Akron Law Review

Volume 55
Issue 3 *Cybersecurity Symposium Issue*

Article 1

2022

Security in the Digital Age

Michael Gentithes

SECURITY IN THE DIGITAL AGE

Michael Gentithes[*]

I. INTRODUCTION

Rapidly evolving technology allows governments and businesses to elevate our collective well-being in ways we could not have imagined just decades ago. Data is now a resource that governments and businesses alike can mine to address the world's needs with greater efficiency, accuracy, and flexibility. But evolving technology and advanced data analytics also come with risk. New digital capabilities also create new means for nefarious actors to infiltrate the complex technological systems at the heart of nearly all of our daily activities. Just as new digital tools emerge to offer unique goods and services, new tools allow wrongdoers to invade our privacy, manipulate data, and undermine our infrastructure systems. New technological frontiers also create a vast array of potential targets for crime and mischief, as both businesses and criminals recognize the value of data and the containers, both physical and digital, in which it resides.

This year's Akron Law Review symposium calls attention to these proliferating risks associated with the incredible pace of technological change that has come to define the modern world. The contributions at this symposium consider how we define and regulate new digital technologies; the governmental structures and incentives that will ensure that responsible actors, both public and private, can protect against

[*]Associate Dean of Academic Affairs and Associate Professor, University of Akron School of Law. Thank you to the members of the Akron Law Review, the organizers of this Cybersecurity Symposium, and to my fellow presenters at the event.

cybercrime and data loss; and the practical steps entities can take to protect against the proliferating security threats of our digital age. At the outset of this wonderful and timely symposium edition of the Akron Law Review, I want to offer a few thoughts on each of those topics to center the discussion in each area.

II. CRYPTOCURRENCY REGULATION, BLOCKCHAIN, AND SECURITY

In recent months, cryptocurrencies have made headlines for their growing role in international finance and prices volatile enough to make any investor seasick. But cryptocurrency, and the technology behind it, has vast repercussions both for our regulatory state and for cybersecurity regimes in general.

Cryptocurrencies are so intriguing in part because of the technological and philosophical advance that underlies them. Blockchain technology uses a "distributed ledger"—a database that is replicated on thousands of computers around the world, all publicly available to interested parties.[1] In the context of cryptocurrencies, those copies of the database will contain the entire payment history of every digital coin then in circulation. As new transactions occur, parties can use that distributed ledger to verify that the parties have coins to exchange, then include the transaction in a new proposed "block" of code to add to the ledger. The proposed new block is then encrypted into a digital "hash" function, which includes a complex mathematical puzzle that must be solved by trial and error (and massive computing power).[2] Only when that puzzle is solved can the block be added to the distributed ledger.[3] That solution can be checked quickly by the other computers with access to the ledger, and if it is verified it can then be added to the ledger's history. Because this solution-and-verification stage can be repeated by so many entities distributed across the globe, there seems to be little opportunity for foul play, either by falsifying past transactions or inserting new and inaccurate information into a block.[4] And before a new block of information can be included in the ledger, it must correctly include the previous blocks in a

1. *The Great Chain of Being Sure About Things*, ECONOMIST.COM, Oct. 31, 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things; *see also* Deborah Ginsberg, *The Building Blocks of Blockchain*, 20 N.C. J.L. & TECH.471, 473-81 (2019).

2. *The Great Chain of Being Sure About Things*, ECONOMIST.COM,, Oct. 31, 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

3. Tal Yellin, Dominic Aratari & Jose Pagliery, *What Is Bitcoin?*, CNN MONEY, (Aug. 8, 2018), https://money.cnn.com/infographic/technology/what-is-bitcoin/; Deborah Ginsberg, *The Building Blocks of Blockchain*, 20 N.C. J.L. & TECH., 471, 477 (2019).

4. Deborah Ginsberg, *The Building Blocks of Blockchain*, 20 N.C. J.L. & TECH. 471, 478 (2019).

way that others in the community deem acceptable; any attempt to modify the prior history of exchanges will be immediately detectable by any one of the thousands of computers that has a copy of the ledger.[5] Because thousands of computers have instant access to all transactions that occur, there are thousands of opportunities for independent verification that no party has altered the prior transactions.

While all this sounds promising, its opacity is a challenge to both the public and would-be regulators. Unlike online transactions using traditional currencies, a digital currency exchange can be proposed for addition to the chain without a third-party banking service acting as an intermediary.[6] That eliminates one opportunity for regulation. Complicating the process even further is the decentralized nature of the blockchain, which is not housed in any single government or entity's hands. Verification of transactions occurs across the globe, but without any clear identifying information about the parties to a transaction or the potentially illicit subject that spurred the exchange in the first place.

This decentralized ledger technology is also difficult to hack, because of the layers of verification and the number of copies widely available. Taking mass control over those distributed nodes of information would require incredible computing power and precise coordination, which seems unlikely if not impossible.

Early efforts to regulate cryptocurrencies focused on developing "know your customer" technology that would reveal the identity of those exchanging cryptocurrencies to ensure that these decentralized forms of exchange did not become a haven for money launderers or terrorists.[7] But no clear global regulator capable of enforcing those rules across jurisdictions has emerged.

Yet further opportunities for regulation may emerge when cryptocurrencies are considered as a store of value—a means of parking cash in a valuable commodity that investors expect to hold, if not increase, in value over the long term. At a minimum, such assets can be taxed. Whether governments treat cryptocurrencies as property taxable for capital gains based upon fair market values at the time they are exchanged,

5. Deborah Ginsberg, *The Building Blocks of Blockchain*, N.C. J.L. & TECH. 471, 478 (2019).

6. Deborah Ginsberg, *The Building Blocks of Blockchain*, N.C. J.L. & TECH. 471, 473-74 (2019).

7. *See, e.g.*, Angus Berwick & Tom Wilson, *Crypto giant Binance kept weak money-laundering checks even as it promised tougher compliance, documents show*, REUTERS, Jan. 21. 2022, https://www.reuters.com/investigates/special-report/finance-crypto-currency-binance/ (discussing failures of early "KYC" technology to reduce money laundering in cryptocurrencies).

or perhaps even as inventory taxed as ordinary gains, they can both regulate cryptocurrencies and limit their use for nefarious purposes.

Beyond the concerns over regulations of cryptocurrencies are the potential security benefits of blockchain technology. Blockchain can create recordings of important information that seem nearly impossible to manipulate given the distributed nature of the ledger and the ability of so many independent entities to verify new additions to it. Both governments and private parties thus see great potential in this technology as a means of providing virtually unmanipulable records of transactions, whether they be in real estate, luxury goods, or notarization. Just as the technology creates opportunities for mischief by hiding the proceeds of traditional crimes, it generates opportunities to simplify the process of verifying critical information at vastly reduced costs.

III. CYBERSECURITY AND INCENTIVE REGULATORY STRUCTURES

While cryptocurrency regulation considers the role of the government in protecting consumers from the dangers of a new kind of offering from businesses, another regulatory front is the way that governments might incentivize best (or better) practices as businesses attempt to safeguard consumers' data. At present, a patchwork of laws at the state and federal level protect consumers from security breaches and penalize companies for insufficient cybersecurity regimes, providing some relief after a hack has already occurred.[8] But those regimes fail to address systemic flaws in corporate and government security regimes, especially those that concern the possible destruction of, or loss of access to, data about individual citizens and consumers.[9] Incentive-based cybersecurity regimes, by contrast, would provide carrots to entice businesses to meet higher security standards that might improve system-wide protection against breaches and data loss.[10] Merely protecting the privacy of individual consumers from breaches with *post hoc* penalties does not address these broader, systemic concerns.

8. Jeffrey Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 401 (2016).

9. Jeffrey Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 402, 404 (2016).

10. "Among the policies that lawmakers might consider are tax credits for cybersecurity investments, a national cybersecurity insurance program, and a safe harbor from data security lawsuits for companies that adhere to a rigorous set of government-mandated security standards." Jeffrey Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 403 (2016).

Developing cybersecurity performance goals and rewarding them appropriately—whether through tax incentives, lower cybersecurity insurance rates, grants, subsidies, or other forms of government stimulus—thus holds great promise for broadening and enhancing cybersecurity efforts across the nation.[11] This may be especially important in protecting our national infrastructure from cyberattack, which could target both private and government networks indiscriminately in an effort to find the weakest links. For example, federal energy regulators have recently considered a program to incentivize enhanced cybersecurity amongst electric companies.[12]

But how should government regulators define minimum cybersecurity standards that would qualify for these varied incentives? Perhaps a focus on the processes used to generate, preserve, and protect data—rather than on outcomes like reducing the frequency of breaches—would best promote effective security regimes. Focusing on process also ensures that companies invest in security measures that are designed to reduce weaknesses along the security chain, rather than focusing on reaching a bottom-line result at the lowest possible cost. The latter method may be a useful one for capitalist enterprises in general, but is likely to generate deeply flawed cybersecurity regimes with easily exploitable weaknesses. Companies may not naturally flock to security measures that are more expensive, yet more carefully designed to focus on the processes through which data flows through the organization. But government incentives could change the corporate thinking and generate a sounder national infrastructure.

The discussion of process-based security highlights another obligation that corporate actors have in the way they manipulate and utilize customer data. In the modern marketplace, big data is big business in part because of the way computing power can be used to manipulate data and tailor business offerings to consumers most likely or able to buy the goods and services on offer. But the predictive algorithms used to interpret the data[13] and determine who is offered the next flash sale, home loan, or even job listing hold vast potential to generate and compound

11. DEPARTMENT OF HOMELAND SECURITY INTEGRATED TASK FORCE, INCENTIVES STUDY ANALYTIC REPORT, EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 19 (June 12, 2013).

12. Grace Dille, *FERC Proposes Cybersecurity Incentives for Electric Companies*, MeriTalk.com, Feb. 9, 2021, https://www.meritalk.com/articles/ferc-proposes-cybersecurity-incentives-for-electric-companies/.

13. Robert Sloan & Richard Warner, *When Is an Algorithm Transparent? Predictive Analytics, Privacy, and Public Policy*, 16 IEEE SEC. & PRIV. 18 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3051588.

injustice in modern society. First, the data-collection process itself may lead to inaccuracies. Faulty or incorrect data, or improper use of technology to clean and sort that data, can cause injustice directly when the inputs to an algorithm are inaccurate.[14] Second, even if the data is accurate, that data itself may be the product of some historical injustice that in turn is compounded by the new algorithm.[15] For instance, some groups, through no fault of their own, may have less wealth, power, health care, or work skills at their disposal—all data points that algorithms will seize upon to parse who should and should not receive a variety of goods, or which social media update should be sent to which user. This will lead to traditionally disfavored groups being disfavored yet again in the modern analytical world. Even if there is no discriminatory intent in the way companies manipulate the data or programmers generate the algorithms, the discriminatory impact may be significant, lasting, and irreversible—especially as artificial intelligence is increasingly prevalent in data analytics, with little opportunity for human control over or interpretation of the algorithms it generates to make these decisions.

A focus on process, rather than results, might again help solve this data-related problem. Actors deploying predictive analytics and predictive algorithms should consider the methods of creating them, ensuring some level of control and transparency over the algorithms themselves rather than seeking an end result that increases profit margins, no matter the disparate effects it may have on traditionally disfavored and underprivileged groups in society.

IV. PUTTING PRIVACY INTO PRACTICE

The cybersecurity objectives identified above are broad and provide little practical guidance for implementation. Focusing on practical steps to protect data privacy is just as important as identifying those broader security goals.

One way to proceed is to identify the greatest areas of risk for data protection by mapping the flow of data throughout an organization. This allows entities to create an overview of security protections already in place and identify the weaknesses in those protections, just as a potential hacker might. It also acknowledges current control over such data—who has access, control, and storage capabilities at any given time—and

14. Deborah Hellman, *Big Data and Compounding Injustice*, J. MORAL PHIL. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840175.

15. Deborah Hellman, *Big Data and Compounding Injustice*, J. MORAL PHIL. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840175.

whether that distribution of authority is ideal to prevent data incidents and breaches in the future. It can also ensure that particularly sensitive information receives enhanced security treatment throughout the organization, tailoring the cybersecurity regime to the areas most likely to face attack or threat in the future.

That basic risk assessment also allows entities to ensure compliance with regulatory regimes that punish entities for data breaches. This looks both to the standardized procedures within an organization, as well as the organizations response plan in case of extraordinary incidents that lead to data breach or loss. Instituting such plans can play a vital role in minimizing the damaging effects of a given hack or security flaw.

Furthermore, this kind of early and repeated risk analysis can highlight the human flaws in any data protection regime within an organization. Because a significant majority of data incidents occur as the result of human error of some form or another, highlighting the weaknesses in the organization's data processing method can heighten awareness to such errors and prevent future incidents. Simply incentivizing individual actors in the organization to pay attention to potential data incidents can have a significant effect.

One way to lessen the load of privacy protection is to reduce an organization's access to and control over sensitive information. This includes ensuring clear and frequent plans for the destruction and deletion of data no longer needed or necessary to the organization's core functions. This again requires frequent assessment of an organization's data controls and procedures, but with an eye towards shrinking the overall data footprint rather than merely ensuring safety at every stage of the process. Minimizing data collection itself will help reduce the risk of data incidents over time.

V. CONCLUSION

Modern technological advances present both opportunities and pitfalls. Governments and businesses can use advances in data processing power to enhance our lives and avoid repeating the injustices of the past, but only if they are cognizant of the risks associated both with securing that data and utilizing it to distribute burdens and benefits. Digital currencies, and the technology advances that underlies them, likewise present opportunities to simplify and secure commercial transactions, but only if properly regulated. And government and corporate actors need process-based recommendations to implement security regimes that meet an acceptable standard of safety for protecting data and infrastructure.

This symposium provides important contributions to these discussions, with the hope that enhancing cybersecurity can likewise enhance the contributions technology can make to all of our lives.