteria and to verify that the bitcoins in question still belong to the buyer. 25

Each bitcoin is located at an “address” that can be seen by anyone who looks at the blockchain. 26 In order to spend the bitcoin located at that address, the user must have a unique “private key.” 27 Whomever has access to the private key may spend the bitcoins located at the corresponding address. 28

Finally, scarcity is a foundational aspect of Bitcoin. By design, there are an explicitly-defined finite number of bitcoins. 29 These bitcoins will be released at a predictable rate over the course of more than 100 years. 30 This slow, methodical release of bitcoins and a known cap on the total released instead of trusting an individual, this would likely cause the value of Bitcoin to collapse and lead users to abandon the cryptocurrency.

24 Id. at 1-3.
26 The address is a hash of the user’s public key. Asymmetric encryption systems generate keys in pairs: a public key and a private key. The public key can be accessed by anyone, while the private key should be kept secret only to the user. Any file encrypted with the public key may only be unencrypted by the corresponding private key. The Bitcoin blockchain takes advantage of this feature, allowing anyone to send bitcoins to an address (through the public key), but only allowing the user with the private key to spend the bitcoins at that address. This does mean that if you lose your private key, the bitcoins can never be spent, and if you if your private key is stolen, the thief may spend the bitcoins associated with that private key. Id. at 2.
27 Id.
28 Relevant to the court’s discussion of whether Faiella was a transmitter, Silk Road held the private key to users’ bitcoins and had authority to suspend or block the account owner from spending their bitcoins. Faiella, 39 F. Supp. 3d at 545 (“These were, in essence, transfers to a third-party agent, Silk Road, for Silk Road users did not have full control over the Bitcoins transferred into their accounts.”).
29 It is, in fact, possible for the cap to be raised through consensus of Bitcoin users, but this would reverse a founding principle of the Bitcoin community. While it is not possible to anticipate what may happen in the Bitcoin community over the next 100 years, this comment assumes that the cap will not be raised, and that scarcity will be maintained as currently defined in the Bitcoin system.
means that bitcoins will never “flood the market” and that, upon final release, inflation of bitcoins cannot occur.\textsuperscript{31} Accordingly, the value of Bitcoin is based on how users value the currency, and that value will be determined entirely by the users without the possibility of manipulation by an issuing authority.

\textit{Silk Road}

Silk Road was an online marketplace that used Bitcoin to allow users to purchase goods anonymously.\textsuperscript{32} Silk Road required users to deposit Bitcoin into their Silk Road accounts,\textsuperscript{33} Silk Road maintained the account, and could restrict a user’s access to the bitcoins in the account.\textsuperscript{34}

\textbf{ANALYSIS}

To determine how Bitcoin should be treated from a regulatory standpoint, this comment first determines that the \textit{Faiella} court acted correctly in defining Bitcoin as money. Second, the comment analyzes the unique non-money attributes of Bitcoin and other virtual currencies. Finally, the comment observes recent developments in the regulation of Bitcoin and potential trends for the future.

\textbf{A. Bitcoin Constitutes Money}

In determining that Bitcoin is money, the \textit{Faiella} court spends a single paragraph defining money and just two sentences determining that Bitcoin qualifies as money under 18 U.S.C. § 1960.\textsuperscript{35} The court dismisses the notion of any perceived ambiguities in its interpretation and ultimately determines that Faiella is a money transmitter.\textsuperscript{36}

Despite Faiella’s arguments to the contrary, the court properly identified Bitcoin as “money.” First, Bitcoin is intended to be used as money; second, Bitcoin qualifies as money under both legal definitions and plain

\textsuperscript{31} Id.
\textsuperscript{33} Chloe Albanesius, \textit{What Was Silk Road and How Did It Work?}, PC MAG (Oct. 3, 2013, 12:55 PM), http://www.pcmag.com/article2/0,2817,2425184,00.asp [https://perma.cc/XM5U-C9HF].
\textsuperscript{34} Id.
\textsuperscript{36} Id. at 545-47.
meaning definitions; finally, because Bitcoin shares so many characteristics in common with money, it would cause a regulatory gap if it were not recognized as money.

1. **Bitcoin is meant to be used as money**

Bitcoin’s use as money is not a creative or unexpected offshoot of the technology or an improvised bartering tool:37 Bitcoin is intended to be used to buy and sell goods and services, and Bitcoin is in fact used for that purpose. The first whitepaper released on the topic confirms this intended purpose: *Bitcoin: A Peer-to-Peer Electronic Cash System*.38 Bitcoin is intended to be cash. Further, as the court notes in *Faiella*, “Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions.”39 This intent may not be relevant if Bitcoin did not contain the requisite qualities of money, but in determining whether an item represents money, intent does matter.40 Its other attributes are designed specifically to circumvent trusted middlemen, governments, and banks,41 but at its core Bitcoin provides the end user with the ability to transact in a manner similar to fiat currencies.

2. **Bitcoin Qualifies as Money Under Both the Legal and Plain Meaning Definitions**

The acceptance of Bitcoin as a stored value that can be traded for goods and services fits the plain-English definition of money or funds, which the court identified as the appropriate definitions to be apply in this instance.42 Money is not defined in § 1960,43 so both parties in *Faiella* offered definitions

---

38 Nakamoto, *supra* note 17, at 1.
39 *Faiella*, 39 F. Supp. 3d at 545.
41 Nakamoto, *supra* note 17, at 1.
42 *Faiella*, 39 F. Supp 3d at 545 (rejecting both parties’ use of Black’s Law Dictionary to define the terms “money” and “funds,” stating that each “are ordinary English words and should be given their ordinary meanings”).
from Black’s Law Dictionary. Faiella suggested defining money as “[a]ssets that can be easily converted into cash” and “[t]he medium of exchange authorized or adopted by a government as part of its currency; esp. domestic currency.” Faiella argued that, if allowed to apply to Bitcoin, this statute could apply to “any asset with liquidity,” and would render the statute meaningless. The government notes, however, that the definition of money transmitting “speaks of transferring not ‘cash’ or ‘currency,’ but ‘funds.’” The government then looked to both Black’s Law Dictionary and the Oxford English Dictionary, defining funds as “money at a person’s disposal; pecuniary resources.”

Regardless, the Faiella court stated that legal definitions “would only be relevant if Congress intended that these terms be given special meanings as legal ‘terms of art,’” and instead applies the ordinary meanings of the words money and funds. The court defined money as “something generally accepted as a medium of exchange, a measure of value, or a means of payment,” and defined funds as “available money.” The court then identifies attributes of Bitcoin that fit each of the three qualifiers in the ordinary definition of money: for medium of exchange, Bitcoin “can easily be purchased in exchange for ordinary currency;” for a measure of value, Bitcoin “acts as a denominator of value;” and for a means of payment, Bitcoin “is used to conduct financial transactions.” The court in SEC v. Shavers similarly interpreted Bitcoin to be money because of its ease of use in typical transactions and because it can easily be exchanged for typical currencies.

---

44 Memorandum of Law in Support of Defendant Robert Faiella’s Motion to Dismiss Count One of the Indictment at 3-4, United States v. Faiella, 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (No. 14 Crim. 243) (Motion to Dismiss); Memorandum of Law in Opposition to Defendant’s Motion to Dismiss Count One of the Indictment at 3-4, 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (No. 14 Crim. 243) (Opposition Memorandum).
45 Motion to Dismiss, supra note 44, at 3-4 (citing BLACK’S LAW DICTIONARY (9th ed. 2009)).
46 Id. at 4.
47 Opposition Memorandum, supra note 44, at 10.
48 Opposition Memorandum, supra note 44, at 8.
50 Id. at 545; see also Funds, MERRIAM-WEBSTER ONLINE, https://www.merriam-webster.com/dictionary/funds (last visited Mar. 19, 2017) [https://perma.cc/PH8R-CMSR] (updating the definition of funds to mean “available pecuniary resources,” and defining pecuniary resources as “of or relating to money”).
51 Faiella, 39 F. Supp. 3d at 545.
While the court’s cursory round of fitting square pegs into square holes adequately dispenses Faiella’s argument, it leaves unaddressed the root of Faiella’s confusion. Dictionary definitions seem to demonstrate a circularity in the definition of money, cash, currency, and funds: each refers to the others, and all roads lead back to the elusive “medium of exchange.”

Most differences between the definitions can boil down to when the money is available and where the money is used. The difficulty arises from the ubiquity of government-issued money; most have likely never used any other medium of exchange, and for good reason. Until recently, society did not have the ability to create a unique medium of exchange that did not have a secondary purpose other than its purpose as money, or the creation of such a token was illegal. In the United


54 See Funds, supra note 53 (specifying that the resource must be available); Cash, supra note 53 (specifying that the resource must be ready at the time of purchase).

55 For instance, currency that must be accepted in one country but cannot be accepted in another. See Legal Tender, MERRIAM-WEBSTER ONLINE, https://www.merriam-webster.com/dictionary/legal%20tender (last visited Apr. 1, 2017) [https://perma.cc/4LT6-7BNN] (defining legal tender as “money that is legally valid for the payment of debts and that must be accepted for that purpose when offered”).
States, for instance, only the federal government may coin money, and other easily-identifiable physical representations of money are strictly regulated.\footnote{U.S. CONST. art I, § 8 (“Congress shall have the power to . . . coin money, regulate the value thereof” and “provide for the punishment of counterfeiting the securities and current coin of the United States”); see also 18 U.S.C. Ch. 25 (2012) (criminalizing counterfeiting and forgery of United States currency).}

So why not call Bitcoin a commodity, as Faiella suggests?\footnote{Memorandum of Law in Support, supra note 44, at 1 (“Bitcoin is a privately created commodity, acquired—or ‘mined’—by solving mathematical problems generated by a software algorithm.”).} Bitcoin’s lack of useful physical form may be the distinction that sets it apart. A bilateral exchange of goods that does not include money is bartering. Bitcoin, in its purest form, is merely a public piece of information that everyone can see. The bitcoin’s value derives from the fact that everyone can see it, and therefore trust that it has not been transferred, and someone can transfer it. If you have the key to transfer the information, then you can access its value. If the key for a given bitcoin is lost, that bitcoin becomes valueless, destined to sit in its assigned address until the blockchain ceases to exist. By common definition, commodities have value in trade.\footnote{See Commodity, MERRIAM-WEBSTER ONLINE, https://www.merriam-webster.com/dictionary/commodity (last visited Apr. 1, 2017) [https://perma.cc/9K65-BHG4] (defining legal tender as “an economic good” or “something useful or valued”).} While the U.S. Commodity Futures Trading Commission (CFTC) classified Bitcoin as a commodity in 2015 to bring it under the purview of the Commodity Exchange Act (CEA),\footnote{7 U.S.C. § 1(a)(9) (2012) (“The term “commodity” means wheat, cotton, rice, . . . cottonseed, . . . and all other goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in.”).} its definition of commodity is extraordinarily expansive and designed to give wide regulatory authority over futures markets.\footnote{Press Release, Commodity Futures Trading Comm’n, CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering (Sep. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 [https://perma.cc/F7KW-PXNF].} This classification should be viewed as a need to regulate the space, which the author agrees is necessary, rather than an identification of virtual currencies as commodities as historically understood.\footnote{Further, as discussed infra The Future of Virtual Currencies, Bitcoin and other virtual currencies may be used to represent commodities or contracts which would typically fall under CFTC purview and which would potentially evade CFTC jurisdiction if not for the reclassification.} Without physical form, if a bitcoin ceases to be...
transferable, it ceases to have value. Because of this lack of any secondary value, Bitcoin is not a commodity.

B. The Non-Monetary Attributes of Virtual Currencies Do Not Preclude Bitcoin’s Use as Money

The technology upon which Bitcoin is built gives it novel characteristics that are distinct from our historic conception of money. A few examples include the method of transaction validation, the ability to attach new information to a bitcoin on the Bitcoin blockchain, and the ability to change Bitcoin properties with proper consensus on the network. These features, and others, inexorably complicate the treatment of Bitcoin and other virtual currencies, but do not supersede Bitcoin’s qualification as money.

1. Virtual currencies may appear or change suddenly

Virtual currencies can spring suddenly into existence. The features and attributes of these currencies will vary, but anyone with sufficient knowledge can write a program to create a virtual currency—the difficult part is establishing a community to use that virtual currency. So, while a worthless virtual currency may appear suddenly, it is more interesting to observe what happens when an established virtual currency undergoes a drastic change, potentially resulting in a new virtual currency. In the two major instances of virtual currency splits, one which occurred and one which may soon occur, the scenarios are quite different but each enlightening.

Bitcoin nodes need not run the same software, but must apply the same validation rules, decided by consensus, for their transactions to be accepted by the other nodes.\(^6\) The Bitcoin community changes the consensus rules by adopting new software but continuing to accept the previous consensus rules until a sufficient portion of the network is running one software.\(^6\) Once a pre-defined sufficient percentage of users is running the new software, all those nodes switch to the new consensus rules.\(^6\) Any node that tried to implement the new software features before the switch would have been rejected by the


\(^6\) *Id.*

network as invalid; this protects the network from changes until there is significant acceptance.\textsuperscript{65} Any node that tries to use the old protocol after the switch is likewise rejected as invalid; this forces any hesitant adopters to update to the new protocol once it is active.\textsuperscript{66}

If two competing protocols are introduced, but neither receives buy-in sufficient to trigger the protocol change, the problem remains unsolved and factions may become restless. As of March 2017, Bitcoin is facing this existential crisis.\textsuperscript{67} multiple solutions were introduced to solve the mempool problem, a growing issue involving a backlog of unrecorded transactions, but no single solution has been popular enough to trigger a switch.\textsuperscript{68} Unexpectedly, or perhaps unavoidably, one community seems staunch enough and large enough to begin operating their own software, Bitcoin Unlimited (BTU), in opposition to the primary, Bitcoin Core (BTC).\textsuperscript{69} This would result in a “hard fork” in the Bitcoin blockchain: two incompatible software programs working from the same original blockchain base. Historic Bitcoin transactions would not be affected, but each new program, BTU and BTC, would build separate blockchains that stem from the same base.\textsuperscript{70} Each program will thus represent an entirely different virtual currency.

All transactions before the hard fork are respected as valid by both programs. After the hard fork, BTC nodes only acknowledge BTC and BTU nodes only acknowledge BTU. Critically, neither blockchain can merge back into the other. The hard fork presents two questions: first, which fork is legitimate; and second, would this sudden change preclude either from being considered money?

Which fork is legitimate? Both. Each is a completely unique virtual currency, and each will be valued according to its users’ perception of its value. So long as someone is running the software to validate and record the transactions, the virtual currency is a valid virtual currency. If that virtual

\textsuperscript{65} Bitcoin Developer Guide, supra note 62.
\textsuperscript{66} Id.
\textsuperscript{69} Id.
\textsuperscript{70} Hence the term “hard fork.” Fork because the single base blockchain supports two incompatible blockchains, and hard because there is no possibility of those blockchains merging back into one another.
currency can be accepted as a medium of exchange, then it is money. The value may shift significantly based on widespread usage, which is heavily dependent upon whether Bitcoin exchanges will accept the virtual currency: that is, whether BTU holders will be able to exchange it for traditional currency. Virtual currency exchanges have indicated that they will accept both BTU and BTC.\textsuperscript{71}

Does the ability to suddenly split into two distinct virtual currencies preclude Bitcoin from being considered money? If virtual currencies are money at all, then the answer to this question must be no. First, as established, anyone can develop a virtual currency and release it at any time; the important and difficult feature of money is having a society that is willing to trust that currency as a medium of exchange. Thus, since such a split is akin to a new virtual currency developing with a built-in trusted user base, there is no reason to treat the ability to split as a critical failure. Second, if the split virtual currency continues to meet the definition of money established above, and would be recognized as money had it not split, there is no reason to categorically deny the qualification of money just because a split is possible. So long as users run the program to validate the transactions and users continue to use these virtual currencies as a medium of exchange, the virtual currencies will remain money.

The discussion of what happens after a hard fork is not entirely theoretical. In June 2016, the Ethereum Project’s blockchain, Ethereum, was hacked and a substantial portion of its investment funds stolen.\textsuperscript{72} The Ethereum blockchain is significantly different from the Bitcoin blockchain, most notably here because it is maintained by a single entity, Ethereum Project. In response to the hack, Ethereum Project rolled back the blockchain to before the hack occurred, patched the vulnerability so that the hack could not happen, and operated the blockchain from that point forward, creating a fork of two universes: one where the hack did occur and one where the hack did not occur.\textsuperscript{73} Some nodes disagreed with the decision to hard fork the blockchain, and decided to continue operating the old program, operating in


\textsuperscript{73}Id.
the blockchain where the hack had occurred. These virtual currencies are now known as Ethereum (ETH) and Ethereum Classic (ETC). Both are respected by major exchanges and both represent a medium of exchange, though ETH is worth significantly more.

2. **Bitcoin Encoding Property**

Unique features of Bitcoin have been exploited to create unanticipated results. For instance, some users have permanently encoded photographs, speeches, and even the original Satoshi whitepaper into the Bitcoin blockchain. These actions require sending bitcoins to an unrecoverable address, essentially an address that no one knows the key to so that no one can ever move those bitcoins. As discussed, losing the private key for an address renders the associated bitcoins valueless; visible but inaccessible until Bitcoin stops existing.

Another example of a unique feature is the “coloring” of bitcoins. Essentially, this process encodes onto a particular bitcoin extra information that represents real-world assets, such as stocks or bonds. Transfer of these assets then uses the same process as a typical Bitcoin transaction and carries the same risks. While the bitcoin represents these assets, it also retains its normal value in the Bitcoin marketplace, but presumably would not be used for that purpose since the assets would be much more valuable.

Does the use of Bitcoin as a mechanism for representing non-money assets preclude Bitcoin from being money? This encoding is a completely new concept: until Bitcoin, pieces of money could not be used to represent

---

74 Id.
75 Id.
78 Id.
80 See id.
81 Colored coins use Bitcoin “dust,” which are quantities of Bitcoin so small as to be essentially worthless. See id.
unrelated assets. One dollar represented one dollar, and short of writing a contract on the back of that dollar, which may potentially invalidate the dollar, there was no way to reliably embed information. Here, the colored bitcoin in question does retain its value as money, but has a much more significant value as a stock or bond. The most logical conclusion seems to be that the colored bitcoin still qualifies as money, but may be subject to non-money regulations related to the assets it represents.

This conclusion introduces a critical new concept: that of treating Bitcoin as money and simultaneously regulating its non-money characteristics. While the non-money characteristics may be more significant to a particular bitcoin than that bitcoin’s value as money, its monetary value does not disappear. Abandoning the qualification of money for all of Bitcoin does not seem to make sense, and abandoning the qualification for a particular piece would open a quagmire of questions. For instance, at what ratio of money:non-money value should a colored bitcoin lose its qualification as money? Alternatively, if those values change over time, does that bitcoin once again qualify as money? What if the assets are still encoded but are no longer transferrable? Instead, legislators and regulators should adopt a regulatory approach with an appreciation for the innovation that these technologies invite, and a flexibility that provides for those unpredictable non-money characteristics. It is much more straightforward to treat all Bitcoin, colored or no, as money, and create a flexible framework that guides legal entities going forward.

THE FUTURE OF VIRTUAL CURRENCIES

The United States is collectively starting to see movement around virtual currency regulation. Though the federal agencies have differed in their approach to classification, most have felt the need to directly address virtual currencies. The SEC recently rejected an application to create a Bitcoin exchange-traded fund largely because of a lack of regulation in the Bitcoin space, perhaps signaling the need for more.\(^{82}\) The *Faiella* decision seems to encourage a trend that, with the exception of some state courts, recognizes the

---

importance of virtual currencies and identify them as money. Now, state legislatures have begun directly addressing the issue.

New York, rushing to license Bitcoin firms in 2015 received heavy criticism and quickly caused an “exodus” of small startups who could not afford the fees. In 2016, North Carolina passed the North Carolina Money Transmitters Act, regulating virtual currencies under money transmitter laws and explicitly carving out exceptions for unique virtual currency considerations, such as Bitcoin miners.

In early 2017, New Hampshire, possibly in direct response to a bitcoin exchange leaving the state due to regulatory burdens, is considering a bill that exempts virtual currencies from money transmitter laws. It is not the first state to do so, as Hawaii faced a similar shuttering of digital currency exchanges, and neither will likely be the last.

While states will inevitably take different approaches to virtual currency regulation, and some may misstep in the process, it is important for legislatures to directly address the advent of virtual currencies, even if they recognize and exempt from regulation. Though they may be classified as money, virtual currencies have enough unique, non-money characteristics that

---

they should be addressed head-on rather than shoehorned into existing statutes. Regardless of the steps taken afterward, a failure to classify virtual currencies, particularly Bitcoin, as money will lead to a regulatory gap that generates confusion in the long run.

CONCLUSION

The Faiella court was correct to determine that Bitcoin is money under 18 U.S.C. 1960, but this classification is just the tip of an iceberg. Virtual currencies’ non-money characteristics present a new challenge that has not been faced before, and that the federal and state legislatures are struggling to tackle. The current patchwork of regulatory classifications may not be unwarranted, given the non-money aspects of virtual currencies that could potentially become more prominent than their use as money. Especially in the case of Bitcoin, however, these agencies may consider applying more flexible classifications to account for the unforeseen and unforeseeable developments of virtual currencies.

The development of the Bitcoin blockchain and the blockchains of other virtual currencies is happening rapidly and shows no signs of slowing. While anticipating how these developments will occur is impossible, recognizing that virtual currencies cannot fit into preexisting frameworks for money transmission is vital. A failure to account for the new categories of technology that virtual currencies have made possible will result in regulatory gaps and confusion between prosecutors, agencies, and courts. Uncertainty in the industry could stifle adoption and hinder investment, and with the amount of innovation that has already been exhibited on the Bitcoin blockchain alone, it is not unreasonable to predict that innovation will continue.
INTRODUCTION

The patentability of business methods has become a controversial subject in recent years as technological advancements force legal scholars and policymakers to reconsider long-standing doctrines. Historically, the U.S. Patent and Trademark Office (“USPTO”) only granted business method patents on rare occasions because they were deemed to be abstractions beyond the confines of patent law.¹ Complicating matters further, Congress has never explicitly clarified the definition of a “business method.”² This lack of guidance has left the courts struggling to formulate a test that determines whether or not business methods qualify as patentable subject matter.

Most legal scholars agree that business methods were first mentioned as non-patentable inventions in Hotel Security Checking Co. v. Lorraine Co. back in 1908.³ Today, entrepreneurs and software coders seeking legal protection face formidable hurdles consistent with the historical view that, because business methods are abstract ideas, it would be “contrary to the spirit

---

³ See Hotel Sec. Checking Co. v. Lorraine Co., 160 F. 467, 469 (2d Cir. 1908).
of the patent law [. . .] to grant patents for [. . . these] analogous systems.”

Many existing software patents covering business methods have even been invalidated in recent years, pursuant to the Supreme Court’s ruling in Alice Corp. v. CLS Bank Int’l. In that case, the court held that a patent for an electronic third-party escrow service—created to reduce the settlement risk associated with financial transactions—was ineligible for patent protection because the invention failed to meet the rigid two-part eligibility test laid out in Mayo Collaborative Servs v. Prometheus Labs. As a result of the Alice Corp. decision, courts have overturned patents at a high rate for innovative methods that are arguably worthy of protection, such as a system that allowed users to exchange loyalty rewards points between different vendors.

However, for a brief window of time prior to Alice Corp., this trend was reversed as a result of the Federal Circuit’s 1998 ruling in State Street v. Signature Financial. After negotiations over a licensing agreement proved unsuccessful, State Street Bank brought an action against Signature Financial seeking a declaratory judgment that a patent was invalid on the grounds of unpatentable subject matter. The U.S. District Court of Massachusetts ruled in favor of State Street, and found that Signature’s technical method for using software to conduct mutual fund accounting existed as an exception to the otherwise broad delineations of 35 U.S.C. § 101. Reversing the district court’s summary judgment, the Federal Circuit attempted to clarify the confusion circling business methods and decisively “lay this ill-conceived exception to rest.” The Federal Circuit ruled that although a mathematical algorithm is an abstract idea, its application as a business method was patentable because it satisfied the useful-concrete-tangible test. This contrasted with the Mayo-Alice test, which centered upon determining whether the subject matter in question was a “patent-ineligible concept”, and if so, whether its elements “transform[ed] that abstract idea into a patent-

4 Ex parte Abraham, 1869 C.D. 59.
9 Id. at 1376.
10 Id. at 1375.
11 Id. at 1374.
eligible invention.” Following *State Street*, applications for software patents increased from nearly 700 in 1996 to approximately 1,300 in 1998.\(^\text{13}\)

This comment analyzes the Federal Circuit’s reversal and concludes that although the court was correct in holding Signature’s invention to be a patentable financial process and eradicating the business methods exception, the Federal Circuit unintentionally created an unnecessary test instead of relying on the text of the statute. By remanding, the court moved closer to striking the proper balance between protecting sophisticated inventions and preventing monopolies over ideas,\(^\text{14}\) but missed an opportunity to narrow the scope of the patentable subject matter.

**TECHNOLOGICAL BACKGROUND**

In 1993, Signature obtained U.S. Patent No. 5,193,056 for a data-processing system under the proprietary name Hub and Spokes.\(^\text{15}\) The system assisted mutual fund accounting and administration\(^\text{16}\) in relation to a new investment structure in which several individually managed funds, referred to as “spokes,” pool their assets together by contributing to one central vehicle with the same investment objective—the “hub.”\(^\text{17}\) Although all assets are commingled, the individual funds continue to levy their own fees and expenses.\(^\text{18}\) This arrangement provides the investors with many benefits, including achieving economies of scale and realizing the tax advantages of a partnership.\(^\text{19}\)

The Hub and Spokes investment system used algorithms to track the financial information flowing from spokes and determine the true value of each fund.\(^\text{20}\) It also allocated the appropriate amount of income, expenses,

---

\(^\text{12}\) Alice Corp. v. CLS Bank Int’l, 134 S.Ct. 2347, 2358 (2014).


\(^\text{16}\) Id.


\(^\text{19}\) *State St.*, 149 F.3d at 1370.

\(^\text{20}\) Id.
gains and losses to each spoke on a daily basis, as required by the IRS. Because these calculations were complex and time-sensitive, performing them by hand was impractical, and a computer or similar device was required. Although Hub and Spokes fund structuring has been largely abandoned in favor of newer methods, this innovation coupled mathematical formulas with technical application in a manner that significantly shaped the investment management industry in the late 1990s.

LEGAL HISTORY

Signature’s method for transforming “discrete dollar amounts [. . .] through a series of mathematical calculations into a final share price” was deemed patentable not based on the nature of the invention, but rather the output it produced. The State Street court relied on a previous case where it upheld a patent on a method for creating a waveform on the digital display system of an oscilloscope because it was “a specific machine [used] to produce a useful, concrete, and tangible result.” By adopting the language from Alappat, the court firmly established this useful-concrete-tangible test and held that even a result expressed in an abstract idea, such as numbers, could qualify a business method as patentable.

A TEXTUAL CRITIQUE OF THE NEW TEST

At its core, patent law exists to “promote the progress of science” by allowing individuals to secure certain rights over their inventions. These rights are not unconstrained: in § 101, Congress limited the subject matter of patentable claims to inventions or discoveries related to “any new and useful process, machine, manufacture, or composition of matter.” Further, § 100(b) of the Act defines a process as an “art, or method” and includes a new use of any one of the statutorily provided categories for patentable subject matter.

22 State St., 149 F.3d at 1371.
24 In re Alappat, 33 F.3d 1526, 1544 (1994).
25 State St., 149 F.3d at 1375.
26 U.S. CONST. art. 1, § 8, cl. 8.
Section 273 provides a defense specifically for business method patents, which suggests Congress intended at least some of these inventions to be covered, so long as they met the relevant statutory requirements. Thus, the methods in State Street certainly constituted patentable subject matter under § 101, and were rightfully granted patents because they were also novel, non-obvious, and contained a written description.

Although applying patentability questions to business procedures may appear straightforward, courts have struggled with interpreting this language in the context of intangible protocols that optimize corporate operations in the digital age. Although this area of the law has undergone significant revisions, beginning with State Street, the Court has consistently held that “laws of nature, natural phenomena, and abstract ideas” are categorically unpatentable. Some scholars argue that the Act leaves open whether or not less traditional business methods, such as those outside of chemical processing and manufacturing, are included under § 101. The useful-concrete-tangible test the court adopted to avoid this question fails to truly clarify this analysis.

Both business methods and technology advance rapidly and unpredictably. As a result, society has witnessed significant shifts in technology over the past few years, and the law has struggled to keep pace with these advancements. The useful-concrete-tangible test from State Street

30 35 U.S.C. § 102 (1994) (“A person shall be entitled to a patent unless – the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention…”).
31 35 U.S.C § 103 (1994). (This statute sets forth that no patents may be granted if “the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious…”).
32 35 U.S.C § 112 (1994). (“The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms…”).
33 E.g., Bilski, 561 U.S. at 601; see also Diamond v. Diehr, 450 U.S. 175, 185 (1981).
was eventually be replaced by the machine-or-transformation test in Bilski, and more recently a focus on whether an abstract idea contains an “inventive concept” in Alice Corp. But even these tests are difficult to apply given modern procedures for executing business tasks. For example, the test from Bilski created a supposed physicality requirement that excludes newer technologies relying on intangible ideas, and the “inventive concept” described in Alice is difficult to distinguish from abstractions. Instead of creating a new test every time the Court backs itself into a corner, an emphasis should be placed on referring to the statute since it was drafted broadly for a purpose.

**THE MISCONCEPTION OF THE BUSINESS METHOD EXCEPTION**

After concluding that Signature’s patented process met the threshold of the mathematical algorithm exception via the useful-concrete-tangible test, the Federal Circuit scrutinized the financial accounting software in light of the business method exception. It found that the lower court eliminated what had historically served as a bright-line rule to measuring patentable subject matter because it was, at best, created in dictum. In hindsight, overturning this rule which was thought to be long-settled proved to be more notable than the creation of the useful-concrete-tangible test and made State Street an infamous case in patent law.

As evidence that the business method exception was originally a misinterpretation, the court explained that the exemption had never been raised in court as a reason to disqualify an invention from patent protection. Rather, claims for business method patents are typically overturned for a more apparent reason associated with Title 35. Even more telling is the fact that the case responsible for giving birth to the exception never even indirectly mentions the concept. A careful analysis of Hotel Security Checking Co. v. Lorraine Co. reveals no implication of a categorical exclusion for business methods. Instead, the modified process for capturing and relaying customer

---

37 Id.
38 Alice Corp. v. CLS Bank Int’l, 134 S.Ct. 2347, 2355 (2014).
40 State St., 149 F.3d at 1375.
41 Price, supra note 23, at 143.
42 Id.
43 Id.
food orders in a manner that minimized fraud and speculation was ruled unpatentable because the nature of its invention would be obvious to anyone familiar with the food service industry. While it is true that the method described in the case is abstract and probably lacks the tangible results necessary to be a patentable business method, the Second Circuit based its ruling strictly on a failure to meet the standards for novelty and non-obvious subject matter respectively set forth in § 102 and § 103.

Most State Street critics accuse the court of exercising a level of judicial activism that ultimately thwarted innovation by allowing creators to monopolize abstract ideas and profit from them unfairly. In reality, this judicially-created exception deeming business methods inherently unpatentable was a flaw reinforced over time. Eventually, the business method exemption became accepted as a “vague and amorphous” legal concept often overlooked by courts. Under this logic, the Circuit Court’s decision to unambiguously eliminate the business method exemption was not a radical move against stare decisis, but a simple correction of the historical error. Indeed, the court resolved that “business methods have been, and should have been, subject to the same legal requirements for patentability as applied to any other process or method.”

CONCLUSION

Early courts that interpreted the Hotel Security ruling as a general exception were understandably trying to create a reliable short-cut for what is often a daunting analysis; however, the attempt backfired. In today’s environment, the line between abstract principles of nature and sophisticated business processes has blurred as technology continues to weave its way into traditional business tasks. For this reason, claims for business method patents must be examined on a case-by-case basis. State Street took a crucial step by highlighting the inadequacy of the business methods exclusion once and for all. Unfortunately, instead of narrowing the scope of patentable methods by reinforcing a reliance on statutory interpretation, the court created a new test that only yielded more confusion and opened the floodgates at the USPTO. This led courts to overcorrect the issue in more recent cases. In particular, Alice Corp. has moved us back to a world where business method patents are

44 Angwin, supra note 13.
45 Michael Risch, America’s First Patents, 64 FLA. L. REV. 1279 (2012).
relatively difficult to obtain. People will undoubtedly continue to invent, but this may be a disincentive that hampers commercial innovations requiring significant research and development investments to move society forward.\textsuperscript{47} It is misguided to claim that technological development uniformly pushes in favor of broader patentability,\textsuperscript{48} but the Supreme Court’s reversion to tighter rules surrounding business methods will undoubtedly have a drastic effect on innovation as technological practices continue to evolve.


In 2010, the Wall Street Flash Crash\(^1\) caused the United States to experience a trillion-dollar stock market crash\(^2\). Within a few minutes, the Dow Jones index lost nearly 9% of its value, which wiped off hundreds of billions of dollars from the share prices of established companies such as Proctor & Gamble and General Electric. Taking advantage of technological advances, traders and brokers used computer algorithms on the floors of stock exchanges to illegally outplace other market participants when trading stocks and securities. The Flash Crash is a concrete example that, as technology advances, stock exchanges are increasingly vulnerable to market manipulation and deceptive trading practices.

Historically, manipulation of the technology used on stock exchanges has not always been as it is today. Brokers directing orders to different parties to be executed in financial markets, also known as order flow, first became computerized in the early 1970’s with the introduction of the “designated

\(^{1}\) “American share and futures indices went into a seemingly inexplicable tailspin, falling 10% in a matter of minutes, with some blue-chip shares briefly trading at a penny, only to recover most of the lost ground before the end of the trading day.” One big, big trade, ECONOMIST (Oct. 1, 2010, 6:42 PM), http://www.economist.com/blogs/newsbook/2010/10/what_caused_flash_crash [https://perma.cc/EQT4-9J3D].

order turnaround” system (“DOT,” and later renamed “SuperDOT”) on the New York Stock Exchange. The DOT system routed orders electronically to the proper trading post and would then execute the trades manually. The “opening automated reporting system” (“OARS”) aided trading specialists in determining the market clearing opening price, which is the monetary value assigned to each stock (known as “Smart Order Routing” or “SOR”). These systems evolved into the more popular algorithms used on the exchanges today, including VWAP, Target Close Pegged, Percentage of Volume, and Implementation Shortfall.

Navinder Singh Sarao, a futures trader from the United Kingdom, was one of the players who used market manipulation tactics to induce the 2010 market crash. Sarao used one of these algorithms to engage in an illegal practice called “spoofing.” Spoofers create illusions of market demand by bidding for stocks and other securities at a rate much higher than they are actually worth and then subsequently canceling their orders before they are filled. The intense market activity around the buying and selling these stock orders attracts other traders to bid for these stocks, resulting in security-price manipulation. Spoofers benefit from the market's reaction because they can

---

10 Id.
influence the rise and fall of share prices and buy and sell stock options accordingly.\textsuperscript{11}

As a response to the 2010 market crash, United States’ lawmakers, the Department of Justice’s Criminal Fraud Section (“DOJ”), and the U.S. Commodity Futures Trading Commission (“CFTC”) began enforcing laws that prohibited illegal activity in securities markets. This comment analyzes Sarao’s prosecution in the United States and his subsequent extradition, which resulted from his illegal “spoofing” activities. Additionally, this comment analyzes the DOJ’s recent increased prosecution of actors engaging in market manipulation. Moreover, this comment will propose an alternative prosecution method in light of the outdated legislation surrounding specific types of computational trading vehicles.

\textbf{Analysis}

In 2015, five years after the Flash Crash, both the CFTC and the DOJ filed civil and criminal actions against Sarao. The DOJ indicted Sarao on twenty-two criminal counts, including spoofing, wire fraud, commodities fraud, and commodity price manipulation.\textsuperscript{12} The DOJ’s evidence supported that Sarao placed several simultaneous large-volume orders at various prices on the Chicago Mercantile Exchange (CME).\textsuperscript{13} Sarao utilized a modified automated trading program to execute these orders and cancel them before they were fully processed. By doing so, he created the false appearance that there was a substantial stock supply, which fraudulently induced other market participants to react by selling or buying stocks. This mechanism artificially lowered the price of these stocks and resulted in many brokers purchasing Sarao’s orders with inflated prices.\textsuperscript{14} By artificially adjusting several stock prices on the market, Sarao was able to induce false market perception, causing several stocks to crash and thousands of individuals to lose money on the market.

Although Sarao took a plea agreement, several implications result from this case. First, the U.S. government finally realized how outdated the legislation is for these new types of computational trading vehicles, including the computer algorithms and high-frequency trading programs used on the exchanges. Congress adopted the Dodd–Frank Wall Street Reform and

\textsuperscript{11} Id.
\textsuperscript{12} Indictment, \textit{supra} note 8.
\textsuperscript{13} Id.
\textsuperscript{14} Id.
Consumer Protection Act as a response to the market crashes caused by manipulative practices, such as those used by Sarao. However, there continues to be an increase in these types of incidents, which are likely resulting from top executive’s desire to increase their compensation (which is generally linked to his or her company's stock prices) and ensuring their company survives in an increasingly unstable economy. Fortunately, federal authorities are bringing more cases involving market manipulation. Sarao’s case will serve as a legal framework that will encourage prosecutors to bring market manipulation cases based on allegation of spoofing. Additionally, the cooperation between the United States and the United Kingdom authorities with regard to Sarao’s extradition and subsequent trial in the United States signifies a likely trend that there will be international enforcement of market manipulation practices. The United States and several other countries are now actively prosecuting spoofing and other market manipulation cases, which were previously thought to be "too vaguely defined" to be prosecuted.

CONCLUSION

Although Sarao entered into a plea agreement with the DOJ in November 2016, the U.S. Congress and the DOJ have focused on ways to prevent and outlaw market manipulation and to expand United States’ jurisdiction abroad. In the meantime, traders and brokers must be aware that

the law is catching up to technology and that the DOJ is actively pursuing those that previously might have been able to use technology to avoid lawsuits.

As government actors continue to examine ways to prevent market manipulation a proper understanding of the technology used by financial markets is essential in balancing free trade and protection of consumers’ rights.
INTRODUCTION

In an increasingly globalized world, the emergence of decentralized systems of virtual currency has created a way for individuals to quickly and easily transfer value directly to one another without the need for a trusted third-party intermediary. While this is useful to many individuals, it creates challenges for society. Cryptocurrencies, such as Bitcoin, are often anonymous, and governments lack the ability to regulate or even track transfers. This can facilitate crime, as in the case of Silk Road, an online...
marketplace for the illegal sale of drugs and weapons.² Some users have also reported theft of their virtual currencies, which is difficult to even prove as a result of their anonymous nature,³ and there is the further potential of these currencies being used to facilitate tax evasion. Ultimately, it may be possible that the advantages of digital currencies do not have to coexist with the current disadvantages. Identifying why legal users seek anonymity in cryptocurrencies and what that anonymity provides could lead to a better application of the technology to harness its potential without increasing crime. This literature review will discuss Prof. Omri Marian’s publications regarding cryptocurrencies and tax evasion, privacy in general, as well as anonymity in cryptocurrencies. It will conclude by suggesting alterations to the framework proposed by Marian that could achieve both privacy, and control over tax collection.

**MARIAN’S RESEARCH AND CONCLUSIONS**

Cryptocurrencies have proven challenging for governments because anonymity and lack of trusted intermediaries, such as banks, allow the currencies to be used as tax havens by their users.⁴ Marian considered these challenges in his 2013 article, *Are Cryptocurrencies Super Tax Havens?*. He outlines two parallel developments that could potentially lead to cryptocurrencies becoming untraceable tax havens, namely increasing use of cryptocurrencies, and the reliance of tax enforcement on financial intermediaries.⁵

The first development is the increasing popularity and acceptance of cryptocurrencies, coupled with their anonymous and untaxed nature. Cryptocurrencies are now accepted in a range of businesses, and the most successful one, Bitcoin, is accepted even by major retailers such as Microsoft, Dell, and Subway.⁶ Bitcoin’s availability as a medium of exchange for goods

---

⁵ Id.
and services eliminates the necessity for Bitcoins to be converted back to traditional currency, making it increasingly integrated in the real economy.\textsuperscript{7} The second development is the targeting by the U.S. government of financial intermediaries in order to combat current tax evasion. The Foreign Account Tax Compliance Act (FATCA) is aimed at punishing foreign banks for failing to disclose the identities of account holders, when those account holders are U.S. taxpayers.\textsuperscript{8} Consequently, there have been a number of arrangements between the United States and other nations to circumvent foreign bank secrecy laws, and thereby expose tax evasion by U.S. citizens.\textsuperscript{9} Taken in combination, the anonymity and lack of intermediaries in the transactions make it impossible to continue the intermediary-based tax enforcement mechanisms, and will lead to cryptocurrencies becoming tax havens for U.S. taxpayers.\textsuperscript{10}

In 2014, Marian revised his paper based on newly available research, in the article \textit{A Conceptual Framework for the Regulation of Cryptocurrencies}.\textsuperscript{11} In this work, he proposes a regulatory framework that would maintain the current levels of privacy and cost to criminal action despite the development of cryptocurrencies.\textsuperscript{12} Marian’s argument updates the premise of both developments outlined in his previous paper. It concedes that Bitcoin is not actually anonymous, and that its pseudo-anonymous nature leads to the possibility of tracing money transfers and potentially identifying users. Similarly, it recognizes that intermediaries are a result of market forces and have naturally developed in various forms in the Bitcoin market as well. He also identifies major retailers as a good intermediary to leverage in combating illicit activity in this new system.\textsuperscript{13}

Marian recommends an elective tax on anonymity during a purchase.\textsuperscript{14} In his framework, a buyer using a cryptocurrency account could either pay an anonymity tax when making a purchase or disclose his or her identity, at which point the tax would not be levied. He proposes for this cryptocurrency transaction tax to be more likely to result in an over-collection of taxes after

\footnotesize
\begin{itemize}
  \item \textsuperscript{7} Marian, \textit{supra} note 4, at 39.
  \item \textsuperscript{8} \textit{Id.} at 41.
  \item \textsuperscript{9} \textit{Id.} at 41.
  \item \textsuperscript{10} \textit{Id.} at 46.
  \item \textsuperscript{12} \textit{Id.}
  \item \textsuperscript{13} \textit{Id.} at 66.
  \item \textsuperscript{14} \textit{Id.} at 64.
\end{itemize}
the assumption that no income tax has been paid on the money used. This would incentivize the user to identify themselves, for example through a private identification number, as it already exists in credit or debit cards. Finally, Marian addresses various possible criticisms of his regulatory system, including the assumption that it would break down if a completely anonymous cryptocurrency was created. He concludes this statement by suggesting that such a currency would be unlikely to succeed, considering there is a necessity for trust in the financial market.

In the first part, this literature review will consider the utility of privacy and anonymity for legal users of a currency, and will give an outline of the current judicial view on the right to privacy in the context. The second part will further analyze the anonymous nature of cryptocurrencies and argue that a completely anonymous system may not only be possible, but could be successful in the market. Finally, the third part will examine the implications such an anonymous currency would have on Marian’s proposed cryptocurrency transaction tax, both in the context of tax evasion and criminal activity in general.

PRIVACY AND ANONYMITY IN SOCIETY

In his 2014 paper, Marian attempted to create a framework of regulation that would allow for privacy in banking to stay approximately at the level it is now. He argued that, while privacy hindered tax collection, privacy has its own societal advantages, and maintaining the currently level of financial privacy may be desirable. In order to better contextualize Marian’s argument, the following section will outline a number of definitions of privacy, how privacy may serve society, and what types of privacy other than anonymity could serve the user base of cryptocurrencies.

A right to privacy in American law was first mentioned in a Harvard Law Review article by Warren and future Justice Brandeis, who defined it as a “right to be left alone.” Papers in sociology, psychology, and philosophy,

---

15 Id. at 65.
16 Marian, supra note 11, at 65.
17 Id. at 62.
18 Id. at 67.
19 Id. at 56.
However, have progressed beyond that definition.\textsuperscript{21} While the advantage of embarrassing facts about an individual staying private is likely the most obvious, the use of privacy also extends to everyday life. In a 1975 article, the philosopher James Rachels argues that the multifaceted nature of humans and their interactions makes some level of privacy necessary.\textsuperscript{22} While someone may employ one type of behavior towards a child, the same person will show different behavior towards a co-worker, spouse, or political figure. Thus, it is important for that person to be able to select the way they are perceived by each audience, an ability which is furthered by autonomy over one’s information. Privacy can therefore also be understood as a person’s ability to control the information they provide to each group of people, or selective self-presentation.\textsuperscript{23}

This concept can also be expanded to society as a whole. With various groups representing “one-tracked and monopolistic” viewpoints, individuals require the use of discretion and privacy to navigate the intricate web of social interaction and exist on a spectrum in-between.\textsuperscript{24} In consequence, each person only knows that which is required of them to know within any given social context, be it private, public, or business-oriented. This allows for individuals to both represent themselves as they wish to in each interaction, and to minimize the difficulty of remembering information irrelevant to the context.\textsuperscript{25} Verschraegen argues that such compartmentalization of information is also useful for government, as “prohibition of political interference in legally recognized private spheres relieves the political system from decision making on a wide range of issues.”\textsuperscript{26} In essence then, privacy serves society by allowing information to be compartmentalized to its relevant audiences, relieving others of responsibility, as well as allowing individuals to exist on a continuum between extreme attitudes.

Looking at currency in particular, it is clear that most financial transactions will transcend groups, identities, and behavior. The same person who may be donating to a Democratic campaign could be donating to pro-life organizations, using the same currency to do both. While there may not be a

\begin{enumerate}
\item Baghaj, \textit{supra} note 21, at 956.
\item Id. at 954.
\item Id.
\end{enumerate}
problem with that, it should be the choice of the individual whether to disclose either one of those actions to the other group, and a lack of privacy in financial transactions threatens the ability to do so. This issue also touches on the subject of equality. Will one of the groups behave differently towards the individual if they know about the other donation? Does the individual have a right to be treated equal to everyone else in the group regardless of tangentially related activities?

However, as is often noted in similar discussions, privacy rights can also shield criminality. If perpetrators will be treated equally to everyone else in other contexts, illegal actions will have less negative impact on their lives, decreasing the potential cost of such conduct. As mentioned by Marian, this will increase the utility of criminal action, leading to an increase of such behavior by rational actors.

In the context of privacy as compartmentalized information, it may not be necessary to have total anonymity, however. In 1967, Westin proposed four states of privacy: Solitude, anonymity, reserve, and intimacy. Solitude is defined as a removal from other people and not applicable here. Anonymity refers to the state of interacting with others without disclosure of one’s identity, and is what is so far the goal of many cryptocurrency developments. Reserve describes a person’s control over the disclosure of information. Finally, intimacy is the state of disclosing information only within an in-group environment. The final two categories are most applicable to the description of privacy above, and were also analyzed in the context of online interaction before: In psychological literature, Taddiken investigated privacy in the context of social interaction, and came to the conclusion that forms of privacy other than anonymity can serve to achieve gratification for social media users. Transferred to financial interactions, it may therefore be possible to satisfy the need for privacy needed without resorting to anonymity. Better separation of who has access to what set of information about a user’s financial transactions could even lead to increased privacy as well as increased cost of criminal action.

28 Marian, supra note 11, at 60.
29 See, ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967).
31 Id.
While sociological and psychological papers show the need of both society and individuals for privacy, and suggest that it was already around before the modern systems of government, the concept of a legal right to privacy is relatively young. It was only in 1890 that the right of privacy was suggested in the Warren/Brandeis article in Harvard Law Journal. Consequently, there are not as many judicial decisions about the right per se as one would expect. However, it is possible to assess the judicial opinion on privacy from the opinion’s balancing between the interests of individuals and the state.

In the *Bowers v. Hardwick* and *Lawrence v. Texas* line of cases, the Supreme Court weighed whether the Fourteenth Amendment protection of liberty and privacy extended to homosexual sodomy in the petitioners’ home. Overruling Bowers in Lawrence, the Court ultimately concluded that it did, stating that petitioners were “entitled to respect for their private lives.” Similarly, a lot of Fourth Amendment jurisprudence weighs an individual’s privacy against the government interest to pursue crime. In this regard, the Supreme Court decided in *Silverman v. United States* that even intruding into the home by a fraction of an inch would be too much, and then extended this protection in *Katz v. United States* to places in which an individual had manifested a subjective expectation of privacy that was seen as reasonable by society. In *Tehan v. United States*, the Court also stated that the Fifth Amendment reflected the right of an individual to have “a private enclave,” and in *NAACP v. State of Alabama* stated that the First Amendment gave an individual “freedom to associate and privacy in one’s association.” While many of these cases show that the Supreme Court strongly recognizes the right of individual citizens to live undisturbed from government interference, Fourth Amendment jurisprudence of the Court also shows a different approach when it comes to information already disclosed to third parties. In

33 Baghai, *supra* note 21, at 959.
36 Id. at 578.
cases such as *United States v. Miller*, the Court has repeatedly held that the Fourth amendment does not protect information disclosed with third parties, even when the information has been disclosed on the assumption that it will be limited in use.\(^{41}\)

While these decisions of jurisprudence extend clear protection to certain aspects of an individual’s privacy, they are largely in line with the “right to be left alone” explained by Warren and Brandeis. Looking at the concept of privacy as a separation of information for relevant audiences as suggested by Baghai, the current state of judicial decisions seem to be a strong violation of the individual’s interest in controlling the information about themselves. If an individual discloses information to a third party, such as a bank, an insurance provider, or a telecommunication provider, such information would not be considered protected. This is the case even though the individual may have very deliberately exercised a level of control over which information they have shared with which group. It therefore seems that, while the judicial system strongly supports the right to privacy, the jurisprudence has not yet moved beyond the context of Warren. In light of increasing collections of information vital to a person’s identity online, such a move may however be necessary, especially if the judicial system wants to remain true to the statement made in NAACP. Notably, Justice Sotomayor’s concurrence in *United States v. Jones* pointed out that “the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age . . .”\(^{42}\)

In summary, it appears that the need for privacy of financial interactions and the government’s need to control criminal activity may not be mutually exclusive. Since anonymity in financial interactions is not necessarily a requirement for privacy of an individual’s actions, the move towards a separation of the two will require a recognition of the separation of various types of information by the government. While the legal system does support the right of privacy for an individual, the current perspective on privacy as a right to be left alone will not be sufficiently subtle to support such a separation.

ANONYMITY IN CRYPTOCURRENCIES

While technology seems to present further complications for privacy, making the balancing act between various interests of society and individuals increasingly difficult, technology may also provide the solution. Assuming that privacy is served through guaranteeing that only a permitted group has access to any one area of information at a time, it may be possible to technologically grant the government the ability to access an individual’s records to detect tax evasion or criminal activity, while decreasing access to other types of information and therefore increasing the level of privacy the individual enjoys. In that way, the technology itself could move towards a compromise with the current legal system, allowing for faster adaption of the judicial decisions to the currencies. The following section will outline the current state of cryptocurrency anonymization, as well as developments towards this direction.

How Do Cryptocurrencies Work? The Example of Bitcoin.

Any electronic currency has to implement mechanisms to establish ownership, protection against double spending, anonymity, privacy, and issuance of new currency. After a number of less successful electronic currencies, Bitcoin’s success was based on how it addresses these challenges, which has been copied in a number of later attempts. Since there is no central authority to issue currency, Bitcoin currency can be generated by anyone through “mining.” With Bitcoin, miners use special software to solve complex math problems and are issued a certain number of bitcoins in exchange. Each user can make a public statement to the Bitcoin network, stating the amount of Bitcoin transferred, as well as accounts from which to transfer and accounts to transfer to. The Bitcoin network records any such transactions of existing bitcoins between users, which are added to a public ledger, called the blockchain. The process of mining does not only create new currency, but is the process of creating the next entries in this ledger, which is essential for the operation of the system. Bitcoin are kept in a “wallet,” specialized software that stores the public and private key pairs associated with previous and

---

43 Reid & Harrigan, supra note 3, at 200.
potential transactions. Every transfer between two accounts has its own public key to be identified, as well as the previous owner’s private key to authorize the transaction. While it is possible to reuse a public key for a transaction, it is generally considered good practice to create a new pair of keys for each transaction. Since no identifying information is needed in the creation of a wallet, there is a certain level of initial anonymity associated with Bitcoin. The blockchain is particularly notable, as the decentralized nature of the system requires this public ledger as a safeguard against double spending. However, the availability of the entire transfer history also means that there are many data points from which it is possible to reverse engineer information on users or user behavior.

**Bitcoin Anonymity**

Even though Bitcoin has been treated as a currency in which users enjoy anonymity during the first years of its operation, anonymity in cryptocurrencies is not as easily achieved as one might assume. In the past 4 years, various academic papers have looked into the anonymity aspects of cryptocurrencies in general, and Bitcoin in particular.

Bitcoin can consequently be said to not reach to the level of anonymous transactions. Various papers have used the blockchain ledger in order to passively analyze the transactions and user bases of Bitcoin, identifying up to 40% of users through various methods. In particular, grouping many accounts and transactions together by using the underlying transfer rules and accepted procedures in Bitcoin, makes it possible map the system and trace money. For example, if one public key is associated with a real ID, such as a tweet of a public key to elicit donations, it is possible to also identify other public keys (and therefore bitcoins) that are likely owned by the same user, but have not been publicly mentioned. Adding to this, the analysis

---

45 Public keys can be understood as the publicly identifiable number of each transfer, a private key as the “password” to confirm ownership of the transaction. See, e.g. Reid & Harrigan, supra note 3, at 203.

46 Double spending concerns the potential problem of an existing bitcoin being sent to two different recipients without the system being able to realise this in time. See, e.g. Jordi Herrera-Joancomartí, Research and Challenges on Bitcoin Anonymity, in 8872 DATA PRIVACY MANAGEMENT, AUTONOMOUS SPONTANEOUS SECURITY, AND SECURITY ASSURANCE, LECTURE NOTES IN COMPUTER SCIENCE 3, 5 (Joaquin Garcia-Alfaro et al. eds., 2015).

47 Id. at 9.
of TCP/IP makes the system even more vulnerable to deanonymization. Koshy et al. were able to create a mapping of the network independent from blockchain analysis. This was furthered by Kaminsky, who used combination of the blockchain analysis with TCP/IP in order to map user accounts to IP addresses and therefore locations.

All of these possible attacks are facilitated further by active participation. Meiklejohn et al. used their bitcoins, transferring them to known users in order to trace the flow of their money through the system and deduce additional information. This is very effective on the level of individual attackers, but would be even more so if it were conducted by a government that is capable of legally compelling the participation and disclosure by many legitimate actors. In particular, compelling the naturally formed intermediaries would add to the effectiveness of such an attack. While services that exchange Bitcoin with real currencies used to be the dominant intermediary, there has also been a development of online wallet providers, coin swapping services, and others which have gained prominence. The online wallet providers, for example, make Bitcoin wallets more accessible to the general public by merely requiring a setup similar to an email account. Further, wallets do not require their own software and may be access from a web browser on any device. This function resembles a bank at the front end, holding the account information of various customers, but is not comparable to a traditional bank in the back-end service, as it is not holding the money or facilitating the transfer. The convenience of online wallets comes at the expense of decreased security, as service providers generally keep record of at least, but sometimes more than, one IP address associated with an account.

Overall, the anonymity in Bitcoin does not appear to be particularly strong. With an increasing number of confirmed data points, it becomes much easier to determine the identity and behavior of the others. Because the blockchain contains all transfer data, users may be easily identified, and even

---

50 Reid & Harrigan, supra note 3, at 202.
51 See generally Meiklejohn et al., supra note 27, at 89.
52 Marian, supra note 11, at 53-54.
users that actively protect their identity may be vulnerable. It is important to note, however, that bitcoin was not created to enable complete anonymity,\(^53\)\(^54\) and that maintaining the core script’s integrity takes precedent with the community around the code. Thus, while multiple processes have been proposed for increasing the anonymity of Bitcoin, none of them have been implemented or are likely to be implemented. Consequently, there are a range of alternative cryptocurrencies that are not yet as common as bitcoin, but which are built on lessons learnt from its vulnerability to deanonymization.

Developments in Anonymity

Cryptocurrencies currently face the tension between keeping a user's information confidential and barring double spending. A decentralized system must have a publicly available ledger in order to avoid double spending, such as Bitcoin’s block chain. If accessed, however, this transfer information may be exploited by others and diminish anonymity\(^55\).

While most current systems disclose all individual transactions in the public ledger, it is also possible to create a system that uses a zero-knowledge proof in order to validate its interactions. Such a system would generate mathematical proof that all transactions have been valid, without actually disclosing the individual transactions. This system requires a trusted setup and would be open to manipulation by the authors.\(^56\) One of the cryptocurrencies currently pursuing this is Zerocash, a successor to Zerocoin: their development is moving into a direction of distributing the trusted setup to multiple nodes which, assuming that at least one of the nodes destroys the relevant files, make it theoretically secure.\(^57\) The computation of the proof would therefore be so far distributed that a manipulation would not only be statistically improbable, but practically impossible.

Theoretical vs. Practical Implementation

\(^{53}\) Nakamoto, supra note 44.  
\(^{54}\) Reid & Harrigan, supra note 3, at 198.  
\(^{55}\) Id.  
\(^{56}\) Eli Ben-Sasson et al., SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge, 8043 ADVANCES IN CRYPTOGRAPHY – CRYPTO 2013, 90 (2013).  
\(^{57}\) Ian Miers et al., Zerocoin: Anonymous Distributed E-Cash from Bitcoin, IEEE SYMPOSIUM ON SEC. & PRIVACY (2013).
A further problem of anonymity is that, while it may be possible to get a perfectly anonymous system in theory, the implementation will always suffer from use-related insecurity. Considering many people have become comfortable with sharing the details of their lives social media, much of the previously mentioned academic research was able to determine identities based on the user’s own posts on twitter and similar media. While a system can attempt to mitigate such disclosures, widespread lack of awareness over what one should or shouldn’t do in order to keep one’s privacy will necessarily create many points of potential attack.

In the same context, a lot of the currency will necessarily have overlaps with real economies, with many users being neither tech experts, nor particularly concerned with their privacy. If A and B have used the transaction in order to buy clothing online, which is shipped to their home addresses and has their names and prices associated with it, C’s transaction will be far easier to determine. While theoretical anonymity is therefore difficult to achieve, anonymity of a widespread cryptocurrency in practice will be yet another step from it.

Nevertheless, there are many developments towards greater anonymity, many of which seem at least theoretically feasible. While the implementation still seems a number of years, or even decades away, computing capacity is steadily increasing and the cryptologists are learning from many issues with Bitcoin.

**POTENTIAL ADJUSTMENTS TO MARIAN’S REGULATORY FRAMEWORK**

**Challenges to the System**

Despite the previously mentioned difficulties, it is within the realm of possibility that a cryptocurrency will be anonymous, or at least difficult enough to crack that it loses feasibility on a large-scale level. If this is on the basis of a zero-knowledge scheme, Marian’s concern that there would not be enough trust in the system for it to work would be eliminated, as users would have mathematical proof of the currency’s trustworthiness without the need to be able to check the history of transactions. That there can be trust in a

58 See Marian, supra note 11, at 67.; see also, Monika Taddicken & Cornelia Jers, *The Uses of Privacy Online: Trading a Loss of Privacy for Social Media Gratification?*, in PRIVACY ONLINE 143, 143-144 (Sabine Trepte & Leonard Reinecke eds., 2011).


60 Id.
system that one does not fully understand is also shown by the large influx of users into the Bitcoin system while it was still widely considered anonymous. While most users were likely not tech experts who would have been able to confirm the trustworthiness themselves, they trusted the perception of its trustworthiness. Consequently, the most extreme scenario would be a trusted currency that would effectively become a black box for outsiders. Any money that is put in disappears to the person not holding the key, and it is impossible to determine the path of the money when it leaves the system.

The effect this would have on Marian’s proposal is significant: a given user A could earn money through illicit activity and then pay the anonymity tax without fear of any trace to his illicit activity. A bolder user B may earn money through illicit activity, and then claim to have gotten to the level of wealth through fluctuations in the market, effectively avoiding the anonymity tax and simply declaring the money as gains from capital assets. Even at a less extreme level, an otherwise law abiding user C could shift his income from capital gains to ordinary income or reverse without fear of repercussions.

Proposed Adjustments
Input Control Scenario

A potential way of combating this would be to accept the black box scenario, but require all input into the cryptocurrency be declared within a set time frame. This would allow for any tax authority to match declared input to declared output, including time stamps, and reduce the possibility for tax evasion. User C from the previous example would have a declared input, calculated gain or loss, and declared output which can be matched to them. Any discrepancy in output can be put down to undeclared input (if it is higher than expected), saving (if lower), or partial use of the anonymity tax (if lower). The indeterminate state of savings or use of the anonymity tax could be declared by the user at the end of the year, with the savings carrying over. This system would, however, suffer from the potential of a user spending their money through the anonymity tax when speculating for a fall of the currency value, and consequently registering a loss on capital assets that is far greater than what they have actually incurred.

Input and Output Control Scenario

---

61 Anthony Vance, et al., Using trust and anonymity to expand the use of anonymizing systems that improve security across organizations, SEC. J. 1, 11 (2015).
A system that would eliminate privacy but stop users A and B as well, would be to eliminate the elective tax, leading to a requirement to declare input, as well as a requirement to identify oneself when purchasing with cryptocurrency. Since the current way of purchasing things electronically and from a distance is to use a credit card, this is unlikely to diminish privacy over the current state, as the users still have the alternative of paying cash in person. This framework would also be more easily integrated into the existing scheme of income taxation, while the previous example would be a mix of income and consumption tax which would be more difficult to implement.

**Crypto-Control Scenario**

Finally, it may be possible to further adjust this system as a result of its digital nature, in order to increase the level of anonymity while decreasing the potential for tax evasion and money laundering: Following a users’ electronic declaration of input into the black box, the government could issue its own cryptographic token, stating the declared value and timestamp, as well as a cryptographic hash\(^2\) of some means of identifying the user's money. The existence of such a token and related adjustment software at the retailer end would allow for someone who opted into this system to pay without disclosing their identity, while giving the retailer confirmation that the money used in the transaction was legitimately declared as income. The software at the retailer end would calculate the amount to be deducted based on a timestamp, and return the token with its diminished value. Once the value of the token runs out, any additional funds that are left over will have to be paid while disclosing one’s identity again, as the discrepancy will be due to illicit funds, or capital gains.

Depending on the implementation of such a system parallel to the currency, various degrees of privacy and anonymity could be achieved. For example, it would be possible to disclose more information to the retailers, eliminating privacy at that end, but making it impossible for the government to trace all purchases. Conversely, it may be possible to disclose more information on the government’s end, making it possible to trace purchases in

\(^2\) In this context, hashing is referring to cryptographic hashing, enabling the shop to verify that the token used is associated with the money being spent, without making it necessary for the government to be informed of the spending, or for the shop to be informed of the amount taxed.
general, but allowing for the user to remain unknown to the retailers. Finally, it may even be possible to create a system where it would be possible for the government to access the overall amounts earned and spent by an individual within the currency, without the ability to tell where it was spent. While none of these scenarios would satisfy the state of “being left alone,” they would all allow for the user or at least the collective of users, to control which information is accessible by which group of people.

CONCLUSION

The development of cryptocurrencies and their successors will undoubtedly continue into the far future, and regulation of it in order to discourage its use as a tool for crime while retaining its advantages will be an ongoing challenge. This literature review outlined the various types of privacy that may be achieved by the technologies used in cryptocurrencies, and determined that it might be possible to satisfy the need for privacy without reaching anonymity. It further considered the current state and developments of anonymity in cryptocurrencies, and concluded that complete anonymity was theoretically possible but far from practical implementation. Looking into Marian’s proposed framework for regulation of cryptocurrencies, it was considered what problems the emergence of a blackbox-type cryptocurrency would create for it, and a number of solutions were proposed. Ultimately, the literature review suggested that the technology may be adjusted in tandem with government regulation to serve both society’s need for privacy as well as its need to deter criminal activity.

Considering the ongoing development of cryptocurrencies and cryptography in general, as well as the theoretical possibility of unbreakable encryption, it is important to consider the implications of such an occurrence for legislature and regulations. To balance the line between regulation and maintaining privacy, it may also be possible to use the same technologies that are creating the problems in order to aid their regulation.
TECHNOLOGY EXPLAINERS

SMART CONTRACTS: A SMART WAY TO AUTOMATE PERFORMANCE

Jenny Cieplak* and Simon Leefatt*

CITE AS: 1 GEO. L. TECH. REV. 417 (2017)
https://perma.cc/N4KP-A3VV

INTRODUCTION ................................................................. 417
WHAT IS A SMART CONTRACT? ............................................ 418
WHAT IS DISTRIBUTED LEDGER TECHNOLOGY? ................. 420
SMART CONTRACTS ON A DISTRIBUTED LEDGER – AUTOMATING PERFORMANCE.. 422
CONCERNS WITH THE SMART CONTRACT MODEL .................. 424
ENFORCEMENT OUTSIDE THE DISTRIBUTED LEDGER CONTEXT .... 426
CONCLUSION ........................................................................ 427

INTRODUCTION

The freedom to contract is one of the oldest and most basic tenets of the American legal system. Subject to limited judicial and statutory exceptions, parties have been and are generally afforded carte blanche in determining the terms of a binding agreement and how those terms are memorialized. The recent emergence of “smart contracts,” that are stored and executed using distributed ledger technology, is another step forward in the process of computerized contracts, following electronic delivery of signatures through PDF and fax to today’s digital signature services. What makes smart contracts unique, however, is that they not only involve the automation of contract formation, but also the execution of the contract’s terms.

* Jenny Cieplak is a counsel in the Corporate Group at Crowell & Moring LLP and is the head of the firm’s blockchain and distributed ledger technologies initiative. © 2017, Jenny Cieplak and Simon Leefatt.

* Simon Leefatt is an associate in the Corporate Group at Crowell & Moring LLP and is a member of the firm’s blockchain and distributed ledger technologies initiative. © 2017, Jenny Cieplak and Simon Leefatt.
WHAT IS A SMART CONTRACT?

There exists no universally accepted definition of a smart contract. Generally, smart contracts are computer protocols that implement the terms of a negotiated contract in a self-executing manner. These contracts may either be written entirely in standalone code, coupled with traditional written agreements reflecting the same negotiated terms codified in the code, or partially governed by both code and a traditional written agreement that is incorporated by reference in the code itself. Smart contracts have broad applicability and, as a result, they may be used to govern or facilitate many types of financial transactions.

Nick Szabo, who is considered by many to have been the originator of the smart contracts concept, described the concept of incorporating contract terms into computer hardware and software by describing a car lien.¹ Without smart contracts, if the owner fails to make payments on the loan secured by the car, the lender must go through the process of repossessing the car. By using a self-executing smart contract to enable a hardware and software function in the car, a lender can make it impossible for the owner to start the car if the owner fails to make payments. Once the loan has been completely paid off, the smart contract can automatically add a new function that disables the previous function.²

Another example, which does not implicate problematic considerations of wealth inequities, is derivative contracts. Consider an interest rate swap, where Party A agrees to pay to Party B each month an amount equal to 5% of notional amount X, and party B agrees to pay to Party A each month an amount equal to some floating rate of interest of notional amount X. In real life, Party A and Party B determine whose payment is larger, and exchange a net amount. Basically, Party A is betting that the floating rate of interest will, on average, be more than 5%, so that he always receives the monthly payment, and Party B is betting the opposite.


² If the smart contract is on a blockchain-inspired distributed ledger, the security interest transaction cannot be deleted (as transactions are permanently encoded), but it can be reversed. Kadhim Shubber, *Banks find blockchain hard to put into practice*, FIN. TIMES (Sept. 12, 2016), https://www.ft.com/content/0288caea-7382-11e6-bf48-b372c8a1043a [https://perma.cc/5M2X-6XE9].
Interest rate swaps are currently documented through transaction confirmations, which incorporate by reference master agreements, schedules, and credit support annexes. The master agreement, schedule and credit support annex, along with other optional documents, are general documents that govern the trading relationship of the parties, and apply to all swap transactions. These documents are typically executed manually, with signatures often delivered by fax or PDF, or by using DocuSign or another electronic signature service. A transaction confirmation is created for each swap which includes the terms of the particular swap, and may be executed “manually, electronically, or by some other legally equivalent means.” The terms and conditions of a particular swap thus appear on multiple transaction documents that are separately viewable in static form, i.e. via local copies either in print form or saved on a hard drive document management system. The parties must then access rate providers to determine periodic payments and send these payments from their accounts. Each of these processes may be automated to some degree, but they are also open to error, both human and computer-based. Data may be entered mistakenly, and flaws in code can also cause errors in information to appear.

In addition to simply documenting the business terms of the swap, parties to swap transactions must undertake a large number of legal and compliance steps. These steps include checking counterparty eligibility, documenting the trade, determining whether the trade must be submitted to a clearinghouse, and regulatory reporting, as well as actually making payments. The process is extremely complex and typically involves multiple systems.

---

5 Interest rates are typically available to the public through widely available sources, but if payments are being made automatically, the parties are likely to want an independent party to confirm the applicable rate in order to prevent one party from gaming the system. Typical interest rate providers are Thomson Reuters and Bloomberg. Accounting and financial systems such as SAP allow their customers to import rate information directly from these rate providers. For a very technical description of how rates are imported into a company’s SAP systems, see *Datafeed*, SAP SERVS. MARKETPLACE, http://help-legacy.sap.com/saphelp_sfin100/helpdata/en/4f/3adadc862e2e4fe10000000a42189e/frameset.html (last visited Apr. 3, 2017) [https://perma.cc/59CX-9P3H].
6 Parties with significant swap business often use technology such as SAP to enter swap information in their accounting systems, which allows for some automation of payments.
across multiple parties. These systems may or may not be connected, and data may not properly transfer. Human errors such as typing mistakes (known as “fat finger” errors) are common as well. A misplaced decimal point in one party’s system could cause mistaken payments and serious disputes. Parties can even have disputes about whether a transaction exists or not.

Instead, a smart contract could be used to encode the terms of the swap, import information from a rates provider, and automate payments from the parties’ accounts. Because each of these processes is based on a smart contract in a shared ledger rather than on multiple systems that may or may not interact properly, there are fewer opportunities for the parties to have conflicting information. The smart contract on the ledger can incorporate the terms of the master agreement, schedule, credit support annex and other relevant documents just as swap transaction confirmations do today. Some solutions even offer the possibility of including an encoded copy of a pdf of a paper contract directly on the ledger.

Of course, for either of the above use cases to function properly, there needs to be a system wherein the parties to the contract are connected. In the car lien example, the computerized contract that is stored in the car’s onboard computer needs to have a way of confirming that payments on the loan have been properly paid. In the interest rate swap example, the computerized contract which is stored on a party’s recordkeeping system needs to have several different types of connectivity — it must communicate with each party’s bank account to enable payments from one party to another, and it must receive information from an interest rate provider to determine the amount of the required payment. Many industries are looking to distributed ledger technology (DLT) to make this communication possible using only one system, rather than multiple different connection systems.

**WHAT IS DISTRIBUTED LEDGER TECHNOLOGY?**

A distributed ledger is essentially a database for tracking assets and information that can be shared among multiple participants. For example,

---


imagine a ledger with a record of all the transactions in shares of a company’s stock, beginning with the initial issuance of the stock to the initial purchasers, and including all subsequent transfers.\(^9\)

The interesting thing about distributed ledger technology is that the ledger is replicated across multiple participants in a network.\(^10\) The ledger can be replicated in its entirety among all network participants, so that each participant can see all changes to the ledger, or segments can be replicated so that participants only see portions of the ledger that are relevant to them.\(^11\)

In each case, the ledger is not just copied from one network participant to another – each copy is considered the “original” copy.\(^12\) Network rules provide that when an asset changes hands or a transaction is created or modified, that resulting change in the ledger is broadcast to all copies of the ledger or, in a ledger system where not all participants have access to the full ledger, the transaction is broadcast only to the relevant parties.\(^13\)

Network participants access their assets on the ledger through cryptographic keys.\(^14\) Only the party or parties with the correct key or combination of keys can transfer or otherwise modify an asset or transaction.\(^15\)


\(^11\) Id.


\(^13\) Id.


SMART CONTRACTS ON A DISTRIBUTED LEDGER – AUTOMATING PERFORMANCE

Distributed ledgers can be used to record information such as the interest rate swap contract described above. The portion of the contract that automates performance should be deterministic (i.e., it should provide for all possible outcomes based on relevant facts). However, to automate performance of the contract, the distributed ledger must also have access to the means of performance and any metric by which performance must be measured.\textsuperscript{16} In the interest rate swap example, the distributed ledger must have access to some asset of the parties’ in order to fulfill the parties’ payment obligations, and it must have access to a provider of interest rate information.\textsuperscript{17}

Some distributed ledgers, such as the blockchain for the cryptocurrency Ether, provide for the automated performance of smart contracts by utilizing a token that is native to the distributed ledger itself.\textsuperscript{18} Users create smart contracts by uploading them to the blockchain and the contract is then propagated through the system as described above. On the Ethereum blockchain, a smart contract consists of program code, a storage file, and an account balance. The smart contract can receive money into its account balance and send money from its account balance. In order to invoke the smart contract process, the parties to the contract “contribute” a certain amount of Ether to the contract. This contributed Ether becomes subject to the smart contract and is used to fulfill the parties’ payment obligations. The program code runs automatically once the parties contribute their Ether, and pays Ether to the party that is supposed to receive it in accordance with the terms of the contract.

However, contributing all of the currency necessary to make all payments under a smart contract is likely impracticable in many situations.


\textsuperscript{17} In the swap example, recall that Party A is paying an amount equal to 5% of some notional amount each month, and Party B is paying an amount equal to some floating interest rate, such as the US prime rate, multiplied by that notional amount. Thus, in order to determine Party B’s payment, the parties need to know what the prime rate is.

Banks that are party to interest rate swaps do not want currency representing the entire amount potentially payable over the course of the swap to be locked in an account. Solutions such as R3’s Corda solve for this issue by creating “state objects,” and in particular “cash states.” A cash state represents an amount of currency that one ledger participant, typically a bank, owes to another ledger participant. A cash state is like a bank account maintained outside the distributed ledger context, in that it does not represent physical fiat currency held by the bank but instead represents an amount owed by the bank to the account holder. The smart contract can access this “cash state” as if it were a bank account, and require the bank to transfer a portion of the “cash state” to the payee.\textsuperscript{19}

In addition to having access to the means of performance, on occasion smart contracts may need access to outside information to determine what is required to perform the contract. If smart contracts, like other computer code, can be described as a series of “if-then” statements, to activate the process, one must know whether the condition has occurred.\textsuperscript{20} For example, an interest rate swap transaction would consist of the following “if-then” statements:

- If fixed rate exceeds floating rate on first day of any month N, fixed rate payor pays to floating rate payor an amount equal to \([\text{fixed rate} – \text{floating rate}] \times \text{notional amount on date that is 15 days after the end of month N}\)
- If floating rate exceeds fixed rate on first day of any month N, floating rate payor pays to fixed rate payor an amount equal to \([\text{floating rate} – \text{fixed rate}] \times \text{notional amount on date that is 15 days after the end of month N}\)

Here, you would need someone to determine what the floating rate of interest is on the first day of each month. The smart contract can then calculate whether the floating rate is higher or lower than the fixed rate, which will be encoded in the smart contract. The concept of “oracles” is useful here. An oracle is a third-party information services provider that will digitally “sign” a transaction, attesting to the occurrence of specific conditions.\textsuperscript{21}

\textsuperscript{19} Hearn, \textit{supra} note 8.
\textsuperscript{21} Thomas & Schwartz, \textit{supra} note 16.
Turning again to the interest rate swap example, an oracle could be used to provide interest rate information on a payment calculation date. The oracle’s digital signature would be retained on the distributed ledger so that parties could review the payment process and confirm that payments were made correctly.

Note that parties to a smart contract will need the oracle to be a trusted party so that there are no insinuations that the oracle has colluded with one of the contract parties, or has reported incorrectly. In the interest rate swap example, neither Party A nor Party B can rely on the other to report interest rate information correctly, because both parties have an economic incentive to make their payment smaller than the other party’s payment. Party A, the payer of a fixed rate of interest, has an incentive to make the floating rate higher so that Party B has to pay more than Party A. Party B has an incentive to make the floating rate lower. While there would be a penalty if either party lied, as performance is automated under the smart contract, the lie would cause a payment to be made in error, and the parties would need to correct the mistake. A more efficient solution would be a trusted data provider to serve that function, which will be neutral to both parties.

Parties will also need to ensure that an oracle does not “go dark” and stop providing information, either due to technical errors or because the oracle simply decides to stop providing services. The oracle should agree to minimum standards of availability and a minimum subscription period. Alternatively, multiple oracles can be used for the same smart contract, using a “majority rules” method to determine when a condition has occurred.

CONCERNS WITH THE SMART CONTRACT MODEL

One notable recent example of smart contracts is the Decentralized Autonomous Organization (“DAO”), a pseudonymous, crowd-sourced investment vehicle using the digital currency Ether. To participate in the DAO smart contract, investors transferred their Ether to a common pool, similar to paying cash to invest in a mutual fund. The DAO smart contract code was designed to enable these investors to vote on how the Ether pool would be invested. The smart contract also contained a function that an investor could
invoke to enable him or her to exit from the DAO. This function, when executed, told the DAO where to distribute their Ether.\(^{22}\)

However, a flaw in the DAO smart contract code enabled a user to continually exercise the removal request – even though he had already taken out more Ether than he had put in. The flaw existed because the removal function could be exercised recursively – that is, the recall function could be exercised continually without checking whether the user had already withdrawn the total amount he contributed to the DAO.\(^{23}\) Because the Ethereum blockchain\(^{24}\) is designed to prevent rollback of transactions, and because there is no central authority to force the user to undo the transaction, there was no mechanism in the code to put the stolen Ether back into the right hands.\(^{25}\) Further, remedies outside the Ethereum blockchain, such as litigation, were not viable because due to the pseudonymous nature of the Ethereum blockchain, which made it impossible to determine the identity of the malfeasant user.\(^{26}\)

Users of smart contracts should be aware of the risks of using untested code in a pseudonymous or anonymous context without remedies for hacking or flaws in code. On networks such as the Ethereum network, anyone can become a network participant simply by downloading and running the code,


\(^{23}\) Phil Daian, *Analysis of the DAO exploit*, HACKING, DISTRIB. (June 18, 2016), http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/ [https://perma.cc/7KDM-EXCG].

\(^{24}\) The blockchain on which the virtual currency Ether is maintained is called the “Ethereum” blockchain. ETHER, https://www.ethereum.org/ether (last visited Apr. 3, 2017) [https://perma.cc/YC38-WRQT].

\(^{25}\) Eventually, leaders in the Ethereum community determined to run a special version of the Ethereum blockchain that basically pretended that the DAO attack had never happened. This special version was accepted by operators of more than 50% of the “hashing” power of the Ethereum blockchain (i.e., machines comprising more than 50% of the computing power of all the computers operating the Ethereum blockchain). After this highly controversial patch, DAO investors got their funds back in a sense. However, this also effected a split or “hard fork” in the code – now there are two Ethereum blockchains, each of which has its own virtual currency, but only one of which reversed the DAO hack. So, the value of Ether is split between the two competing blockchains. Pete Rizzo, *Ethereum Hard Fork Creates Competing Currencies as Support for Ethereum Classic Rises*, COINDESK (July 24, 2016, 9:21 PM), http://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/ [https://perma.cc/XSE2-8M3P].

\(^{26}\) Siegel, *supra* note 22.
which is open source and available to everyone. No identification or authorization is necessary. In contrast, many of the distributed ledger platforms being built now are meant for use on a permissioned-only basis. In a permissioned-only ledger, one or more network operators act as gatekeepers on the network and only allow participants to access the network once they have been identified and met any applicable access criteria. If the identity of all participants is known, a malfeasant participant can be subject to legal remedies.

**ENFORCEMENT OUTSIDE THE DISTRIBUTED LEDGER CONTEXT**

Provisions such as payment requirements can easily be automated, and with oracles automatic termination can be instituted upon the occurrence of specified events. However, even for relatively standardized contracts such as interest rate swaps, enforcement of provisions such as confidentiality requirements is likely to require court intervention. And in cases such as the DAO where flaws in code allow a participant to take actions that are not permitted by the terms of the agreement among the parties, court invention may also be needed.

In such a situation, courts should be able to look to enforcement of digitally-signed contracts as a roadmap. For example, the Uniform Electronic Transactions Act provides for a broad variety of electronic methods of assenting to a contract, including “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” Digital signatures using public/private key cryptography should fall comfortably into this definition.

Of course, to take advantage of remedies only available in court, the counterparty to the contract must be identifiable. The recent DAO hack illustrates this point best. Unknown hackers exploited a weakness in the code of the DAO contract and withdrew Ether from investors who were parties to the DAO contract. The reason why other participants in the DAO had no recourse against the hackers was not due to some perceived difference between smart contracts and traditional contracts, but because the parties against whom the contract would be enforced were unknown. This is a key

---

27 The Digital Asset Platform, supra note 10.
28 Uniform Electronic Transactions Act, Section 2(8).
29 Siegel, supra note 22.
argument in favor of permissioned ledgers, where parties’ identities are known and validated.

CONCLUSION

Smart contracts can be viewed as merely another means to evidence legally binding relationships—however, their emergence has and will continue to change the way parties transact. As the use of smart contracts becomes more widespread, the efficiency gains they promise will become reality. However, market participants will need to be aware of potential security flaws and ensure that they can trust not only the counterparty to the contract, but also the code itself.
Machine Learning and FinTech

Spencer McManus*

Cite as: 1 GEO. L. TECH. REV. 428 (2017)
https://perma.cc/29UG-CF3E

INTRODUCTION

Machine learning describes the process through which computers can learn without continued human input. In the era of big data, machine learning is particularly promising because it allows for identification of patterns in large data sets. Machine learning has applications in fields as diverse as medicine, e-commerce, and banking. This essay will discuss the application of machine learning, particularly explanation-based learning, to the financial tech industry, focusing on fraud detection.

A BRIEF HISTORY OF MACHINE LEARNING

The concept of machine learning first arose in 1950 with Alan Turing’s paper Computing Machinery and Intelligence,1 in which Turing proposed to answer the question, “Can machines think?” To answer this question, Turing crafted what became known as the “Turing Test” with three participants: one human judge, one human player, and one computer. The judge, placed separately from the human and the computer, aims to determine which of the two is a human and which is a computer. A computer “passes” the Turing Test when the judge cannot consistently distinguish the computer

* GLTR Staff Member; Georgetown Law, J.D. expected 2018; University of California, Davis, B.A.S. 2015. © 2017, Spencer McManus.
1 A.M. Turing, Computing Machinery & Intelligence, 59 MIND 433 (1950).
player from the human player.\textsuperscript{2} Turing predicted that humans could program computers that would pass the test by 2000.\textsuperscript{3}

Over the next four decades, scholars and programmers refined the concept of machine learning and developed new tests. In 1959, IBM programmer Arthur Samuel created a checkers program in which the computer improved progressively the more it played.\textsuperscript{4} Programmers focused on developing machines that performed pattern recognition over the next two decades. These efforts culminated in the introduction of Explanation-Based Learning (“EBL”),\textsuperscript{5} in which a machine uses a set of programmer-supplied “training data” to identify patterns, synthesize rules, and apply the rules to new sets of data.\textsuperscript{6}

From the 1990’s to today, work has transitioned to developing machines that can handle large amounts of data to draw conclusions.\textsuperscript{7} Machine learning has been extended to include “deep learning,” which involves use of increased processing power to analyze visual and auditory data in real-time.\textsuperscript{8} Large technology companies have developed their own proprietary machine learning code that acts as the backbone for certain features of their products.\textsuperscript{9} Future development focuses on continued improvement in natural language processing—which allows for human voice interaction with devices\textsuperscript{10}—and applying machine learning to new industries.

\textsuperscript{2} Id. at 442.

\textsuperscript{3} Id.


\textsuperscript{5} See infra Part II.

\textsuperscript{6} See generally Gerald Dejong & Raymond J. Mooney, Explanation-Based Learning: An Alternative View, 1 MACH. LEARNING 145 (1986).

\textsuperscript{7} See Marr, supra note 4.


\textsuperscript{9} Examples include Facebook’s DeepFace, which powers the social network’s facial detection feature, and numerous digital assistant applications, including Apple’s Siri, Amazon’s Alexa, and Microsoft’s Cortana. See, e.g., Steven Levy, The iBrain is Here, and It’s Already Inside Your Phone, BACKCHANNEL (Aug. 24, 2016), https://backchannel.com/an-exclusive-look-at-how-ai-and-machine-learning-work-at-apple-8dbfb131932b#.6wi4d8qcy [https://perma.cc/Z9KG-8LQ8] (explaining how Apple uses machine learning in their products, including Siri).

\textsuperscript{10} See Perry Li, Natural Language Processing, 1 GEO. L. TECH. REV. 98 (2016), https://www.georgetownlawtechreview.org/natural-language-processing/GLTR-11-2016/
PATTERN RECOGNITION AND EXPLANATION-BASED LEARNING: AN E-COMMERCE EXAMPLE

Although there are several methodologies for machine learning, this article focuses on explanation-based learning. Explanation-based learning (“EBL”) involves teaching a machine to detect patterns in data based on a set of programmer-supplied “training data,” using the patterns to create a rule and then applying the rule to larger sets of data to make predictions. A simplified but powerful example from the e-commerce industry will help illustrate the process.11

Retail companies face the challenge of catering to individual customers in a growing global economy. Machine learning can help retailers by providing extremely personalized predictions about how an individual’s shopping habits may change given a change in personal circumstances. The simple system illustrated here will involve a machine learning system predicting whether a customer is pregnant.

Training Data

The first requirement for a machine learning system is “training data.” Training data consists of different data points (called “features”), which come together to form an individual “record,” and an output value (the “target”).12 Training data is necessary because the machine cannot make predictions without examples of how the different features affect the output. In our example, the features will be the customer’s age and whether or not she purchases two products commonly associated with pregnancy. These features come together to form ten “records”: in this case, a purchasing history for one


11 This example is based on the (in)famous Target “baby club” story, in which Target, using a machine learning model, predicted that a teenage customer was pregnant. Target started sending her baby coupons, which were discovered by her father, who had not yet been informed about the pregnancy. For background, including more on how e-commerce companies leverage machine learning, see Charles Duhigg, How Companies Learn Your Secrets, N.Y. TIMES MAGAZINE (Feb. 16, 2002), https://nyti.ms/2jEboTD [https://perma.cc/9Y2L-HCLH].

customer. The target is whether the customer was actually pregnant. Table 1 shows this data.

<table>
<thead>
<tr>
<th>#</th>
<th>AGE</th>
<th>PREGNANCY TEST?</th>
<th>PRE-NATAL SUPPLEMENTS?</th>
<th>PREGNANT?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>24</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>36</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>40</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>33</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>25</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9</td>
<td>35</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Table 1. Training data for hypothetical pregnancy prediction.**

**Decision Trees**

From this set of ten records and their corresponding outputs, the computer can form a “decision tree,” a process for evaluating the probability of the output occurring given the value of each feature. This is a decision tree for this problem, with row (A) showing the probabilities of pregnancy given the training data in Table 1.

---

13 This hypothetical example ignores the difficulty (and potentially legality) of determining if a customer was actually pregnant. See id.
With this small amount of data, the decision tree is not particularly useful to the retailer. The ten records do not capture the purchasing trends of the entire customer base; two branches of the tree remain empty. Imagine instead that a larger set of training data (say, with 10,000 records) produced the probabilities in row (B) in Figure 1. This data would be useful to a retailer, especially where the data produced high or low probabilities.

**Evaluating the Model**

Now that the model has been developed from an adequate training set, the retailer can utilize the model to make predictions about new customers. A retailer could, say, send coupons for baby products to a potentially pregnant customer who fits in one of the high probability categories. If the customer is indeed pregnant, the coupons might encourage her to shop at the retailer.

However, no decision tree is perfect because of practical limitations in data collection. In this case, the decision tree uses a limited set of data to produce probabilities that a customer with a given shopping history is pregnant. The retailer needs to evaluate if its model is actually effective at predicting if a customer is pregnant.
The shaded areas are where the retailer uses the model and determines that a customer is pregnant; the white areas are where the retailer determined the customer was not pregnant. The retailer should aim to minimize the number of women in the red shaded area (a “false positive,” where the retailer determined someone was pregnant, but she wasn’t) and maximize the number of women in the green shaded area (where the retailer correctly identified someone as pregnant).

The retailer can evaluate this by calculating “precision” and “recall.”14 In our example, precision is the percentage of customers predicted to be pregnant who actually are. Higher precision indicates fewer false positives. Recall is the percentage of all pregnant customers who are identified by the model. Higher recall indicates fewer false negatives. There is a relationship between precision and recall. As a retailer raises the probability threshold for predicting someone is pregnant, it will reduce false positives (and thus increase precision), but it will also increase false negatives (thus reducing

---

recall). If a retailer decides that the model must have 85% certainty that a customer is pregnant instead of 75%, it will exclude customers whose product purchases suggest between a 75% and 85% probability of pregnant. It is very possible that customers in this range are pregnant, but that the increased probability threshold will produce false negatives for these customers.

A retailer faces obvious obstacles in determining numbers of actually pregnant customers, but this could be accomplished through surveys of customers. By further refining the model through evaluation of the most predictive features, the trade-off between precision and recall can be reduced, creating a higher quality model and giving the retailer the maximum benefits of a machine learning system.

EBL AND FRAUD DETECTION

EBL is commonly used in the financial technology space to detect credit card fraud. Financial institutions often license fraud-detection software from third-parties. This software, in its most simplified form, utilizes hundreds or thousands of features to form a decision tree, producing probabilities used to predict if a transaction is fraudulent.  

Using a system similar to that in the pregnancy example, fraud detection companies identify features that, when analyzed together, are highly predictive of fraud. In this simplified example, a fraud detection company could build a system using three different features to detect basic instances of fraud on a single card: the country of use for a charge, the charge amount, and the number of countries used in a given time period.

<table>
<thead>
<tr>
<th>#</th>
<th>COUNTRY</th>
<th>CHARGE AMOUNT</th>
<th>NO. COUNTRIES IN 24-HOUR PERIOD</th>
<th>FRAUD?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USA</td>
<td>$20</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>RUS</td>
<td>$150</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>USA</td>
<td>$200</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>CAN</td>
<td>$10</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>CAN</td>
<td>$15</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

TABLE 2. Training data for a simple fraud detection model.

15 See, e.g., Manapat, supra note 12.
16 See id.
Fraud detection can be quite difficult. From a cursory examination of the training data, there does not seem to be a consistent pattern. Although some transactions may be quite obviously fraud (such as record 2, where a charge was made in a country not present in other records), other patterns are not so evident (such as a correlation between number of countries and fraudulent charges). Machine learning becomes particularly useful in the fraud detection industry because it enables companies to quickly analyze complex sets of data. For example, the developer of this model may determine that the third feature is not particularly predictive of fraud. One benefit of EBL in this space is that companies can identify relevant features and exclude irrelevant ones.\(^{17}\)

EBL continues to grow in other financial spheres as well. Banks use EBL to analyze customer traits (including past defaults, job status, and marital status) to approve or reject loans.\(^{18}\) Other financial institutions use EBL to power “robo-advisors” that advise customers on allocating investments and financial instruments.\(^{19}\) In the future, EBL could power new security systems for banking (such as facial recognition) or even finance-specific customer service systems.\(^{20}\)

CONCLUSION

Since Alan Turing first hypothesized a thinking machine in 1950, machine learning has developed into a powerful tool. In explanation-based learning, one of the many different types of machine learning, a human provides a set of training data, which includes several features and records, from which a machine extrapolates patterns and creates rules. We encounter these systems every day: in e-commerce and fraud detection, machine learning forms a critical backbone. Future development of EBL will focus on applying the technology to new technologies in the era of big data.


\(^{19}\) Id.

\(^{20}\) Id.
INTRODUCTION

Soon after the New York Department of Financial Services (DFS) proposed a comprehensive cybersecurity regulation in September 2016, fear rippled throughout the financial services and technology industries. The proposal imposed unprecedented obligations on banks, insurance companies, and other financial services firms under the jurisdiction of New York’s Department of Financial Services. Two months later, DFS significantly revised the proposal and issued a regulation that went into effect on March 1, 2017.

The following will discuss the new requirements New York’s financial regulators will impose on its regulated companies, and argue that the revised

---

1 Assistant Professor of Cybersecurity Law, United States Naval Academy; J.D. Georgetown University Law Center; M.P.P., B.A. University of Michigan; The views expressed in this Article are only those of the author and do not reflect the views of the Naval Academy, Department of Navy, or Defense Department. © 2017, Jeff Kosseff.


regulation is a model of a rigorous, fair, and technologically sound cybersecurity regulation. New York’s regulation could serve as a model for a uniform nationwide cybersecurity regulation that would provide certainty and clarity to companies while protecting the confidentiality, integrity, and availability of information and systems. Cybersecurity law in the United States currently is a patchwork of outdated privacy and computer crime laws; New York’s regulation, in contrast, is a model cybersecurity statute for the modern era.

BACKGROUND OF NEW YORK’S FINANCIAL CYBERSECURITY RULES

As every industry becomes increasingly dependent on technology, they become increasingly vulnerable to cyberattacks. Wall Street is a particularly attractive target for criminals and state actors worldwide, as the results of a successful attack could lead to mass economic disruption and a financial windfall for the hackers. In 2016, the U.S. Justice Department revealed that over five years, hackers linked to the Iranian government had attacked more than four dozen U.S. financial institutions, including Bank of America Corp., the New York Stock Exchange, and JPMorgan Chase & Co.

On September 13, 2016, New York Governor Andrew Cuomo announced a “first-in-the-nation regulation” designed to protect the cybersecurity of banks, insurance companies, and other financial institutions that are regulated by the New York DFS. The proposed regulation would require regulated companies to establish cybersecurity programs and policies, conduct annual cybersecurity assessments, and take other specific steps to

4 See Portia Crowe, The pillars of American finance are under attack, BUS. INSIDER (Oct. 18, 2015, 2:06 PM), http://www.businessinsider.com/wall-street-cyberattacks-2015-10 [https://perma.cc/E4QJ-3JFN] (“Wall Street has a cybersecurity problem. Hackers have gone after banks, brokerages, and news wires, and now it looks as if they may have gone after business reporters as well.”).
secure information and networks.\(^7\) In a written statement, Cuomo boasted that New York “is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, global terrorist networks, and other criminal enterprises.”\(^8\)

Regulated financial institutions were not as enthusiastic about the proposal. In a November 14, 2016 letter to DFS, representatives from institutions such as the American Bankers Association and the National Association of Mutual Insurance Companies wrote that although they “strongly support” New York’s goal of protecting financial institutions’ customer information and information technology systems, the proposal was not “risk-based, flexible, [or] workable.”\(^9\) Among their concerns with the initial proposal, the required cybersecurity programs and policies did not account for the amount of risk that a company faces.\(^10\) Moreover, they argued, certain proposed requirements, such as annual assessments of all service providers, are “practically unworkable or technically infeasible.”\(^11\) DFS responded on December 28, 2016 with a revised proposal, which went into effect on March 1, 2017.\(^12\) The new proposed regulation incorporated many of the concerns that industry groups raised, and eased some of the other proposed requirements. For instance, the American Insurance Association praised the New York regulators for addressing “our concerns regarding some of the more restrictive and burdensome requirements of the regulation[].”\(^13\)

\(^{7}\) Id.

\(^{8}\) Id.


\(^{10}\) Id. at 1.

\(^{11}\) Id. at 2.

\(^{12}\) 23 NYCRR § 500, supra note 2.

OVERVIEW OF NEW YORK’S FINANCIAL CYBERSECURITY REGULATION

New York’s cybersecurity regulation is among the most detailed and thorough in the United States. This section provides an overview of the regulation’s key provisions.

Under the regulation, regulated companies must conduct periodic assessments\(^\text{14}\) that consider the risks particular to the companies’ cybersecurity, information system, and nonpublic information, which includes: (1) business information that could cause a “material adverse impact” to the company if disclosed; (2) individual’s personal information, which is a name or other identifier in combination with a social security number, drivers’ license number, financial account number, financial account password, or biometric information; or (3) certain health information.\(^\text{15}\) Companies must use these risk assessments to develop cybersecurity programs that: (1) address risks to the security and integrity of nonpublic information; (2) use “defensive infrastructure” to protect systems and nonpublic information; (3) detect cybersecurity events, which are broadly defined as act or attempts “to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System[;]”\(^\text{16}\) (4) respond to cybersecurity events and reduce harm; (5) recovery from cybersecurity events; and (6) fulfill reporting requirements.\(^\text{17}\)

The cybersecurity program must require monitoring and testing to regularly evaluate the program’s effectiveness.\(^\text{18}\) If an agency does not continuously monitor for vulnerabilities, they must annually conduct penetration tests to determine whether the systems are accessible to hackers.\(^\text{19}\) Companies that do not continuously monitor also must conduct bi-annual vulnerability assessments.\(^\text{20}\) The programs also must develop programs to ensure the ongoing security of applications that have been developed in-house.\(^\text{21}\) Moreover, companies must securely dispose of nonpublic information once it is no longer necessary for business purposes.\(^\text{22}\)

\(^\text{14}\) N.Y. COMP. CODES R. & REGS. tit. 23, § 500.09.
\(^\text{15}\) tit. 23, § 500.01(g).
\(^\text{16}\) tit. 23, § 500.01(d).
\(^\text{17}\) tit. 23, § 500.02.
\(^\text{18}\) tit. 23, § 500.05.
\(^\text{19}\) Id.
\(^\text{20}\) Id.
\(^\text{21}\) N.Y. COMP. CODES R. & REGS. tit. 23, § 500.08 (2017).
\(^\text{22}\) tit. 23, § 500.13.
Cybersecurity programs also must include written incident response plans, which address the processes and goals for responding to cybersecurity events, the roles and responsibilities of decision-makers, internal and external communications, remediation procedures, and reporting incidents. Companies must notify DFS within 72 hours of determining that a cybersecurity event occurred. In addition to developing cybersecurity programs, regulated companies must develop written cybersecurity policies, approved by a senior officer or the board of directors, that address the following topics, if applicable:

- Information security;
- Data governance and classification;
- Asset inventory and device management;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Systems operations and availability concerns;
- Systems and network security;
- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and third party service provider management
- Risk assessment; and
- Incident response.

The regulation also requires companies to have a Chief Information Security Officer (CISO), employed directly by the company, an affiliate, or a third-party vendor. The CISO is responsible for compliance with the cybersecurity regulation and must submit a written report to the Board of Directors, at least annually, that documents the company’s cybersecurity program and risks. Companies also must ensure that cybersecurity personnel receive updated and sufficient training, and they must ensure that third-party

23 tit. 23, § 500.16.
24 tit. 23, § 500.17.
25 tit. 23, § 500.03.
26 tit. 23, § 500.04.
28 tit. 23, § 500.10.
service providers adhere to adequate cybersecurity policies and practices. Companies also should maintain “audit trails” that allow them to reconstruct financial transactions after cybersecurity events and help them detect and respond to potentially harmful attacks. The regulation also requires companies to use “effective controls” to prevent unauthorized access, and suggests that these controls may include multi-factor authentication or risk-based authentication, which requires additional information at log-in if the system detects anomalies.

The regulation also strongly encourages companies to encrypt nonpublic information both while the information is being transmitted across networks and while it is in storage (or “at rest”). However, the regulation allows companies to determine whether encryption is appropriate based on their risk assessments. If companies determine that encryption is infeasible, the CISO must approve alternative controls and review them at least once a year.

The regulation is less onerous on small businesses, which have fewer than 10 employees (including independent contractors, less than $5 million in gross annual revenues over the previous three fiscal years, or less than $10 million in year-end total assets.) Those companies are exempted from the following requirements: having a CISO, monitoring and testing their networks, maintaining audit trails, application security policies, training cybersecurity personnel, using multi-factor authentication or encryption, and maintaining an incident response plan.

Regulated businesses must comply with much of the regulation by September 1, 2017, though they will receive more time to adopt some of the requirements.

**THE STRENGTH OF NEW YORK’S REGULATION**

New York’s revised regulation could serve as a national model for modern cybersecurity law, particularly due to its sensible, risk-based approach.
instead of an across-the-board, bright-line rule that applies regardless of the actual risk of harm. Under New York’s risk-based approach, a company would be wise to focus its cybersecurity efforts on the protection of highly sensitive information, such as bank account numbers. In other words, New York’s regulation provides an incentive for companies to more effectively allocate their cybersecurity resources.

To be sure, the risk-based framework might create uncertainty for companies, which could legitimately fear that a regulator might believe their safeguards are insufficient for the amount of risk that the company faces. However, companies likely could overcome this uncertainty by carefully documenting the reasoning behind their decision to store data in a certain manner. As DFS implements the rule, it would be useful for the Department to issue non-binding guidance that provides examples of compliance with this risk-based framework.

New York’s financial cybersecurity regulation also is unique in that it refers to some of the most relevant and current safeguards, such as multi-factor authentication and vulnerability testing. About a dozen states have enacted data security statutes, but most of those laws only generally require the companies to adopt “reasonable” security procedures. Even Massachusetts, which has the most rigorous general data security requirements of the dozen states, is not as detailed and current in its requirements as the New York regulation.

Financial institutions also face data security regulations under the federal Gramm-Leach-Bliley Act, a 1999 statute that broadly requires agencies to adopt safeguards to “insure the security and confidentiality” of customer records, to protect the security and integrity of the records, and to protect those records from unauthorized access. Individual financial regulators have promulgated somewhat more specific regulations under the statute, but they focus primarily on data security, and not on cybersecurity.

---

38 See, e.g., Cal. Civ. Code § 1798.81.5 (“A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”).
41 Id.
The two are similar, but distinct, and can implicate different concerns. Data security refers to the protection of information stored by a system; cybersecurity refers to the integrity of a technological system. A compromise to the system could mean that an adversary has accessed private information stored by it, or it could mean the system has been rendered unusable. If Wall Street firms were focused only on securing the data, then they might not devote sufficient focus to detecting and repelling a threat to the cybersecurity of their entire system and networks. A massive denial of service attack could hobble Wall Street by making it impossible for securities to be traded for weeks, and the result would be an economic catastrophe.

Data security is, of course, an important component of cybersecurity. But cybersecurity is more broadly focused on attacks on networks and systems, in addition to information, which the New York regulation acknowledges. That more nuanced approach is why New York’s cybersecurity regulation is better suited for today’s threats than the data security laws that were passed in the late 1990s and early 2000s. By defining “cybersecurity event” as “any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such information system,” New York has focused not only on data security, but on cybersecurity as a whole.

The New York regulation also has benefits compared to the approaches of state and federal regulators, which often bring enforcement actions under general consumer protection statutes. For instance, the Federal Trade Commission (FTC) has brought dozens of data security cases under Section 5 of the Federal Trade Commission Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.” The statute defines “unfair” practices as those that cause or are likely to cause “substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” The FTC finds practices to be deceptive “if there is a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in

---

43 Id. (“These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.”).
44 N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(d).
the circumstances, to the consumer’s detriment.” The FTC has not promulgated any formal regulations as to the types of data security that are unfair or deceptive, though it has produced some informal recommendations based on previous enforcement actions. While the New York regulation does not prescribe specific steps to satisfy the requirements, it provides more details as to the types of issues that companies must address in their cybersecurity programs and policies.

The New York regulation is forward-looking, unlike many of our current approaches to cybersecurity. For instance, immediately after a data breach, a company must focus on how to properly notify consumers under the data breach notice laws of 47 states and the District of Columbia, each of which has unique requirements for the types of information that trigger the notice and the contents of the notice. While there are valid reasons for notifying customers – both to be transparent and to incentivize to invest in adequate security – our cybersecurity world has become hyper-focused on notifying consumers and regulators after a breach has occurred. Why not focus on rigorous and appropriate requirements that help to prevent breaches from occurring in the first place?

CONCLUSION

Although New York’s regulation only applies to banking, insurance, and financial services companies that are regulated by DFS, the vast majority of the regulatory structure is industry-neutral and could be used in cybersecurity laws that apply to any industry. I am not suggesting that every industry regulator in every state develop its own data security framework based on the New York financial regulation. Indeed, complying with a patchwork of overlapping data security requirements would be confusing, if not impossible, for many companies, similar to the difficulty of complying with 48 data breach notification laws. Rather, the New York regulation could

serve as a model for national cybersecurity legislation. For more than a
decade, Congress has considered many bills that would set a standard for
national data security and breach notification, preempting state laws. Those
proposals have failed to gain traction. However, these proposals generally
have suffered from the same shortcoming of other state and sector-specific
laws – they focus narrowly on data security, and not on modern cybersecurity
threats. The New York regulation, in contrast, addresses many of the most
pressing cybersecurity issues that companies face every day, and does so in a
way that fairly accounts for the burdens that regulations impose on small
companies that have limited information technology budgets. Although a
national law might ultimately look quite different from the New York
regulation, this at least provides a framework as we begin to think about the
contours of a strong, fair, and rigorous national cybersecurity law.
FINTECH MEETS THE TELEPHONE CONSUMER PROTECTION ACT

David Goodfriend* and David Nayer*

Cite as: 1 GEO. L. TECH. REV. 446 (2017)
https://perma.cc/E28J-9HNB

INTRODUCTION

It could happen any time—at work, at home, or on vacation. You receive a text message and glance at your smartphone. Your bank-issued credit card provider just sent you a message asking if you recognize a recent transaction. “Did you authorize a purchase of $5,000 for Super Bowl tickets? Text 1 for YES, 2 for NO.” You remember using your card to purchase tickets to an NBA playoff game but not to the Super Bowl. You reply, 2, and your credit card provider suspends the transaction. This text message may have saved you a significant amount of money and alerted you to possible identity theft. However, your card provider may have exposed itself to financial liability—not for the security breach, but for the unsolicited text message.

Fraud alerts from financial institutions are a classic application of “fintech,” the increasingly prevalent application of modern technology to enhance financial services.¹ Many fintech uses, including the above example, implicate the Telephone Consumer Protection Act (TCPA), a law passed in 1991 intended to prevent potentially unwanted, automated marketing calls.

While some of these communications, like the example above, may benefit the consumer, many are a source of frustration. Nearly 100,000 complaints of violations of the Do-Not-Call list were filed at the FCC in 2014, and amounting to forty percent of FCC consumer complaints.\(^2\) A fraud alert from a bank-issued credit card delivered via an automated outbound text message to a customer generally falls within the scope of what TCPA regulates but, as discussed below, the definitions of key terms in the TCPA have not always kept up with technology.

Recent action by the Federal Communications Commission (“FCC”) in establishing requirements for the behavior of financial institutions in circumstances like the fraud alert illustrates how telecommunications laws and policies have been slow to keep up with fintech developments. The story of fintech regulations shows how the advocacy of industry groups and consumer representatives can lead to compromises that seem to miss the mark. Current policy outcomes can be explained by regulators balancing opposing political perspectives instead of looking at the actual use of the technologies in question. This should come as no surprise to veterans of the administrative advocacy process, but the implications may be very real for fintech providers and consumers.

**A BRIEF INTRODUCTION TO THE TCPA**

The TCPA, as amended, and including its implemented FCC regulations, provides consumers with numerous protections from potentially unwanted telemarketing and automated calls.\(^3\)

Consent—and the requirement to seek it—is the lynchpin of TCPA liability. For all covered communications, the caller must receive prior express consent from the recipient to avoid liability.\(^4\) Covered communications include telemarketing or advertising messages,\(^5\) but communications under emergency circumstances are exempt.\(^6\) Text messages are treated as calls in

---


\(^3\) See 47 U.S.C. § 227; see also 47 § C.F.R. § 64.1200.

\(^4\) See 47 U.S.C. § 227(b)(1)–(2); see also 47 C.F.R. § 64.1200 (a)(1)–(3).

\(^5\) See 47 C.F.R. § 64.1200(a)(2).

\(^6\) See 47 U.S.C. § 227(b)(1)(A); see also 47 C.F.R. § 64.1200(a)(1).
the TCPA. Consent requirements also vary depending on the recipient, with wireless numbers generally subject to more protection from covered communications than residential landlines. The statute prohibits covered communications made with an artificial or pre-recorded voice (popularly known as robocalls) to both wireless and residential wireline numbers. Covered communications to wireless numbers made using an autodialer, equipment that can produce and call numbers using a number generator, are prohibited without prior express consent. For those calls that are permitted, the TCPA lays out further restrictions to minimize their invasiveness.

The FCC may exempt from consent requirements certain wireless calls not charged to the wireless customer and with such conditions as may be necessary to protect the customer’s privacy. This includes ensuring that text messages do not count against plan minutes or text message limits.

---

9 “Robocall” is used casually throughout the Omnibus Order, and is applied synonymously with calls that “require consumer consent” under the TCPA. See Omnibus Order at ¶ 1 & n.1.
10 See 47 U.S.C. § 227(b)(1)(A)(iii) and (b)(1)(B). Many Americans will note the prevalence of these artificial calls in the run-up to an election. By rule, robocalls to a residential line do not require consent if they are made on behalf of a tax-exempt organization, or if they do not constitute advertising or telemarketing. 47 C.F.R. § 64.1200(a)(3). However, artificial calls are also subject to further restriction; they must state the name of the calling entity at the beginning of the message. During the message, the call must state a telephone number. Solicitations must, within two seconds of stating the number, provide an automated, voice or key-activated opt-out system. 47 C.F.R. § 64.1200(b).
11 47 U.S.C. § 227(b)(1)(A)(iii). The statute also prohibits autodialers from targeting emergency services and hospital guest rooms, which may better illustrate the overall purpose of the restrictions. 47 U.S.C. § 227(b)(1)(A). As with robocalls, the consent requirement for autodialed calls is lifted if the message does not include advertising or telemarketing, or is made with the prior express written consent of the called party or the prior express consent of the called party when the call is made by or on behalf of a tax-exempt organization. 47 C.F.R. § 64.1200(a)(2).
12 Further restrictions include compliance with the National Do-Not-Call Registry (notably maintained by the Federal Trade Commission, not the FCC), maintenance of an internal do-not-call list and acceptance of call recipients’ desire not to be called again, and a prohibition on solicitations made outside the hours of 8 a.m.–9 p.m. in the recipient’s time zone. 47 C.F.R. § 64.1200(b), (c).
14 See Omnibus Order at ¶ 127 (citing Cargo Airline Order, 29 FCC Rcd 3432 at *3, ¶ 12).
The FCC enforces the TCPA and has promulgated regulations implementing the above protections. In addition to these agency remedies, the TCPA also creates a private right of action, so individuals may enjoin or recover actual monetary damages (with a minimum of $500 per violation) from TCPA violators, “if otherwise permitted by the laws or rules of court of a State.”

Most enforcement actions are brought in federal court and the damages can be enormous. Courts tend to apply FCC interpretations of the TCPA in determining the meaning of the statute.

**EVOlUTION OF THE TCPA – 2015 OMNIBUS DECLARATORY RULING**

Likely resulting from plaintiffs invoking judicial jurisdiction, stakeholders have come to the FCC seeking backward-looking declaratory rulings, rather than forward-looking, prophylactic rulemakings. In comparison to the rulemaking process, these declaratory rulings are disruptive, giving them unusually powerful implications across multiple industries, including financial services.

The latest example of this backward-looking approach is the FCC’s latest major interpretations of the TCPA, the 2015 TCPA Omnibus Declaratory Ruling and Order, combining twenty-one requests for clarification of various TCPA rules. This ruling is currently being challenged in the D.C. Circuit by a group of nine plaintiffs. While there are many issues raised and addressed in this Declaratory Ruling, three particularly interest financial services providers—the definition of autodialer, the expansion of the consent requirement, and the creation of a safe harbor for certain types of messages from financial institutions.

---

17 See Omnibus Order at ¶ 2.
19 See Omnibus Order at ¶ 2.
Predictive Autodialers

The Omnibus ruling attempted to clarify the definition of autodialing technology, which, as discussed above, is prohibited from calling emergency services and wireless numbers absent sufficient consent. Petitioners sought clarification as to whether “equipment used to make a call is an autodialer subject to the TCPA only if it is capable of storing or generating sequential or randomized numbers at the time of the call,” 20 (emphasis added).

The FCC stood by its functionality-based interpretation of the TCPA’s autodialer definition, affirming that “dialing equipment generally has the capacity to store or produce, and dial random or sequential numbers (and thus meets the TCPA’s definition of ‘autodialer’) even if it is not presently used for that purpose, including when the caller is calling a set list of consumers.” 21 Commenters (now Petitioners-appellants) contested the Commission’s statutory interpretation and argued that the definition of “capacity” was overbroad and limitless, and it could even extend to smartphones that store numbers in a directory and can make a pre-programmed, outbound call. 22 The FCC disagreed, reasoning that the record included no evidence of individual customers being sued under the TCPA for use of a smartphone, the scenario raised by petitioners. 23

In the opening example of the automated fraud alert text message, the sender of the text message generally uses predictive algorithms to identify transactions outside of a consumer’s normal behavior and automated equipment to send an outbound text message to the consumer. Although the FCC has concluded that the use of such techniques generally meets the FCC’s definition of “autodialer,” plaintiffs challenging the FCC’s interpretation argue that the definition is too vague as to future applications of the rule, rendering the Order both unconstitutional for its vagueness, 24 and impractical for compliance purposes. Defenders of the FCC decision argue that the FCC upholds Congress’ stated intent in passing the TCPA as demonstrated by Congressional validation of the broad regulatory approach 25 made to best

20 See Omnibus Order at ¶ 11.
21 Id. at ¶ 11-12.
22 Id. at ¶ 20-21.
23 Id. at ¶ 21.
25 See id. at 66.
capture as many intended technologies as possible. Thus, while sending a fraud alert via text message arguably could violate the TCPA’s consent requirements, it is difficult if not impossible to predict how future technological message-sending technologies might or might not trigger TCPA requirements.

Changes to the Consent Requirement

The FCC’s Omnibus Order also tackled questions related to the establishment, revocation, and transferability of consent. When a customer transfers her preferred method of communication with a company to a wireless device, the prior express consent remains intact despite the transfer to a new device. By contrast, if a wireless number is reassigned to a new subscriber, the original consumer’s consent does not transfer and callers may be liable, but for a one-call window intended to allow callers that do not have actual knowledge of the reassignment to seek necessary consent. The FCC also noted that because the TCPA is silent on the revocability of consent, the FCC interprets this absence in a light most favorable to consumers—consumers may unconditionally revoke their consent at any time. The Omnibus Order also ruled that simply having a contact in a phone’s address book alone does not grant prior express consent to receive messages from the contact under the TCPA.

These alterations to the consent regime also have been challenged by appellants as a violation of the Administrative Procedures Act and an impractical solution. Appellants argue that complying with the requirement to allow consumers to revoke consent by any reasonable method is unworkable, and therefore the regulation is arbitrary and capricious. Allowing customers to revoke consent in any way that a court later determines is reasonable arguably places an impractical burden of individualization and prevents callers from adopting a uniform cancellation policy.

---

26 See Omnibus Order at ¶ 16 (citing 1992 TCPA Order, 7 FCC Rcd at ¶ 6).
27 See id. at ¶ 47.
28 See Omnibus Order at ¶ 54.
29 See id. at ¶¶ 75-90.
30 See id. at ¶ 56.
31 See id. at ¶ 52.
33 See id. at 74.
Financial Institutions’ Safe Harbor

In a decision directed expressly at the financial services industry, the FCC’s Omnibus Order established a free-to-end-user safe harbor for financial institutions’ use of text messages and voice calls to consumers for non-telemarketing, non-advertising messages. Responding to a petition by the American Bankers Association (“ABA”), the FCC exempted from the prior express consent requirement, within limited conditions, certain messages about time-sensitive financial issues.34

The Order specified that financial institutions35 need not obtain prior consent to robocall or text message the customer if such calls or texts:

1. Are free to the user; meaning the call or text does not count against any wireless plan limits, such as minutes or text caps;36
2. Are limited to content concerning (a) alerts about fraud or identity theft; (b) alerts of possible security breaches of a customer’s personal information; (c) messages about steps customers can take to prevent or remedy harm caused by a data security breach; and (d) actions needed to arrange for receipt of pending money transfers;37
3. Are sent only to the wireless number provided by the customer of the financial institution;
4. State the name and contact information of the financial institution;
5. Do not include any telemarketing, cross-marketing, solicitation, debt collection, or advertising content;
6. Are limited to one minute or less for voice, 160 characters or less for text messages;
7. Number no more than three messages over a three-day period per event;
8. Offer recipients an easy “opt out” option to avoid such communications in the future, which in the case of text messages must be the ability to respond “STOP,” and

34 See Omnibus Order at ¶¶ 128-39.
35 Omnibus Order at ¶ 127 n.424. For purposes of the safe harbor, “financial institution” means any institution in the business of providing financial services “as described in section 4(k) of the Bank Holding Company Act of 1956.”
36 See id. at ¶ 139.
37 See id. at ¶¶ 128-33.
9. In the event a consumer opts out, the financial institution honors that request immediately.\footnote{See id. at ¶ 138.}

The FCC justified this safe harbor on the time sensitivity of the use cases in question and the speed at which consumers tend to open text messages.\footnote{Omnibus Order at ¶ 128. Although not discussed in this article, the safe harbor exception also applies to certain healthcare-related messages for similar reasons.} Citing record evidence, the FCC noted that “seconds count” in situations where fraud may be occurring,\footnote{Omnibus Order at ¶ 129.} and that similar time sensitivity exists where data security breaches or identity theft may have occurred.\footnote{See id. at ¶ 129.} It noted the “urgency” of the situation, the “unpredictable timing” of the problem, and the “financial repercussions” at stake.\footnote{See id. at ¶ 130.} Similarly, with respect to money transfers, senders and recipients may not have engaged in such transfers in the past and verification in real time is necessary, an “exigency” the FCC found to be time-sensitive.\footnote{See id.}

The FCC relied on evidence submitted by the ABA that 98% of text messages are opened within three minutes of receipt, justifying text messaging as the ideal communications platform for financial institutions’ time-sensitive communications.\footnote{See id. at ¶ 128 (citing ABA Petition at 5).}

In the case of the Super Bowl ticket purchase fraud alert discussed above, if a customer receives an alert of possible fraud from a financial institution, such messages would have to conform with the FCC’s TCPA consent exemptions (unless the institution had already received prior consent). The message must be: free to the customer, with zero impact on her phone bill; within one of the Order’s four content categories discussed in the second item above, in this case a fraud alert; sent to the wireless number provided by the customer; sent with the name and contact information of the financial institution; within prescribed length and frequency limits; free of any telemarketing, cross-marketing, solicitation, debt collection, or advertising; and sent with the “STOP” opt-out.
ADVOCACY BEHIND THE FINANCIAL INSTITUTIONS SAFE HARBOR

The safe harbor exemption for certain exigent financial-services messages potentially saves financial institutions from massive liabilities, presumably improving the service that they provide to their customers, but the exemption is subject to some seemingly random conditions, such as the three-calls-over-three-days limit. The administrative process and advocacy through which the safe harbor arose explain some of these peculiarities and illustrate how public policy often results in compromise between adversarial parties, to the complete satisfaction of none.

The ABA’s initial request for a declaratory ruling set out the four situations under which it sought an exemption from prior notice requirements and offered limitations on the use of such communications.45 The FCC quoted directly from the ABA’s petition,46 and adopted many of its recommendations nearly verbatim.47

However, the ABA was not acting in a vacuum. The National Consumer Law Center, a non-profit consumer advocacy organization specializing in TCPA and financial services issues, opposed the ABA petition, arguing that if the text messages concerned real emergencies, then such messages would fall within the well-established emergency exemption for prior consent and would not require any further safe harbor.48 It also argued that financial institutions could secure prior consent to make calls or send texts in certain circumstances, rendering a safe harbor unnecessary.49 In the event that the FCC adopted the ABA’s proposed safe harbor, however, NCLC argued for stricter limitations than those proffered by ABA, such as a limit on the number of communications and an easy opt-out option.50

The FCC seems to have struck a compromise. It adopted the ABA’s requested safe harbor but tempered it with the NCLC-recommended easy opt-out and cap on the number of calls or messages (i.e., no more than three calls

46 See Omnibus Order at ¶ 127 (quoting ABA Petition at 3).
47 See Omnibus Order, supra note 26 at 29.
49 See id. at 5.
50 See id.
or messages over a three-day period for any given event).\(^{51}\) The ABA originally had argued against any cap on calls or text messages, such as that established in a prior declaratory ruling, pointing to the importance of reaching the customer in exigent circumstances and noting that institutions had no incentive to send repeated messages other than to alert a customer to protect his or her assets.\(^{52}\)

According to individuals involved in the deliberations, FCC staff sought NCLC’s agreement to a certain number of calls or texts within a given time frame, to which NCLC ultimately acquiesced, despite having originally argued against any safe harbor. This is consistent with a statement made by the ABA in one of its final ex parte filings, in which it stated that an agreement had been reached with consumer advocates.\(^{53}\) Although the ABA originally argued that there should be no limit on the number of contacts to ensure that customers were reached, ultimately the FCC imposed the cap of three messages over a three-day period.\(^{54}\)

The cap on calls or texts, while adapted from earlier precedent, appears to be a middle ground position unrelated to the on-the-ground facts and is disfavored by the affected parties—the banks, which do not want a cap,\(^{55}\) and the consumer advocates, which did not support the safe harbor device in the first place.\(^{56}\) Moreover, to ensure that text messages are “free” to the recipient, the consumer’s wireless provider—not the financial institution instigating the message—ultimately has discretion. A financial institution must have an agreement in place with every wireless provider to ensure that safe-harbor communications are free to all recipients. A failure by the wireless carrier to comply places the financial institution outside of the safe harbor and thus subject to liability. This is a tenuous chain of responsibility for a financial institution seeking the benefit of the safe harbor.

NCLC’s argument that emergency communications already are exempt from the prior notice requirement begs the question, why not simply deem the four situations to be emergencies outside the scope of the prior-consent requirement? This would have afforded the financial institutions

\(^{51}\) See Omnibus Order at ¶ 135.

\(^{52}\) See Omnibus Order at ¶ 134 (citing Cargo Airline Order, 29 FCC Rcd 3432 at 5, ¶ 18).


\(^{54}\) See Omnibus Order at ¶ 135.

\(^{55}\) See Petition for Exemption, supra note 45, at 18.

\(^{56}\) See Letter from Margot Saunders, supra note 48 at 4-5.
sufficient clarity, if that is what they sought, without the detailed restrictions imposed in the ruling. Consumer advocates logically could wonder, given this easier option, whether motives in addition to liability protection might have animated the ABA proposal.

**THE FUTURE OF THE TCPA**

The future of these and associated rules *writ large* is uncertain. The D.C. Circuit is reviewing aspects of the 2015 ruling and could remand all or parts of the order back to the FCC for reevaluation. Then-FCC Commissioner, now Chairman Ajit Pai issued an exhaustive dissent alongside the Omnibus Order, which many of the appellants cited in their brief and echo in theory.57

Under the new leadership of Chairman Pai, the FCC could take a less restrictive view of the consent requirement, easing the regulatory burden on financial institutions to spend resources achieving that consent. On the other hand, the safe harbor could remain unchanged. Even on remand from the D.C. Circuit, Chairman Pai—a former Senate staff member and student of politics—could decide that there are too many political risks to reversing entirely what could be characterized as “anti-robocall” rules. Chairman Pai even acknowledged in his dissent that “fraudulent telemarketing” is a problem, one that he has experienced personally.58 In his first speech after being named Chairman, Pai restated his feelings on telemarketing and suggested that the FCC should make it easier for consumers to report robocalls and for the FCC to take action.59 Ahead of his March 23, 2017 FCC Open Meeting, Chairman Pai previewed an agenda item aimed at reducing unwanted robocalls.60 He called upon the FCC to take further action to prevent these calls. The proposed rules empower the private sector, giving carriers tools to block calls that come from unassigned numbers. Regardless of how the TCPA may be altered by judicial or administrative decisions,

57 See DISSERTING STATEMENT OF COMMISSIONER AJIT PAI, supra note 2.
58 Id. at 1.
however, the statute and fintech surely will continue to intersect, especially as technological innovations in financial transactions proliferate.
INTRODUCTION

Today, the average person spends the majority of time plugged into the internet. A phone has become a pocket assistant that lives in the Cloud, binge streaming TV shows online has become a popular Saturday night affair, and most job searches entail uploading a resume to the Internet. Even children can be exposed to the Internet at young ages through education websites and tablet apps. Many children may turn to physical toys to get some time away from screen. Toy manufacturers, however, are increasingly developing toys that connect to the Internet.1 Many physical toys on the market today, though screenless, connect to the Internet in some way, whether directly to the Cloud or via an app. These are called connected toys.2

---

2 Id.
There is a range of connected toys on the market right now. Some focus on giving a child a companion, some focus on toy customizability, and some focus on education. Wiggy, a connected toy, focuses on financial education.

THE TECHNOLOGY

In 2016, Spiral Toys released Wiggy, a physical piggy bank that connects to an app through which parents, relatives, or other loved ones can send money to children for finishing chores or as birthday presents. The physical pig toy connects to the Wiggy app on a device through Bluetooth, while the app connects to the internet. The funds that parents send to their children’s Wiggy account show up on the child’s app account. Parents can also choose to withdraw funds, set tasks, or use ‘stars’ in the app to send a more abstract reward. Children can set tasks, view their funds, and add items to a wish list.

---

3 See Meet Wiggy, WIGGY, http://wiggyapp.com/ (last visited Mar. 15, 2017) [https://perma.cc/A8JJ-AN38]. Additionally, the app’s functions were explored and downloaded onto an Android on February 2, 2017.

4 Apps that accompany connected toys may connect to the internet in a variety of ways. Some apps may connect directly to the internet, sometimes to a cloud server, which enables certain features such as location tracking and receiving data from the internet that allows deeper levels of interactive playtime. For example, the connected Furby toy allows real-time interaction with the physical toy reacting to games one can play on the accompanying app. See Furby Connect World, Permissions: View Details, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.hasbro.FurbyWorldAPPSTORE&hl=en (last updated Dec. 6, 2016) [https://perma.cc/D62C-APPK]. This contrasts with other ways an accompanying app may connect with the internet, such as when the app goes through automatic updates, connecting to the cloud only when it updates the app, but not sharing or receiving data in any way. For example, the accompanying app for CHiP, a robot dog, does not connect to the internet directly unless it is processing an update to the app as the app only acts as a remote control for the physical toy. See CHiP – Your Lovable Robot Dog, Permissions: View Details, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.wowwee.chip&hl=en (last updated Jan. 26, 2017) [https://perma.cc/6TLT-YK7E]. The Wiggy app connects to the internet directly as it tracks location and receives data from the internet. See Wiggy Toy App (Unreleased), Permissions: View Details, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.spiraltoys.wiggypiggy&hl=en (last updated Feb. 1, 2017) [https://perma.cc/63XD-U9WH].
Using technology to teach children practical lessons about money is nothing new. Spiral Toys, however, seems to be developing a way to connect parent bank accounts to Wiggy to allow funds to be rooted in spendable money. The company stated that this aspect of Wiggy would “become a reoccurring monthly revenue stream for Spiral. Spiral has found multiple avenues for maximizing the revenue opportunity with Wiggy by developing these revenue streams.” Spiral explains that this service is implemented using Wiggy Cards. The Wiggy Card would function like a digital wallet and pre-paid debit card for children. The details of how Spiral will gain revenue through this service, or how children will be able to use the pre-paid debit card and whether only certain venues will accept it remains unclear. That being said, the service that Spiral describes implies that Wiggy may act as a sort of financer between banks and consumers, much like Venmo.

5 In 1971, the game Oregon Trail was developed, with the 1992 computer game version popularly used in schools to teach children not just about history, but also about resource and finance management. See Bonnie Burton, Oregon Trail game co-inventor talks pioneer survival and life lessons, CNET (Feb. 6, 2016), https://www.cnet.com/news/oregon-trail-game-co-inventor-talks-pioneer-survival-and-life-lessons/ [https://perma.cc/Q9JP-KMZN].

6 It is unclear whether Spiral Toys is in the process of developing or has already implemented a method that would allow parents to link their Wiggy accounts to bank accounts to send their children spendable money. See Wiggy: The Smartest Way To Get Your Kids Savings, SPIRAL TOYS, http://spiraltoys.com/wiggy/ (last visited Feb. 12, 2017) [https://perma.cc/2TN8-3KGV] (stating “Once each task is complete, you transfer the reward to your child’s Wiggy Card instantly[.]” and “[i]n short, the Wiggy Card is real money! It functions as a digital wallet and prepaid debit card designed just for kids.”); see Spiral Toys Provides Product Update and 2016 Outlook, SPIRAL TOYS (June 30, 2016), http://spiraltoys.com/spiral-toys-provides-product-update-and-2016-outlook/ [https://perma.cc/JF2Z-EE8S] (stating “Spiral has expanded the current feature set to include parent approved ecommerce transactions by potentially partnering with large online retailers such as Amazon and Walmart through their affiliate programs. This affiliate program will become an additional revenue stream for Spiral. In addition, Spiral is developing a debit card program with a leading nationwide debit card provider. Doing so will allow parents to set-up a debit card for their children from their Wiggy account.”).


Usually P2P services do not produce revenue unless done with a credit card that charges fees. This brings up an interesting question of what kinds of laws apply to a connected toy such as Wiggy, which implicates both children’s personal information and financial privacy issues.

**THE LAWS**

Organizations that conduct P2P services may be referred to as money transmitters, since they are not financial institutions, such as a bank, but still handle the exchange of financial substance and information. In this case, Wiggy can be considered a money transmitter toy. Setting aside several state data breach or financial privacy acts that may apply, several federal privacy laws may apply to a money transmitter toy such as Wiggy.

*Children’s Online Privacy Protection Act*

First, the Children’s Online Privacy Protection Act (COPPA) applies to a connected toy such as Wiggy. COPPA regulates operators of online services that directly target children under the age of thirteen, or companies that have actual knowledge that they are collecting, using, or disclosing personal information from children under thirteen. The Federal Trade Commission (FTC), which has the ability to bring enforcement actions against online service providers under COPPA, has indicated that it considers COPPA to apply to connected toys, as some of their functions rely on online services. The FTC applies COPPA to online services such as online games, websites, and applications. COPPA applies to these connected toys as well since they are providing children services online through the physical toy directly to the cloud or through an associated application.

---

10 See id.
11 See id.
12 Children’s Online Privacy Protection Act (COPPA) 15 U.S.C §§ 6501–6508 (2013), http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cb905fc4b409&node=16%3A1.0.1.3.36&rgn=div5 [https://perma.cc/HFL4-KZ64].
14 See id. at pt. A, subdiv. 9.
15 Id.
COPPA implicates several regulations on connected toys, including obtaining consent from parents and limitations on collecting, using, and securing children’s data in certain ways. For example, toy manufacturers need to give clear and accessible notice about their privacy policies, must delete children’s data if requested by parents, cannot condition a child’s participation on the collection of children’s personal information, cannot retain children’s personal information for longer than necessary to fulfill the purpose of collecting the data, and must take reasonable steps to release children’s personal information only to third parties who can assure the capability of maintaining the confidentiality, security, and integrity of such information.16

Despite these regulations, there are some nuances that may confuse toy manufacturers with how to protect the data they collect. For example, COPPA covers children’s data that is obtained from a child rather than data about a child,17 meaning that toy manufacturers attempting to comply with COPPA would prefer to treat all the data they collect in blanket form rather than spend the time to figure out what kinds of data is actually obtained from children. This may clash with other types of regulations that may apply to a money transmitter toy like Wiggy such as the Gramm-Leach-Bliley Act, which regulates data associated with financial institutions such as banking and credit card information.

**Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions and to money transmitters if they receive “nonpublic personal information” from an unaffiliated financial institution.18 It is unlikely that Spiral is

---

16 See Children’s Online Privacy Protection Rule (COPPA), 16 C.F.R. § 312 (1998), [http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5](https://perma.cc/ZM86-5LS2).
17 See id. at § 312.2.
18 See Financial Privacy Rule (GLBA), 16 C.F.R. § 313 (2000), [http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&ftpl=/ecfrbrowse/Title16/16cfr313_main_02.tpl](https://perma.cc/HRL2-D44P); FED. TRADE COMM´N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT (July 2002), [https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm](https://perma.cc/Z6QH-F3GJ) (explaining that “Even if your business is not a financial institution that has consumers or customers, the Privacy Rule may limit your use of NPI. Your ability to reuse and re-disclose the information may be
considered a financial institution, let alone a financial institution that has customers. The FTC defines a financial institution as an organization that is significantly engaged in financial activities that might include lending, exchanging, transferring, investing for others, or safeguarding money or securities, providing financial, investment, or economic advisory services, brokering or servicing loans, debt collecting, or providing real estate settlement services.\(^{19}\) The Wiggy Card, though potentially thought of as transferring money from parent to child, does not seem to be done by the toy itself or even the toy manufacturer. Spiral, when explaining the Wiggy Card, implied that it partners with a bank to conduct transfers from a parent’s bank account to a pre-paid debit card meant for children using Wiggy’s application as the platform of the transfer rather than a separate financial institution.\(^{20}\) This seems to be far from a significant engagement.\(^{21}\)

A service like Wiggy Card, however, may certainly be considered a money transmitter that receives nonpublic personal information (NPI) from an unaffiliated financial institution. Under the GLBA, nonpublic information is considered “any information an individual gives you to get a financial product or service,” “any information you get about an individual from a transaction involving your financial product(s) or service(s),” or “any information you get about an individual in connection with providing a financial product or service.”\(^{22}\) This may include names, social security numbers, bank account numbers, and other related information. NPI does not include information that one can reasonably believe is lawfully made public such as federal, state, or local government records publicly available and information that is widely distributed media.\(^{23}\) The caveat here is that when a list is derived from NPI, even if some of the information in the list is not NPI, the list itself is still restricted if you receive NPI from a nonaffiliated financial institution,” namely money transmitters that receive information from a nonaffiliated financial institution).

19 See Fed. Trade Comm’n, supra note 18.
21 See Fed. Trade Comm’n, supra note 18 (stating that the FTC’s “significantly engaged” standard is intended to exclude certain activities that might otherwise fall under the Privacy Rule. Two factors are particularly important in determining whether you are “significantly engaged” in a financial activity. First, is there a formal arrangement? A storeowner or bartender who "runs a tab" for customers is not considered to be significantly engaged in financial activities, but a retailer that offers credit directly to consumers by issuing its own credit card would be covered).
23 See id.
considered NPI. In Wiggy Card’s case, a list of Wiggy Cards distributed to children may be considered NPI if the list contains parents’ names associated with the financial service of transferring funds from a bank account to a child’s Wiggy Card. It is unclear whether a list of just children’s names associated with Wiggy Cards containing no information on the Wiggy Card or the financial information association associated with the Card is considered NPI.

The GLBA restricts NPI reuse and re-disclosure. When it comes to NPI received by nonaffiliated financial institutions, money transmitters may disclose the information to process financial services in a necessary capacity without informing consumers of these processes. If Wiggy uses NPI in a way that is not necessary to deliver a financial service, however, Wiggy can only use NPI from consumers that were informed of these possible uses in a privacy notice given to them by the financial institution and who subsequently did not opt out. Even then, the use of NPI is limited to internal purposes and re-disclosure is limited by the privacy policy of the associated financial institution.

These regulations, when paired with other relevant laws like COPPA, can lead to some confusion for toy manufacturers attempting to deliver a service like the Wiggy Card. This is because financial data may be paired or comingled with children’s data. For example, account numbers are prohibited from being disclosed for marketing purposes, but it is not against COPPA to use children’s personal information for contextual advertising, creating technical difficulties for companies to pull different data lists for different purposes while attempting to comply with different privacy regulations. Because COPPA’s regulations are largely built around parental consent, it also brings in issues of how to properly give transparent and accessible notice to parents to understand how information may be collected, used, and

24 See id.
25 See id. at pt. III.
26 See id. at pt. II.
27 See id.
28 See FED. TRADE COMM’N, supra note 18, at pt. IV.
29 As opposed to behaviorally targeted advertising. For example, a company may use potential personal information such as a child’s age to deliver age appropriate advertisements to six-year-olds versus twelve-year-olds, but may not create profile of a child to target specific advertisements to a certain child based on that child’s unique interests and personal information. See FED. TRADE COMM’N, supra note 18.
transferred. It also highlights issues on how to give parents and children alike control over different types of data, whether financial or children’s data.

**Unfair or Deceptive Acts**

In order to solve for issues relating to notice, consent, and user control, the FTC has some limited enforcement actions based on unfair or deceptive acts.\(^\text{30}\) Based on public statements Wiggy has made about its services, the FTC is able to enforce against services such as the Wiggy Card. Unfair practices are considered acts that cause or are likely to cause substantial injury to consumers, cannot be reasonably avoided by consumers, and are not outweighed by countervailing benefits to consumers or to competition.\(^\text{31}\) Deceptive practices are considered acts where a representation, omission, or practice misleads or is likely to mislead the consumer; a consumer’s interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and the misleading representation, omission, or practice is material.\(^\text{32}\) The FTC usually evaluates deceptive practices when looking at privacy policies.\(^\text{33}\) By not distinguishing between financial and children’s data, companies may find themselves under FTC investigation for deceptive practices as privacy policies may lead users to misunderstand the way their data is being collected, used, and shared if the difference between types of data is not distinguished. Therefore, it is important for companies like Wiggy to publish privacy policies in accessible places and ensure that their data collection, use, and transfer policies are transparent to consumers. This would include describing the differences between financial and children’s data and explain the security and consent implications of both to parents.

In February 2017, one of Spiral’s other connected toys, CloudPets, was identified as having various security and privacy issues. CloudPets was


\(^{32}\) See id.

shown to have kept children’s personal information in an unsecure fashion, allowing the data to be breached.\textsuperscript{34} CloudPets’ privacy policy states that CloudPets takes “reasonable measures to protect personal information in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration, and destruction. For example, we use secure, encrypted communications when transferring all personal information over the web.”\textsuperscript{35} As demonstrated, Spiral’s privacy policies contradict its actual practices and may land CloudPets and possibly other Spiral’s connected toys under FTC investigation and enforcement. As of now, there does not seem to be an accessible privacy policy for Spiral’s Wiggy, leaving Wiggy similarly vulnerable.

\textit{Self-Regulation}

Self-regulation may be a good option for money transmitter toys like Wiggy to ensure they adhere to privacy regulations. Because of the possible clash between current privacy regulations, companies can bring some consistency by taking initiative through implementing best practices already being practiced by big players in the ecosystem. The best practices that toy manufacturers can take include reasonable security, accessible and transparent privacy policies, and allowing consumer control.\textsuperscript{36} For example, money transmitter toys could implement easy to use user interfaces in their accompanying apps that would allow parents to easily unlink bank accounts from connected toys and apps and be certain that such data is not being retained unnecessarily.

Although there are several FTC-approved safe harbor organizations that companies could join in order to state their compliance with COPPA


\textsuperscript{35} Terms and Conditions, Privacy Policy, SPIRAL TOYS, http://spiraltoys.com/products/cloudpets/terms-and-conditions/ (last revised Jan. 15, 2016) [https://perma.cc/9JFB-942C].

\textsuperscript{36} See FUTURE OF PRIVACY F., \textit{supra} note 1, at 12–16.
regulations, toy manufacturers that also provide P2P services may encounter difficulties finding cohesive self-regulation structures specifically made for money transmitter toys. They should look to innovating best practices by looking to financial regulations, while paying attention to the types of information they are collecting from children. Parents, while they can take several steps to educate themselves in how companies collect data, should not have to jump through hoops to understand whether a finance education toy protects their financial data or their children’s personal information.

THE SOCIAL IMPLICATIONS

Connected toys are not only becoming more popular, but they are also expanding the ways in which children are experiencing the physical world. Though connected toys root from virtual worlds, a physical representation of that world can lead to several physiological implications. Toy manufacturers not only should look to current legal implications, but should also look to potential social implications that may inspire future regulations. Several connected toys autonomously develop personalities, whether through artificial intelligence or through a child’s imagination. Children can quickly bond with their toys and adding an element of education to toys may lead children to rely on toys for more than play. Though educational toys are not new, connected toys may create a culture among new generations that change the way that children view the physical world.

Wiggy, for example, provides an incentive for parents to stray away from giving children physical cash, while simultaneously allowing children to

---


see finances as more abstract than a dollar they may hold in their pocket. Though it is unclear how this may change the way children view the value of money or how they learn accounting, social implications are important to take into consideration when developing toys that rely heavily on the internet.

CONCLUSION

In time, connected toys will become a standard birthday gift. Connected toys may start to replace babysitters or act as home teachers. Toys may even become personal accountants for children. In cases where toys may cross over into territories not usually attributed to children, such as finance, toy manufacturers should look to current privacy regulations and aim for best practices in order to build trust and protect consumers. By having descriptive, transparent, and accessible privacy policies and providing reasonable security, toy manufacturers can take the first steps in finding a balance in protecting consumer’s data while also being able to use data to develop and deliver better services to users.
The electricity market is undergoing a transformation. The basic tenet of a centralized production, transmission and distribution system where consumers purchase electricity from a single provider is increasingly developing into a decentralized, multiple provider system centered on renewable energy, in which the customer may produce, consume, and then sell excess electricity capacity like a commodity in an open market, where transactions are transparent, verifiable, and secure. Major drivers of this shift include customer demand for energy independence from the broader electricity grid controlled by utility companies; reduction in energy costs; and the global commitments of influential multinational companies to purchase electricity from renewable energy sources to reduce carbon emissions.

Technology companies have also begun to move into the energy space; Apple’s request to become a wholesale provider of renewable energy throughout the country was recently approved by the Federal Energy Regulatory Commission (“FERC”). Companies like Apple, Google,

---

4 The World’s Most Influential Companies, Committed to 100% Renewable Power, RE100, http://there100.org/re100 (last visited Mar. 3, 2017) [https://perma.cc/69RQ-WHFT]
Amazon\(^6\) and other non-utility enterprises may ultimately become direct competitors to traditional utility companies in the sale of renewable energy based electricity directly to retail customers through blockchain technology. For now, Apple and Google are authorized to sell excess energy capacity in the wholesale energy markets and could do so with blockchain technology. In the future, if either Apple or Google were to provide energy from renewable sources to customers in retail markets under various distributed energy scenarios, a viable blockchain distributed ledger technology would provide the same seamless, secure and transparent accounting of these transactions.

Blockchain technology is potentially the mechanism to transform energy trading in a decentralized electricity market. The blockchain is a shared and trusted distributed ledger technology that permits the recording of any digital asset transaction between parties over a decentralized encrypted network. Initially developed as a mechanism to record financial transactions using the Bitcoin cryptocurrency financial technology or “fintech,” the blockchain technology has generated broad interest in other business sectors,\(^7\) including energy trading.\(^8\) Blockchain technology confirms transactions in real time, and ensures the integrity of transactions through the secured

---


\(^5\) AWS is committed to running our business in the most environmentally friendly way possible, AMAZON, https://aws.amazon.com/about-aws/sustainability/ (last visited Apr. 4, 2017), [https://perma.cc/9544-C3SH] (Announcing Amazon’s expansion of the company’s investments in renewable energy production with the development of a Ohio wind farm and Virginia solar farms creating a total of ten renewable energy projects globally).


exchange of digital currency.\(^9\) Furthermore, the blockchain technology is promoted as beyond the hackers’ nefarious reach.\(^10\)

Siemens announced on Nov. 21, 2016 an agreement with New York startup LO3 Energy to jointly develop microgrid\(^11\) that enable local energy trading through blockchain technology.\(^12\) For example, a provider of electricity from a rooftop solar system would feed excess electricity back into the existing local grid, and receive payments from customers purchasing the renewable energy. The technology being tested stores and validates data that permits direct transactions between energy producers and consumers. In April 2016, successful peer-to-peer (“P2P”) energy transactions occurred in Brooklyn, New York between rooftop solar producers of renewable energy and consumers through the use of LO3 Energy’s blockchain technology over the company’s TransActive Grid.\(^13\)

Various industry analysts have begun to chart the possible implementation of blockchain technology in energy markets. A Navigant Research report concluded that while utility companies are exploring the use of blockchain technology, the immediate benefit of the technology is in P2P energy trading among smaller decentralized distributed energy systems such as microgrids, in which owners of distributed energy resources such as solar and wind production facilities sell energy directly to customers.\(^14\) In a Price

\(^11\) Microgrid definitions, BERKELEY LAB, https://building-microgrid.lbl.gov/microgrid-definitions (last visited Apr. 4, 2017) [http://perma.cc/55N3-KRJ9] (The United States Department of Energy defines a microgrid as “a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode.”).
\(^13\) Id.
Waterhouse study, the company determined that the blockchain technology will support transparent energy supply chain transactions and play a role in energy metering, billing and confirmation of ownership of assets, among other potential benefits.\textsuperscript{15}

The success in deploying blockchain technology in energy trading markets or any other business enterprise will depend upon how the practical applications of the technology develop, and how those applications will be regulated.\textsuperscript{16} Whether the development and use of blockchain technology is driven by open-source agreements, protected by patents and licensing agreements, or a combination of both approaches to deploying the technology is an open question.\textsuperscript{17} Furthermore, whether Bitcoin will become the currency of choice in the energy trading markets, or for any other digital market transaction and how the financial transaction is regulated, is an open question. The absence of a single standard or approach to government regulation of the application of the currency transaction applicable to use of the technology in commercial transactions is emblematic of the regulatory hurdles that must be overcome. Federal regulators have pursued different approaches to regulating Bitcoin. The Commodity Future Trading Commission (“CFTC”) has begun to regulate the trading in cryptographic currencies, such as Bitcoin, as financial derivatives.\textsuperscript{18} The Office of the Comptroller of the Currency (“OCC”) has requested comments on whether the federal government should create special purpose national banks for fintech companies.\textsuperscript{19} The Securities and Exchange Commission (“SEC”) has sought comments on whether transactions using blockchain technology require registration under existing regulations for

\textsuperscript{15} PWC GLOBAL POWER & UTILITIES, supra note 8.
\textsuperscript{17} Olga Kharif, Big Banks are Stocking Up on Blockchain Patents, BLOOMBERG (Dec. 21, 2016, 5:00 AM), https://www.bloomberg.com/news/articles/2016-12-21/who-owns-blockchain-goldman-bofa-amass-patents-for-coming-wars [http://perma.cc/2S7G-NZE8].
transfer agents or clearing agencies. The outcome of these domestic questions regarding the legal and regulatory treatment of block chain distributed ledger technology will impact efforts to create standards to govern the use of the technology in domestic and international trade in goods and services now under consideration. Uniform standards on interoperability, data security, and currency payments are imperative if blockchain technology is to become the electronic distributed ledger technology for goods and services, including energy transactions.

In the private sector, the National Association of Securities Dealers Automated Quotations System (“Nasdaq”) has encouraged the use of blockchain technology. Nasdaq announced on Dec. 30, 2015 that “an issuer was able to use its Nasdaq Linq private blockchain ledger technology to successfully complete and record a private securities transaction - the first of its kind using blockchain technology.” Furthermore, Nasdaq continues to promote blockchain technology as a transformative technology that ensures efficiency, transparency and data security in financial transactions.

On February 28, 2017, a blockchain technology consortium known as the Enterprise Ethereum Alliance (“EEA”) was launched by a diverse group of multinational businesses and software developers, including Accenture, Banco Santander, BlockApps, BNY Mellon, BP, Credit Suisse, Cryptape, ING, Intel, J.P. Morgan, Microsoft, String Labs, Thomson Enterprise. The EEA was created to further the development of a free to use, open source industry standard for blockchain solutions to serve as the foundation for

---


business transactions by ensuring transparency, trust, privacy, and performance in peer-to-peer and multiparty agreements among other applications.25 According to Jeremy Millar, founding board member of EEA, “Ethereum is already one of, if not the, most widely used technologies for developing and deploying enterprise blockchains. Enterprises love the availability of open-source implementations, a single standard, the rapidly growing developer ecosystem, and availability of talent. But enterprises expect resilient secure systems and a robust controls environment. EEA aims to bring these together, both to provide enterprises the forum they need and also to advance Ethereum generally.”26

The response of government regulators to unanswered questions regarding the regulatory treatment of the technology and how best to exploit the use of blockchain distributed ledger technology in the trading of goods and services are expanding. On February 9, 2017, Congressmen Jared Polis (D-Colo.) and David Schweikert (R-AZ) announced the launch of the Congressional Blockchain Caucus.27 The bipartisan caucus is “dedicated to the advancement of sound public policy toward blockchain-based technologies and digital currencies.”28 Congressman Schweikert has replaced former Co-Chair of the Blockchain Caucus Rep. Mick Mulvaney (R-S.C.) who was recently confirmed as President Trump’s Director of the Office of Management and Budget. The importance of harnessing the value of blockchain technology in domestic and international commerce is reflected in the comments of Congressman Schweikert, “Open blockchain networks and distributed ledger technologies are still new, but it’s critical for members of Congress to begin comprehending both their current applications and future use cases” and that “it is critically important the United States remain competitive regarding emerging technologies, and distributed ledger technology is the open, secure, efficient technology backbone we’ve been looking for.”29 Recently, the United States Department of Energy (“DOE”) requested proposals on the use of blockchain distributed ledger technology to

26 Id.
28 Id.
29 Id.
ensure the security of energy transactions. The request for proposals states that “DOE is currently investigating novel approaches to leverage and explore blockchain technology, initially developed within the financial sector, for the realization of robust fossil energy-based systems” and that “proposals are sought to develop novel concepts for energy systems that rely on blockchain technology to assure robust systems that are less susceptible to cyber-attack.”

With the rise of fintech, a global effort is underway to create universal standards for seamless, transparent and secured electronic commercial transactions based upon the blockchain distributed ledger technology. The International Organization for Standardization (“ISO”), an independent, non-governmental international organization that develops standards in response to global challenges, has established a technical committee, ISO/TC 307, to develop voluntary standards for the use of blockchain distributed ledger technology in national and international trade in goods and services.

Based upon the proposal of Standards Australia to the ISO in 2016, the mandate of the technical committee is development of global “standardization of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications, and

---

31 Id.
The work of ISO/TC 307, under the leadership of Standards Australia, commenced in Sydney, Australia on April 3-5, 2017. The United States, Canada, China, Germany, Japan and Russia are among seventeen participating ISO members while Argentina, Iran, Israel, and South Africa are among seventeen observing ISO members.

The scope of economic, legal, and regulatory parameters for the use of blockchain distributed ledger technology in public and private exchanges is evolving and may take decades to be fully realized. As this occurs, the technology will continue the transformation of electricity market energy supply transactions. Navigant has described this evolution as the emergence of a decentralized energy marketplace, an “energy cloud,” in which blockchain technology can serve as a secure digital ledger for energy transactions. The nexus between private sector innovation and limited government regulations, however, will determine whether blockchain technology transforms the global economy in goods and services, including distributed energy transactions. The results of the ISO/TC 307 will greatly impact the evolution of blockchain distributed ledger technology as a viable records keeping component in national and internal supply chain management of energy transactions.
President Donald Trump’s first hundred days in office were characterized by a whirlwind of executive actions and attempts to fulfill campaign promises. Yet the technology sector’s primary concern has been Trump’s lack of regulatory action and unknown policies. How this administration will impact emerging technologies like fintech is still relatively uncertain, but an analysis of actions that indirectly affect fintech, the known backgrounds of confirmed and nominated appointees, and influential outside sources promoting fintech agendas may provide insight.

On February 3, 2017, President Trump attempted to roll back parts of the Dodd-Frank Act,¹ the 2010 bill that regulates large swathes of the financial sector.² Though the executive order doesn’t expressly mention the act, Press Secretary Sean Spicer made the intentions of the order clear in a press briefing given the same day the order was signed.³ The order calls for the review of all financial regulations for compliance with six “Core Principles,” which include preventing taxpayer-funded bailouts and enabling American firms to be competitive with foreign companies as well as domestic and foreign markets.⁴

Thought to be a defining part of President Obama’s legacy, the Dodd-Frank Act was a legislative reaction in 2010 to the financial crisis of 2008. In the technology sector, entrepreneurs reacted to the crisis in a different way: by creating programs and algorithms to bring increased transparency and automation to much of the traditional Wall Street practice. Companies like Betterment and Wealthfront put consumers back in the pilot seat of their own finances, curtailing potential conflicts of interest or temptations to breach fiduciary duties.

However, President Trump also issued a memo directing the Department of Labor to consider rescinding its rule imposing a fiduciary duty on financial advisors for retirement accounts. Fintech companies originally responded to this rule by creating robo-advisors, as it was believed that the compliance costs for money managers would disincentivize retaining smaller clients. The White House’s orders could remove this incentive and stifle fintech growth in this area.

In this regard, President Trump’s stance on reduced federal regulation runs counter to leaders of fintech, many of whom have advocated for fintech-specific regulations as a means of spurring growth via more coherent

---


9 Betterment’s vertical integration structure combined traditionally separate steps like financial advice and trading, meaning consumer have access to a virtual one-stop-shop style investment vehicle. Similarly, Wealthfront has automated the process of investing and given consumers access to their portfolio via mobile interfaces that can be accessed at any time.


11 Id.
compliance programs.12 The President has also suggested the abolition of one of the most recently established executive agencies, the Consumer Finance Protection Bureau.13 The CFPB, a pro-fintech agency, was created by Dodd-Frank14 with a single goal: “watching out for American consumers in the market for consumer financial products and services.”15

The CFPB has supported the growth of fintech companies, encouraging what it calls “consumer-friendly innovation.”16 A full repeal of Dodd-Frank could spell the end of the CFPB, which may lead to a host of consumer finance issues related to fintech.17 According to Nilesh Vaidya, senior vice president and head banking and capital markets for Capgemini Financial Services, the end of the CFPB could cause “a rise in mortgages being written which are not really affordable to consumers . . . the likelihood for delinquencies would increase.”18

The CFPB has also shut down fintech companies that do not promote consumer welfare, which are companies that are acting essentially as new age payday lenders.19 Continuing to balance support for and enforcement of fintech requires skilled and knowledgeable agencies, like those found at CFPB, but even if Dodd-Franks stays, legislation introduced in both the House and Senate on February 14, 2017 call for the repeal of the agency.20

13 Id.
18 Id.
President Trump will likely face serious opposition from Democrats and their supporters on these actions affecting fintech, so instead of focusing on these moves directly, scrutinizing Trump’s appointees offers another approach to understanding this administration’s impact on fintech.

Trump is expected to name former Texas Congressman Randy Neugebauer to replace the director of the CFPB. Representative Neugebauer has been a vocal critic of the CFPB. He has called for fewer regulations and attempted to replace the director position with a multi-member commission, which would limit the organization’s ability to independently draft regulations.

The fight over the head of the CFPB could last through next year, as current Director Richard Cordray’s term extends to 2018. Though the D.C. Court of Appeals ruled that the CFPB head can be removed at will rather than the for-cause standard typically used at independent agencies—which could also seriously curtail regulation in opposition to White House policies—that decision was vacated and an en banc hearing will be heard on May 24, 2017.

Given that President Trump has already fired officials who disagree with him and attempted to wipe clean Obama appointments at DOJ, Director


23 Id.


25 “With the for-cause provision severed, the President now will have the power to remove the Director at will, and to supervise and direct the Director.” PHH Corp. v. Consumer Fin. Prot. Bureau, 839 F.3d 1, 8 (D.C. Cir. 2016), reh’g en banc granted, order vacated (Feb. 16, 2017).

26 Order Granting Rehearing En Banc, 839 F.3d 1, 8 (D.C. Cir. 2016).

Cordray may be dependent on legal relief to retain his position through his appointed term.

President Trump’s Secretary of Commerce Wilbur Ross may also shed light on how this administration plans to deal with fintech and traditional banking institutions.\(^2^9\) Ross, an investor and banker, targeted failing banks during the financial crisis of the 2000s.\(^3^0\) In 2011, at the height of the European debt crisis, Ross was part of a group of investors that acquired 35\% of the Bank of Ireland.\(^3^1\) While traditional banks themselves are seeking ways to improve services through many of the same processes employed by independent fintech companies—such as mobile interactions—many fintech companies view themselves as disruptors of the industry.\(^3^2\) There is real tension between these old titans and the newer, scrappier service providers that Commerce is expected to mediate.\(^3^3\) Though Ross sold his interests in the Bank of Ireland in 2014, his former involvement may create conflicts of interest that influence his actions at Commerce.\(^3^4\)

Steven T. Mnuchin, President Trump’s Treasury Secretary, is yet another veteran banker and a former Goldman Sachs employee.\(^3^5\) Mnuchin put himself at odds with many popular views on automation and technology in a March interview when he said artificial intelligence is “50-100 years away”


\(^{3^0}\) Id.

\(^{3^1}\) Id.


\(^{3^3}\) Id.


\(^{3^5}\) Id.

\(^{3^6}\) Id.
from supplanting human jobs.\textsuperscript{37} That position was criticized by several new outlets, all of which agree that AI is currently impacting American job loss\textsuperscript{38}—one paper even pointed that 47 percent of the total U.S. employment could be automated in the next two decades. Secretary Mnuchin’s comments can impact tech stock valuations,\textsuperscript{39} meaning assertions like the one on AI could affect fintech companies’ ability to continue to find funding or support.

In his new role, Secretary Mnuchin will assist President Trump in matters ranging from financial regulation to revamping the tax code. However, the two men are sending mixed messages on tax reform: Mnuchin has stated that “there would be no absolute tax cut for the upper class” in stark contrast to President Trump’s adopted position.\textsuperscript{40}

President Trump’s potential tax plans have fintech companies feeling skittish. Much of the White House’s current plan regarding tax reform focuses on corporate taxation without addressing individual tax concerns.\textsuperscript{41} While this will likely benefit the larger, established corporations, many emerging fintech start-ups are structured for pass-through taxation, meaning the individual owners shoulder the gains or losses rather than the company itself.\textsuperscript{42} Without reforming individual tax regulations, these start-ups may find themselves at an extreme disadvantage when competing with traditional institutions.\textsuperscript{43} Nevertheless, some think tanks argue that even small businesses will benefit from corporate tax reform, painting start-ups as holding up beneficial changes.


\textsuperscript{39} Summers, supra note 38.


\textsuperscript{42} Id.

\textsuperscript{43} Id.
in exchange for special treatment. As this tension builds, new and fragile technology sectors are watching every move closely.\textsuperscript{44}

If President Trump fails to take a concrete position on fintech, state governments may enter the regulatory sphere. In New York state, where fintech has been growing rapidly and seems to be the current home of the sector,\textsuperscript{45} top financial regulator Maria Vullo has demanded that the federal Office of the Comptroller of the Currency not interfere with the state’s plan to regulate fintech and that federal oversight would allow circumvention of state consumer protection laws, as well as potentially creating another “too big to fail” class of institutions.\textsuperscript{46}

This action by the OCC is actually a holdover from the Obama White House, when the OCC announced desires to grant fintech companies national banking licenses.\textsuperscript{47} A federal charter could allow disruptive companies to more easily anticipate regulations and implement uniform policies compliant with federal oversight, as opposed to a patchwork of state and local legislatures.\textsuperscript{48}

Seemingly ignoring New York’s position, in March the OCC rolled out its licensing manual for fintech companies to apply for a charter.\textsuperscript{49}

Reacting to the White House’s ambiguous stance on fintech, private organizations are currently attempting to give suggestions on how the White House can deal with fintech to the benefit of all.

Tech giants Google, Apple, Amazon, PayPal and others formed Financial Innovation Now and sent a letter to President Trump laying out a series of recommendations, including creating and appointing a Treasury Undersecretary for Technology who would work with other federal financial

\begin{thebibliography}{9}
\bibitem{44} Id.
\bibitem{46} Id.
\end{thebibliography}
regulators and the banking sector to foster fintech.\textsuperscript{50} Another group, Consumer Financial Data Rights Group, acting as a self-styled trade organization on behalf of fintech companies, strives to improve consumer access to financial data.\textsuperscript{51}

The National Economic Council released a report in early January 2017 titled “A Framework for FinTech.”\textsuperscript{52} The report, which could be considered a final piece of advice on fintech from President Obama, lays out suggested policy objectives for financial services, from positive innovation to national competiveness.\textsuperscript{53} In addition, the report includes ten statements of principals, designed to provide a framework to contribute to the policy objectives.

However, Trump has tapped former Goldman Sachs president Gary Cohn as the new head of the NEC. The senior economic advisor’s comments seem indicative of a deregulatory stance,\textsuperscript{54} in line with President Trump’s supposed positions. Mr. Cohn has been highly influential at the White House since the beginning of the new administration.\textsuperscript{55} President Trump has even included Cohn as a founding member of the newly minted Office of American Innovation.\textsuperscript{56} The new office aims to bring private sector efficiencies into government agencies.\textsuperscript{57}

\textsuperscript{50} Rob Haralson, \textit{FIN calls on President-elect Trump to promote innovation in financial services, appoint senior financial technology leader}, FIN. INNOVATION NOW (Nov. 30, 2016), https://financialinnovationnow.org/2016/11/30/fi-trump-transition-letter/ [https://perma.cc/Y5QE-8KCQ].
\textsuperscript{52} NAT’L ECON. COUNCIL, A FRAMEWORK FOR FINTECH (Jan. 2017).
\textsuperscript{53} Id.
\textsuperscript{57} Id.
Cohn’s clout may have taken a hit during the recent failure to pass the Republican-backed repeal of the Affordable Care Act. Cohn was at the front of the charge to push the Congressional bill by bringing his economic expertise into the conversation through meetings with Republican leaders. When the bill failed to pass, sources in the know claim Cohn shouldered a portion of the blame. How Cohn’s NEC could affect fintech has become even harder to predict.

The whirlwind of information and actions facing fintech growth is creating a situation fraught with uncertainty and competition for control. Despite independent action from federal regulatory agencies, state organization, or private tech groups, Trump’s administration could change the rules of the game overnight with certain proposed or potentially proposed actions. Fintech companies are trying to get ahead of the chaos, but are watching the White House closely to gauge the winds. If 2016 was a year of fintech expansion, 2017 and beyond could see a slow-down unless clear guidance emerges.


American consumers using peer-to-peer ("P2P") payment services, such as Venmo and PayPal, could unwittingly violate U.S. foreign policy—at least if their transactions involve parties on the Treasury Department’s foreign sanction list. The Office of Foreign Assets Control ("OFAC"), a division of the Treasury Department, enforces economic sanctions based on U.S. national interests, and prohibits Americans from doing business with foreign actors that threaten “the national security, foreign policy or economy of the United States.” While it is unsurprising that Americans are barred from transacting with entities under OFAC sanctions, consumers might be surprised by how easily they can fall under investigation, especially for seemingly innocuous transactions.

In one recent incident, a United States consumer found himself caught between an otherwise unremarkable Cuban sandwich purchase and an investigation for possible OFAC violations—simply for typing a certain keyword ("Cuban") while making a Venmo payment. In a similar episode, a PayPal user’s transaction came under investigation after the consumer paid another American to review a book entitled Castro’s Cuba. PayPal halted the transaction, and its compliance department sent a boilerplate email to the customer, detailing the reason for the block:

“PayPal is committed to complying with and meeting its global regulatory obligations. One obligation is to ensure that our customers,
merchants, and partners are also in compliance with applicable laws and regulations, including those set forth by OFAC, in their use of PayPal.\(^4\)

PayPal’s message went on to ask the consumer for an explanation as to the “goods and services involved in the transaction,” further requesting the customer email its compliance department and visit the PayPal Resolution Center to explain the following text from the transaction message: “Hi Ben - Your Castro's Cuba review is up! Thanks so much! Carla.”\(^5\)

These regulatory compliance efforts illustrate a problematic trend for P2P payment start-ups; fintech companies have struggled to abide by federal regulations in P2P transaction services, (perhaps due to the rapid nature of P2P transactions,\(^6\) and the substantial technical burden in vetting the billions of dollars in such transactions for regulatory compliance),\(^7\) resulting in significant monetary judgments against the companies.\(^8\) Whereas a decade ago, transactions with foreign nationals might have been made via traditional wire transfers, these transactions can now happen much more rapidly, circumventing those larger intermediaries and passing through applications such as Venmo in a fraction of the time.\(^9\) Traditional banking institutions, however, are generally more experienced in regulatory compliance than newcomer, disruptive P2P services—and with the comparatively pedantic nature of traditional services, questionable money transfers can be easier to spot and interdict before they are completed.\(^10\)

Electronic P2P payments—generally defined as informal, digital money transfers between two persons—have become a prominent feature of the sharing economy. According to the Federal Reserve, the number of P2P payments increased from $146.6 million to $205.3 million from 2009-2012,

---


\(^5\) Id.


\(^8\) See, e.g., infra, note 16.

\(^9\) See generally Aliya Ram, *Peer-to-peer forex platforms come of age*, FIN. TIMES (Apr. 1, 2015), https://www.ft.com/content/60aa6e8a-8798-11e4-bc7c-00144feabdc0 [https://perma.cc/L9PC-A3G7].

\(^10\) See generally Lohr, supra note 6.
The markets seem to have grown logarithmically since then: in 2015, Venmo alone processed more than $7.5 billion in P2P payments (with an annual growth of 174%), and one Business Insider report estimates that total U.S. P2P transactions volume could reach $86 billion by 2018.¹²

One reason for the P2P economy’s rapid growth is the lower transaction costs associated with services such as Venmo, PayPal, or Apple Pay.¹³ Not only can consumers avoid financial burdens such as credit card fees, ATM withdrawal charges, or the nominal cost of a new checkbook, texting the payment to a friend is just easier than signing a receipt or going to withdraw cash. As one commentator put it, these services “make transferring money faster, less expensive, and more precise.”¹⁴ Still, with a rapidly expanding industry, and even faster financial transactions, service providers are hard-pressed to ensure that transactions remain in compliance with regulatory schemes. In addition, the regulatory compliance will impact the profitability of P2P service providers, increasing the transaction costs both financially and socially.¹⁵

PayPal learned this lesson the hard way in 2015; the P2P giant settled a case brought by the Treasury Department for $7.7 million, apparently for 486 unintentional violations of U.S. economic OFAC sanctions.¹⁶ According to OFAC, for several years until 2013, PayPal’s internal compliance mechanisms were either non-existent, or insufficient to “identify, interdict, and prevent” transactions that could violate OFAC sanctions.¹⁷ Pursuant to the settlement order, PayPal enhanced its compliance processes—presumably by including search algorithms to target keywords, or combinations of keywords,

¹³ Id.
¹⁴ Id.
¹⁵ See, e.g., infra, note 16.
¹⁷ Id.
to meet OFAC’s requirements to “identify, interdict, and prevent” potential OFAC sanctions.  

OFAC has long regulated traditional financial institutions to ensure compliance with U.S. national interests, but for newcomer P2P start-ups, the PayPal case illustrates that they, too, are within the ambit of OFAC regulation. OFAC’s stated mission is to administer and enforce “economic and trade sanctions based on U.S. foreign policy and national security goals.” Under the authority of federal legislation and Presidential national emergency powers, OFAC can unilaterally block transactions and freeze assets within United States jurisdiction if parties to the transaction fall within any group of targeted actors. Specifically, OFAC, compiles a list of “individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries.” It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific, known as “Specially Designated Nationals” or “SDNs.” Their assets are blocked and U.S. persons are generally prohibited from dealing with them. To this end, Americans suspected of entering into any such prohibited transactions will similarly be blocked from doing so.

Unfortunately for PayPal and its P2P cohort, compliance with these OFAC regulations is perhaps more onerous than they initially considered—and the best way to comply might very well be a massive data keyword dragnet, such as one that catches transactions including “Cuba” or “Syria” in the message thread.

While American consumers might find the extra regulatory compliance measures a bit ridiculous, burdening a few customers could be a small price for PayPal to pay, especially when the alternative price tag is closer to $8 million. Still, it remains to be seen whether there are better

22 Id.
23 See, e.g., Williams, supra note 18.
24 See, e.g., Merchant, supra note 16.
methods for companies to comply with OFAC sanctions, or whether OFAC itself needs to adapt to a brave, new, financially-innovative world. The federal government should weigh the costs and benefits of existing U.S. foreign policy measures against the costs and benefits of stimulating U.S. fintech growth in P2P payments. Adapting regulations or penalties for fintech companies, for example, could increase the companies’ profitability and competitiveness, without destroying foreign policy. Unless OFAC adopts new policies, however, American companies and citizens can expect the same enforcement measures, stiff penalties, and keyword dragnets to continue.
I. INTRODUCTION

The global insurance industry has approximately $15 trillion in assets under management and $5 trillion in annual premium revenues.¹ $1.2 trillion of the annual premium revenues come from the United States alone.² Despite the financial appeal to investors, this industry has seen fewer technological improvements than any other financial services sector.³ Insurance providers have among the lowest customer satisfaction and loyalty ratings of any industry, suggesting that a technological overhaul of the industry could bring welcome improvements.⁴ Fewer than half of people in the United States aged twenty-five to sixty-four have life insurance coverage and more than half of all homes in the United States are underinsured.⁵ This leaves the insurance market substantial room to grow and adapt if the market addresses needed

³ See Cusano, supra note 1.
⁴ Dickinson, supra note 2.
⁵ Id.
improvements to technology. Technology innovators have noticed this glaring need; in 2014, investors poured $2.6 billion into “insurtech,” over ten percent of all fintech investment that year and over a three-fold increase from the previous year.\(^6\) With the arrival of the insurtech revolution, the industry will likely continue to innovate and transform by adding efficiencies and growing the customer base.\(^7\)

**II. DISCUSSION**

Insurance is built on data. Insurance companies must determine liability and assess how they can afford to cover individual consumers.\(^8\) Insurtech is improving the ways in which data is gathered and processed. This essay will examine how these new capabilities allow insurance companies to improve their existing consumer offerings, alleviate their regulatory burdens, and create new products that better conform to modern society and behavior.

**A. Insurance: How it Works**

Insurance is a paid safeguard against loss.\(^9\) Payment to the insurer, the premium, is determined through underwriting, a systematic process of measuring risks and assigning dollar amounts to them.\(^10\) A premium varies based on how likely an individual is to experience adverse effects as compared to the average insured party.\(^11\) Policies are pooled with other policyholders’ premiums so those in the risk pool subsidize one another.\(^12\) Money not spent on payouts, reinsurance,\(^13\) or operating costs of the company is kept as profit.\(^14\) Because inaccurate assessments might require higher-than-expected payout, the insurance industry’s profitability depends primarily on

---

\(^7\) Id.
\(^9\) Id.
\(^10\) Id.
\(^11\) Id.
\(^12\) Id.
accurate underwriting. In traditional underwriting methods, underwriters assess historical data to consider the likelihood that a particular event might occur again. An ideal underwriting process consists of calculating variables for the specific risk type and covered individual to discern a premium that both entices the buyer and generates enough revenue to cover possible adverse events and create profit. In such an idealized process, the underwriter considers every factor that informs risk and remains entirely objective and unbiased. Perfect underwriting rarely exists in reality. Insurers sacrifice comprehensiveness for speed and cost. Underwriters often lack sufficient data or risk analysis techniques that reflect actual probabilities. Improving and underwriting data analysis represents a huge step forward for accurately calculating risk, to the benefit of the insurer and insured.

B. Improving Underwriting and Data Analysis

Ninety percent of the world’s stored data was created in the past two years, much of this highly personal. The Internet of Things has spread data sensors and transmitters throughout our environment. These sensors identify changes or occurrences around them and send this data to cloud storage systems. Wearable devices and smartphones collect information on physical activity, heart rate, geolocation, and habits. Telematics boxes in cars gauge how safe drivers are. Sensors in buildings determine air quality, while those on the street track traffic patterns and weather conditions. Individuals post their interests and state of mind on social media. Insurers use this new wealth of data to underwrite more effectively, employing several techniques including (1) machine learning, (2) risk mitigation, (3) personalization, (4) continuous underwriting, and (5) fraud detection.
1. **Machine Learning**

Machine learning systems are a form of artificial intelligence that creating analytical models by adapting to the massive amounts of data they analyze with limited human intervention.\(^{22}\) When applied to insurance, machine learning identifies norms of human behavior and finds risk-correlating patterns.\(^{23}\) Previously, only humans could conduct pattern recognition. A human underwriter would identify an issue and then find the degree to which it correlated to the underlying risk. For instance, a calculable percent of the time, working in an environment with asbestos leads to death before the average lifespan of otherwise demographically similar individuals. Machine learning automates this process so that a human does not have to look for known risks or identify trends within the data, and will not misdiagnose degree of risk through bias. Machine learning can recognize patterns that human underwriters never thought to investigate, or those that correlate with risk so subtly that they were not previously identified.\(^{24}\) Automating the underwriting process also makes it faster.\(^{25}\) Finding and pinpointing these additional degrees of risk maximizes the calculation’s accuracy. Machine learning has the potential to revolutionize a process built on human’s limited quantitative and pattern recognition capabilities.

2. **Risk Mitigation**

The growing trove of personal data and corresponding analytics also allows insurance companies to limit major risks before they occur. Oscar, a new health insurer that integrates technology throughout its business, encourages its clients to wear connected devices and share collected data with the company.\(^{26}\) Oscar provides discounts for customers who are proactive about their health, which can be demonstrated by high levels of activity on


\(^{23}\) Rubenacker, *supra* note 20.

\(^{24}\) *See id.* (For example, this could find previously unconsidered traits that make a driver more likely to crash.).

\(^{25}\) *Id.*

their wearable device. On the other hand, wearable health monitors can also identify warning signs of adverse health, altering insurers of potential issues ahead of time. Other sensors identify problems as they happen, long before the insured party notices them. For example, a sensor in a shipping crate can alert the insurance company that a claim will be filed and the insured company should take steps to mitigate supply chain disruptions that the insurance company may otherwise have to cover.

3. Personalization

Among the more revolutionary and attractive innovations from a consumer standpoint is the industry’s new, technology-driven policy personalization capability. In a traditional “risk-pooling” underwriting system, insured individuals answer questions or undergo exams so the underwriter can determine their risk relative to their peers. The process produces an approximate risk profile for each individual. Insurers then group individuals into risk pools, which leads to the mitigation of miscalculations by collectively balancing out inaccuracies. The more a person’s risk profile reflects the actual odds that they will experience an adverse event, the less their policy needs a risk’s pool’s corrective effects. This in turn leads to smaller risk pools. Data from the Internet of Things now produces a more accurate risk profile for individuals, making risk pools unnecessary.

Wearables, smart phones, other sensors, and social media profiles monitor specific and individualized information based on metrics such as activity levels. They also provide more complex calculations such as behavioral trends and interests that differ from an average person’s. Insurers can use this data to charge individuals more accurately, reducing the need for any given insured individual to be subsidized by another.

28 Rubenacker, supra note 20.
30 Id.
31 See id.
32 Id.
34 Id.
Personalized insurance plans also create corresponding harms to customers. Historically, individuals with greater risks face challenges obtaining insurance, a concern compounded by the use of personalized data. Those with high risk factors that normally would balance out as part of a risk pool may instead lose their subsidy and have to pay higher premiums. In extreme cases this may make groups of “uninsurables,” people with risks so great that their premiums become exorbitant. While certain risk-carrying variables may be reversible, such as unsafe driving behavior, others, like living in an impoverished area with bad air quality or having a previously unknown genetic predisposition to a disease, are difficult or impossible to change. Unfortunately, these factors may correspond both with the greatest need for insurance and an inability to pay. Customers who refuse to generate and share data for insurers create an additional complication. Insurers, and companies generally, resolve imprecise pricing data by shifting risk to the consumer, and are almost certain to do the same for customers that limit an insurer’s access to their personal data in the form of higher prices.

4. Continuous Underwriting

The Internet of Things creates a consistent stream of data. Insurers can see information that reflects a client’s health, driving speed, or home security in real time. Previously, insurers only received this information when a claim was filed or a policy renewed, and even then this information could often be imprecise or even fraudulent. Continuous data collection is useful in multiple ways. For example, insurers can create and compare information case studies. By looking at various factors leading up to a claim, including those that the insured did not see as pertinent, insurers can identify new risk factors and identify potential adverse events before they occur. Moreover, rather than waiting for renewal, insurers can revise contracts as risks factors appear and disappear so that pricing remains accurate. Technologies, in addition to those that gather and analyze risk, alleviate practical concerns and make continuous underwriting possible. For example, blockchain technology embedded in virtually tamper-proof smart contracts enables a rapid back and

---

35 Thomson, supra note 29.
36 Id.
37 Id.
38 Rubenacker, supra note 20.
39 Id.
Rather than regularly meeting with clients to review and sign contracts, smart contracts are written in embedded code which can automatically change according to external considerations, such as changes in risk profiles or market forces. These smart contracts allow all parties to see changes in real time, share identical and up-to-date versions, and sign automatically.

5. Fraud Detection

Insurers are also using this new wealth of data and analytical capability to detect fraud. Weather sensors on streets and in cars can show whether a crash occurred because of traction failure or negligence. Geolocation on a smart phone can determine whether a home owner was present during, and possibly responsible for, a house fire. Social media usage may suggest financial distress as a motive for fraud. Natural language processing programs determine if an insurance claimant’s speech patterns, generally keywords that rarely occur together in truthful expression, indicate lying. In practice, many of these fraud markers are bundled with historical data to create comprehensive fraud-detection models. Improving fraud detection could be as vital to the industry as improved underwriting. Fraud accounts for almost forty percent of all money paid out by insurers, and fraudulent claims lead to losses for insurers that are largely shifted to consumers who pay a higher price. Accordingly, eliminating fraud benefits both insurers and the insured.

C. Regulating New Industry Entrants

Increased data breadth, frequency, analysis, and specificity, and the streamlined traditional insurance functions that they improve, enable insurers
to offer new products. A primary reason it has taken a data-driven revolution for the insurance industry to see transformative development is that complex and expensive regulatory barriers exist.\textsuperscript{48} In the United States, the federal government plays only a small role in the insurance regulatory system. Individual states issue most insurance regulations.\textsuperscript{49} New entrants to the market have been rare because creating an insurer with nationwide coverage requires approval from fifty-one different regulators to begin operations. Ongoing compliance presents a significantly more time-consuming, and labor as well as cash-intensive, task for a startup than working with a single federal body. No other financial industry contends with such a disparate regulatory system.\textsuperscript{50}

Capitalization requirements are common across insurance regulatory systems in the United States.\textsuperscript{51} The need to have a large and unencumbered cash supply is a significant barrier to new entrants.\textsuperscript{52} Insurers use trends within the tech start-up world to satisfy these obligations. Some start-ups, including Oscar, have capitalized through venture funding, treating this requirement as any other operation and growth cost for private investors to provide in exchange for an ownership stake.\textsuperscript{53} Another capitalization method is peer–to-peer (P2P) lending in which clients of the company double as investors and capitalize their peer investors’ policies. If claims, and associated fees, filed on the policies for which an investor provides capitalization do not exceed the capitalization amount, investors receive returns.\textsuperscript{54} P2P insurance capitalization schemes have successfully fulfilled regulatory requirements in Germany, but are largely untested in the United States.\textsuperscript{55}

\begin{itemize}
  \item \textsuperscript{48} Dickinson, supra note 2.
  \item \textsuperscript{49} Martin F. Grace & Robert W. Klein, \textit{The Future of Insurance Regulation in the United States}, BROOKINGS INST. PRESS (2009), http://www.jstor.org/stable/10.7864/j.ctt1262wz.4 [http://perma.cc/63AL-DLNB] (explaining that there has been some movement in the past twenty years to shift regulation to the federal level. Despite some progress such as the Gramm-Leach-Bliley Act, which allows financial holding companies to own insurance providers along with banks, regulation is still overwhelmingly concentrated at the state level.).
  \item \textsuperscript{50} Id.
  \item \textsuperscript{51} Dickinson, supra note 2.
  \item \textsuperscript{52} Id.
  \item \textsuperscript{53} Id.
  \item \textsuperscript{54} Guy Chazan, \textit{Tim Kunde’s Peer-to-Peer Approach to Insurance}, FIN. TIMES (Sept. 7, 2016), https://www.ft.com/content/9f2de95e-49e6-11e6-8d68-72e9211e86ab [http://perma.cc/5HE3-XTZM].
  \item \textsuperscript{55} Dickinson, supra note 2.
\end{itemize}
Other start-up “insurers” avoid regulatory strictures entirely by performing a subset of traditional insurance competencies. Rather than act as a full-fledged insurer, they occupy a portion of the vertically integrated insurance chain and can only create an insurance product available to the consumer by partnering with other companies that have sufficient capitalization, generally large, existing insurers. This allows innovative data collectors, analyzers, and consumer facing platforms to symbiotically partner with companies that have the legal and financial infrastructure to create policies and pay claims. Often these companies are platforms with which users interface to purchase specialized contracts that are formally underwritten and held by more comprehensive insurers. Though companies that satisfy only a portion of needed insurance capabilities forgo the potential revenues of operating a vertically integrated business, they still gain entry to the prohibitive industry. Existing insurers that previously held a monopoly over the industry face a more complex cost benefit calculation. They sacrifice a share of their profits for more efficient underwriting and improved user-facing products. However, they risk losing name recognition and brand loyalty by allowing partner companies to exclusively interface with consumers. Insurers that contract with startups to interface with clients risk losing customer loyalty to their more public, undercapitalized partners. Nonetheless, these deals are seen as vital to both established insurer and modular and are becoming increasingly common. Recent trends in the banking industry, where such agreements are now standard practice, could provide a model for the future of insurance. Large banks have launched open platforms and application programming interfaces through which start-ups can develop products that seamlessly integrate into a large bank’s operations. The programs increase innovation and solidify partnerships by creating reliance on the bank or banks’ proprietary programming system.

---

56 Ralph, supra note 17.
57 Id.
58 Oliver Ralph, Ten Fintech Start-Ups that Are Causing a Stir in Insurance, FIN. TIMES (Oct. 2, 2016), https://www.ft.com/content/db833e5a-6eb1-11e6-a0c9-1365ce54b926 [http://perma.cc/AP24-MBN6].
60 Id.
D. New Insurance Products

Specialization within the distribution chain means that many new industry entrants allow insurers to reach untapped markets. One way they do this is by developing microinsurance. Where traditional insurance is comprehensive, microinsurance is based on transactional consumption, covering more particular property and behaviors for short periods of time. Microinsurance offerings are better suited to the sharing economy, particularly participants in the economy that can afford to pay insurance premiums but find that available coverage does not fit their lifestyle. New offerings include mile-by-mile or hour-by-hour auto insurance for borrowed or rented vehicles, and property insurance for individual items. New insurance models often do not come to fruition until other tech start-ups create a need. For instance, Slice did not launch its insurance for users of home-sharing services until AirBnB developed and popularized home-sharing. None of these insurance products would be possible without partners that provide capital, infrastructure, and the advanced technologies already discussed. On-demand, particularized insurance requires constant data input, instant risk pricing, and smart contracts that can be signed from a smart phone as a customer gets into a borrowed car.

Insurtech companies incorporate technologies other than those closely related to underwriting to further improve their specialized offerings. These companies provide accessible user interfaces so consumers can purchase on-demand coverage easily. One new vertically integrated property insurance company, Lemonade, enhances its in-house underwriting and capitalization capabilities with user-friendly technology. Lemonade registers consumers

\[\text{Dickinson, supra note 2.}\]
\[\text{Insurtech in 2017, supra note 59; Ralph, supra note 58; Bernard Marr, The Sharing Economy - What It Is, Examples, And How Big Data, Platforms And Algorithms Fuel It, FORBES (Oct. 21, 2016), https://www.forbes.com/sites/bernardmarr/2016/10/21/the-sharing-economy-what-it-is-examples-and-how-big-data-platforms-and-algorithms-fuel/31eaf4097c5a [https://perma.cc/BJN7-GH7U] (explaining that the sharing economy is based on limited ownership of property, real property, and funds by an individual, supplemented by extensive lending of these goods amongst groups of individuals).}\]
\[\text{Ralph, supra note 58; Ralph, supra note 17.}\]
\[\text{Insurtech in 2017, supra note 59.}\]
\[\text{Ralph, supra note 58; Ralph, supra note 17.}\]
with two different chat bots, a male and a female, that function similarly to Apple’s Siri.67 The process takes as little as ninety seconds and requires no human-to-human communication.68 Lemonade’s particular approach has attracted many customers that were previously uninsured.69 Data suggests that ease of enrollment has contributed to this growth.70 Twenty-five percent of people who price a Lemonade policy go on to buy one, an abnormally high number in the insurance industry.71 Companies offer new functionality in other forms. For example, other property insurance companies are experimenting with damage assessment drones.72 In addition, Oscar allows its policy-holders to receive a consultation from a doctor within ten minutes of making a request via their app.73

Recent industry shakeups have brought more than technological change. Lemonade’s efficient underwriting process allows it to use a non-traditional premium structure. Consumers pay a certain premium which includes a fixed fee kept by the company.74 The rest is used to pay claims. Anything leftover is then donated to a charity that the policy holder selects.75 Because improved risk underwriting allows for more precise return and profit projections, Lemonade is able to structure its business to align the interests of the insurer and the insured.76 Lemonade is not incentivized to deny claims and its customers are less likely to file fraudulent claims in a more trusting environment.77

[http://perma.cc/8M62-2W68] (explaining that Lemonade is currently only available in New York, but is in the process of registering nationwide. It aims to be available to 97% of the United States’ population by the end of 2017).

67 Id.
68 FAQ. LEMONADE, supra note 14.
70 Id.
71 Id.
72 Insurtech in 2017, supra note 59.
73 Why Oscar?, supra note 27.
74 FAQ, supra note 14.
75 Id.
76 Sawers, supra note 46.
77 Id.
III. CONCLUSION: INSURTECH IN THE NEAR FUTURE

The insurtech revolution is here, but not yet at its apex. If other fintech areas are any guide, innovation will continue. Underwriting methods will improve, new offerings will become available, and beneficial new partnerships will form. As with any data heavy industry, privacy concerns will arise and innovations in other areas are likely to force further transformation in ways that have not yet occurred. For example, autonomous vehicles are expected to decrease car insurance premiums sixty-three percent by 2060 and the insurance is likely to revolve around technology warranties and cyber-attacks rather than human error. The new data gathering and analysis techniques that currently exist, and likely ones that will in the future, will continue to analyze risks with increasing accuracy. Corresponding user-facing innovation will lead to insurance products for self-driving cars and whatever other societal trends arise.

78 Ralph, supra note 17.
Native American tribes possess something special—tribal sovereignty. “Tribal sovereignty includes tribes’ right to govern themselves, define their own membership, manage tribal property, and regulate tribal business and domestic relations.” Tribal sovereignty also recognizes the existence of a government-to-government relationship between tribes and the U.S. government. This relationship often complicates the intersection of tribal, state, and federal law. This is increasingly true in a world connected online. Specifically, it has spurred debate in regard to online lending and co-regulation of financial technology in Indian Country. While tribes try to grow their economies through financial technology opportunities, outside third parties are seizing the opportunity to exploit tribal sovereignty and immunity as a means to make large profits “on” the reservation via the internet through online “rent-a-tribe” models. Tribes must be able to regulate these online...
financial entities because the impact is imminent and the need for financial technology is Indian Country is a means of survival for the tribe.

Economic development in Indian Country is scarce. Tribes are typically located in isolated areas and are becoming more dependent on technology advancements and e-commerce to maintain economic sustainability and connectivity. Economic stability in Indian Country often comes from gaming which alone is at least a $30 billion-dollar industry, federal funding, and more recently from e-commerce and other internet businesses. A growing need to increase the number of tribal entities online, build tribes’ economic status, and engage with online lending naturally drives tribes to engage in financial technology ventures.

Tribes have been quick to embrace financial technology in Indian Country. Tribes located in remote areas without sufficient traffic to engage profitably in casino gambling have found revenue from consumer lending over the internet for example. Some tribes regulate tribal enterprises, provide online lending, educate and protect consumers, and use financial technology to increase tribal lending opportunities. Many tribes have created individual tribal lending entities (hereinafter “TLE”), which are typically tribal chartered and funded by a third party. TLEs make loans over the internet to consumers throughout the United States. These loans may be on terms that are unlawful under state laws where the borrowers reside. Tribes aim to gain revenue through these ventures and to adequately regulate the practice. However, due to the lack of funding, tribes need a third party to fund these entities. The third

6 Native American tribes in the United States face many socio-economic deficits compared to other minority and white peers. See COHEN’S HANDBOOK OF FEDERAL INDIAN LAW [§ 21.04] (Nell Jessup Newton ed., 2015) (in 2005, the average unemployment rate for Indians on or near reservations was 49%); see also ROBERT T. ANDERSON ET AL., AMERICAN INDIAN LAW: CASES AND COMMENTARY, 7 (West Academic, 3rd ed. 2015) (in 2006, Native Americans were found to be poorer than their white peers with 27% below the poverty line).
9 Id. (TLEs are financed by a third party and because TLEs are deemed an "arm" of the tribe, TLEs benefits from the tribe's sovereign immunity).
10 Id.
11 Id.
parties capitalize on this model, earning massive profits and circumventing state laws—using the location of the tribes.\textsuperscript{12}

In 2010, Congress enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to recover from the financial crisis in 2008.\textsuperscript{13} The Dodd-Frank Act directed the Consumer Financial Protection Bureau (CFPB) to respect the status of tribal governments as co-regulators and to allow tribes to oversee e-commerce businesses and protect consumers.\textsuperscript{14} Prior to the Dodd-Frank Act, “federal enforcement of substantive consumer lending laws against non-depository payday lenders was generally limited to civil prosecution by the Federal Trade Commission (FTC).”\textsuperscript{15} However, no reported decisions could be found regarding the FTC's assertion of jurisdiction over TLEs.\textsuperscript{16} Thus, CFPB now is in new terrain with no precedent of asserting jurisdiction of TLEs in Indian Country. TLEs are considered “covered persons” under the Act.\textsuperscript{17} However, tribes are not stated in the definition of “covered persons.”\textsuperscript{18} In fact, tribes likely will argue given their sovereignty, tribes alone have the power to decide whether to and on what terms they may lend to others online.\textsuperscript{19} Currently, three tribal lenders are asking that the Ninth Circuit halt the mandate to comply with civil investigation demands by the CFPB.\textsuperscript{20} The tribal lending companies plan to

\textsuperscript{12} Paul Walsh & Neal St. Anthony, \textit{State Bars Internet Lender, Wins $11.7M Settlement Over ‘Rent-Tribe’ Loans}, STAR TRIBUNE (Aug. 18, 2016), http://www.startribune.com/state-bars-internet-lender-wins-11-7m-settlement-over-rent-a-tribe-loans/390577961/ [https://perma.cc/53GT-P97J] (providing an example in which CashCall Inc. collected payments that were higher than allowed by state law through a rent-a-tribe model).


\textsuperscript{15} See Miller \textit{supra} note 8 (presenting reasons why tribes may argue CFPB cannot assert jurisdiction over TLEs. For example, tribes may further argue “\textit{a fortiori} that tribes are "states" within the meaning of Section 1002(27) of the Act and thus are co-sovereigns with whom supervision is to be coordinated.”).

take the split decisions regarding the question of the proper structure of CFPB’s authority under the Consumer Financial Protection Act over tribes and tribal companies to the Supreme Court.  

In 2012, the Native American Financial Services Association (“NAFSA”) was formed in order to advocate for Native American sovereign rights to regulate and to enable tribes to offer responsible online lending products. This would allow tribal regulators to control the exploitation of financial technology issues such as the “rent-a-tribe” model. Through the protection of consumer rights and sovereign immunity, NAFSA “provides vital services to tribally operated lenders serving the under-banked with better short term financial services, furthering economic development opportunities in Indian Country.” This entity has become vital in facilitating tribes’ co-regulation in areas such as online lending. Nonetheless, as technology advances, the federal government continues to increase oversight. For example, in 2016 the Office of the Comptroller of the Currency (OCC) released “Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective” to support responsible innovation in the federal banking system. To adjust to the ever-changing laws, regulations, and technology some tribes have followed suit and developed their own regulations or commissions. For example, the Otoe-Missouria Tribe established the Consumer Finance Services Regulatory Commission to protect consumers and online lending businesses, which other tribes have also done. In 2016, the

21 Id.
23 Id. (Barry Brandon, Executive Director of NAFSA noted that Dodd-Frank, the legislation that created the CFPB, specifically assigns co-regulator status to tribal nations).
Tunica Biloxi Tribe of Louisiana started a regulatory commission to oversee tribal consumer lending. The tribe recognized that the federal government has taken the role in lending through the Consumer Financial Protection Bureau (CFPB), and so that is the model the tribe looked at.

In 2016, tribes actively continued to request that the United States Congress honor tribal sovereignty and ensure the CFPB does as well with any rule they produce on short-term lending. Tribes can sufficiently regulate online lending themselves. John R. Sotton, Chairman of the Otoe-Missouria Tribe, stated in The Hill, “As sovereign nations it is time for Washington [D.C.] to recognize that our businesses are not only legal and lawful, but have strict regulations already in place providing oversight of our tribal enterprises and ensuring consumers are protected.” Moreover, Sherry Treppa, Chairperson of the Habematolel Pomo of Upper Lake, stated that she remains “concerned that the CFPB is developing its proposed action in a vacuum without consulting with tribes to learn about the innumerable tools that we have developed…” She too urged Congress to “take an approach that respects tribal sovereignty and one that takes account of both consumer need and the robust self-regulation that sovereign tribes have established.”

Tribes should be allowed to regulate or co-regulate in the financial technology space when the tribe has created tribal laws and commissions that are consistent with federal regulations. Tribes are in the best position to understand and guard against “rent-a-tribe” models. Many outside lenders take advantage of tribes and sovereign immunity. For example, CashCall tried to exploit state lending laws and limits by conducting business on reservations. The U.S. District Court for the Central District of California

---


27 Id.

28 Id.

29 See Shotton, supra note 14.

30 See Native American Financial Services Association, supra note 22.

31 Id.

32 See McLannahan, supra note 5.

33 See Consumer Fin. Prot. Bureau v. CashCall, Inc., No. CV 15-7522-JFW (RAOx), 2016 U.S. Dist. LEXIS 130584 (C.D. Cal. Aug. 31, 2016) (holding that CashCall Inc. violated federal law when it offered high-interest loans through a firm based on tribal lands in states where such loans were barred).
recently ruled against such behavior in a win for CFPB.\textsuperscript{34} This presents a
typical scheme with online lending that the tribe should be able to regulate or
co-regulate to prevent.

Amid fast-paced change surrounding the Dodd-Frank Act,\textsuperscript{35} the right
for tribes to co-regulate will be an issue in e-commerce and financial
technology to watch. Most recently, President Trump signed an executive
order to erode much of the Dodd-Frank Act. Trump directed his Treasury
Secretary nominee to draft a report within 120 days identifying laws, treaties
and regulations that conflict with his de-regulatory principles.\textsuperscript{36} Results of the
new administration’s actions could potentially impede or erode the tribal right
to co-regulate and will impact the ability of tribes to control their own e-
commerce. Given that tribes have unique needs and practices, local control
over the sovereign nation and their own entities makes sense. A change to
local control could impact how tribes interact with outside players, manage
short-term lending, and a rollback could be detrimental to their economic
status if tribal needs are not accurately calculated by federal regulations.
Arguably, tribes know their industries best and will be able to develop
regulations specific to each tribe more effectively. A sovereign nation that
meets regulation standards and regulates their own entities sufficiently should
be able to act parallel to a federal regulation that does the same thing. We
should continue to honestly follow the CFPB Tribal Consultation policy\textsuperscript{37} as
federal regulations advance and allow co-regulation with tribes.

\textsuperscript{34} Id.
\textsuperscript{35} Antoine Gara, With A Stroke Of The Pen, Donald Trump Aims To Wave Goodbye To The
Dodd Frank Act, FORBES (Feb. 3, 2017),
\textsuperscript{36} Id.
\textsuperscript{37} CONSUMER FIN. PROT. BUREAU, TRIBAL CONSULTATION POLICY (Apr. 22, 2013),