A Democracy of Users

John P. Dever & Captain James A. Dever*

"Well, Doctor, what have we got – a Republic or a Monarchy?"
"A Republic, if you can keep it."

Response attributed to Dr. Benjamin Franklin when queried as he left Independence Hall on the final day of the Constitutional Convention, September 17, 1787.[1]

INTRODUCTION

This article addresses how a Republic can thrive in a digital world. A number of Americans were first exposed to the Internet in the 1990s. In those years, the noise of Internet dial-up was the sound of progress, and AOL's treasured phrase "You've got mail!" linked users and communities in new and profound ways that only a short time before were the strict purview of science fiction. In 2017, individuals

* *James A. Dever* is an active duty Judge Advocate in the U.S. Army. He previously served at the Cyber Center of Excellence, Fort Gordon, GA. The views expressed in this article are solely those of the author and do not reflect the official policy or position of the United States Army, Department of Defense, or U.S. Government.
John P. Dever Jr. holds a L.L.M. in National Security Law from Georgetown University. He is currently the Leader of AML / Sanctions Program for Wholesale Banking, Wells Fargo. Prior to joining Wells Fargo he was the Finical Crimes Compliance Leader and Global Crisis Management Leader for GE Capital, Americas. Before joining the private sector, he served as an Assistant U.S. Attorney in the Northern District of Illinois and as an Assistant General Counsel in the Federal Bureau of Investigation's National Security Law Branch, Counterterrorism Division. He began his career on active duty in the U.S. Army as a Judge Advocate. He served multiple combat deployments and is the recipient of the Bronze Star and the Purple Heart Medals.
[1] 3 THE RECORDS OF THE FEDERAL CONVENTION OF 1787, 85 (Max Farrand ed. 1911).

navigate their world via digital devices. In a practical sense, analog maps are museum pieces, as many people get from A to B using a variety of smart phone apps. The use of this new technology is pervasive. Even a stop at a red light often entails a driver reaching for her smartphone to view a work text or Facebook news feed. Today's citizen lives an e-existence and therein lies a multitude of possibilities and pitfalls.

The article begins by discussing two of the issues that show both the incredible potential of the internet while simultaneously representing how the internet can also present very real danger, Big Data and the Internet of Things. Citizens must remain cognizant that privacy is constantly at stake in this electronic world. Perhaps not surprisingly, opinions differ regarding how best to protect privacy; although coding it appears to be a fruitful endeavor. As cybersecurity becomes the new arms race between hacker and system, illegitimate versus legitimate user, nations and private entities alike must develop resilient policies to account for a paucity of law. Most importantly, to secure the Republic for the next century, users must prize the responsibilities of citizenship. Democracy flourishes in the marketplace of ideas yet users are increasingly being drawn into digital echo chambers where faction is exorcised while accepted tropes are exalted. Systems and hardware must be better protected against hostile and unintended cyber events, but the ultimate safeguard of a Republic is the well-informed user-citizen.

I. THE FUTURE IS NOW

A. Big Data

Big Data refers to collecting and storing large

amounts of various granular data in real time and using data analytics to reveal insights from the aggregated information.[2] As the second decade of the twenty-first century draws to a close, people are becoming increasingly connected to the Internet in ways that sometimes obfuscate the relationship between human interaction and Big Data. The amount of information contained in Big Data is staggering. Much of the world's stored information today is digital, and existing mathematical terms struggle to quantify it.[3] The types of information that is now digitized include information that once existed in analog format (books, census records, customer information) as well as new kinds of information made possible by modern technologies.[4] In addition, digitization alters the nature of the information itself. "Information that can be digitized can also be collected, searched, quantified, compared, assessed, and endlessly repurposed."[5] This ability to manipulate data

---

[2] Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997 (2016); *see also* Charles McLellan, *The Internet of Things and Big Data: Unlocking the Power*, ZDNET (Mar. 2, 2016), http://www.zdnet.com/article/the-internet-of-things-and-big-data-unlocking-the-power.

[3] The largest current recognized number is a yottabyte: a digit with twenty-four zeros. *See* John Foley, *Extreme Big Data; Beyond Zettabytes and Yottabytes*, FORBES (Oct. 9, 2013), http://www.forbes.com/sites/oracle/2013/10/09/extreme-big-data-beyond-zettabytes-and-yottabytes.

[4] President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* (May 2014), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [http://perma.cc/87G9-HSCP] (distinguishing between data "born digital" and "born analog").

[5] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 20

allows it to be presented in any fashion the presenter wishes, with little regard to veracity.

Additionally, Big Data provides a different way of understanding and probing the world of information. Consider how Big Data has altered conventional research–if traditional scientific research begins with a question and then uses that hypothesis to identify and collect the appropriate data, Big Data upends that practice.[6] As near limitless information is being generated all of the time, researchers working with Big Data do not have to shape or limit their data collection. Nor are they restricted to beginning with a hypothesis. Indeed, the question can arise from the information itself. "This is why, for example, the constant stream of posted tweets on Twitter can generate data and insights for meteorologists, advertisers, and epidemiologists."[7]

B. Internet of Things

Billions of people are online. In the past decade, user demand drove a veritable explosion of smartphone sales and their applications. The next wave of information technology will likely be the Internet of Things (IoT).[8] The IoT comprises an evolving array of technologies that extend the idea of instantaneous connectivity beyond computers, smartphones, and tablets to everyday objects such as home

(2016).

[6] *Id.*

[7] *Id. See also* Victor Luckerson, *What the Library of Congress Plans to Do with All Your Tweets*, TIME (Feb. 25, 2013), http://business.time.com/2013/02/25/what-the- library-of-congress-plans- to-do- with-all- your-tweets [http://perma.cc/F5RN-UB5M].

[8] Poudel, *supra* note 2, at 997.

appliances, cars, and medical devices.[9] Market research indicates that 220 billion IoT devices will be in use by 2020.[10]

The goal of the IoT is to enable ubiquitous connection: a reality where the real, the digital, and the virtual are converging to create smart environments.[11] The underlying drivers of the IoT include massive increases in processing power, digitization of data, storage capacity, wireless communications and networking capabilities.[12]

The term IoT was first coined in 1998 by British technologist Kevin Ashton during a presentation to Procter and Gamble. He said "[a]dding radio-frequency identification and sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception."[13] The visionary concept was that radio-frequency identification devices could be used to order, track, and study manufacturing processes in an entirely innovative manner.[14] In 2009, Ashton reflected on the implications for the IoT:

---

[9] *Id.*

[10] Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME (JAN. 13, 2014), http://time.com/539/the-next- big-thing- for-tech- the-internet- of-everything [http://perma.cc/7YCH-GY79].

[11] Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641 (2015).

[12] Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 8 (2015).

[13] Kevin Ashton, *That 'Internet of Things' Thing*, RFID JOURNAL (June 22, 2009), http://www.rfidjournal.com/articles/view?4986 [https://perma.cc/X679-AWNF].

[14] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 813 (2016).

> "If we had computers that knew everything there was to know about things using data they gathered without any help from us we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory."[15]

To be sure, the IoT offers vast possibilities to advance the myriad ways people connect, interact, and benefit from a digital world. And yet dangers aplenty lurk alongside the splendid technological possibilities.[16]

Certain innovators and technologists are making connections between the IoT and virtual/augmented reality. On March 25, 2014, Facebook founder Mark Zuckerberg announced in an online post that his company acquired Oculus Virtual Reality, the leader in virtual reality technology.[17] Zuckerberg stated that his "mission is to make the world more open and connected.… this has mostly meant building mobile apps … (but VR) is a new communication platform … you can share unbounded spaces and experiences (with) people."[18] Employing triumphal language, Zuckerberg expounded upon the possibilities of a future wherein people were connected to virtual reality – "(it) was once the dream of science fiction. But the internet

---

[15] Thierer *supra* note 12, at 10.

[16] Nikole Davenport, *Smart Washers May Clean Your Clothes, but Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on A Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 268 (2016).

[17] Mark Zukerberg, Oculus VR Acquisition Announcement (Mar. 25, 2014), https://www.facebook.com/zuck/posts/10101319050523971.

[18] *Id.*

was also once a dream, and so were computers and smartphones. The future is coming…"[19]

II. PRIVACY FRONTIERS

A. Big Data and Privacy

Information privacy and data security are sometimes described as two sides of the same coin.[20] As people are often wary of new technology, advancements in communication techniques can be perceived as threats to privacy and lead to policymakers and consumers demanding additional safeguards against intrusion.[21] Certain experts

---

[19] *Id. See also* Ross Gerber, *Internet of Things, Virtual Reality And Smart Cars Driving Chips to the Next Level*, FORBES (Sept. 29, 2016, 4:32 PM), http://www.forbes.com/sites/greatspeculations/2016/09/29/internet-of-things-virtual-reality-and-smart-cars-driving-chips-to-the-next-level/#172a36ff451d.

[20] *Id.* Patrick Manzo, Executive Vice President, Global Customer Service and Chief Privacy Officer of Monster Worldwide, Inc., commented on the relationship between data and privacy: "Data security and data privacy are two sides of the same coin, and we trade that coin for consumer trust." He "defines data security as, simply, knowing where your data is located, and who may access the data. Data privacy is predicated on data security and requires further understanding how personal data is being collected, processed (and by whom), and transferred, and the consistency of these practices with applicable laws, regulations, and the reasonable expectations of the relevant consumers." Eileen Spear, *Data Privacy and Data Security: Two Sides of the Same Coin A Conversation with Patrick Manzo, Executive Vice President, Global Customer Service and Chief Privacy Officer of Monster Worldwide, Inc.*, NATIONAL LAW REVIEW (May 11, 2015), http://www.natlawreview.com/article/data-privacy-and-data-security-two-sides-same-coin-conversation-patrick-manzo-execut.

[21] Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV.

maintain that in 2026, up to one-third of Americans will be living with a digital device inside their bodies.[22] While "digital pills" may offer many potential benefits, a number of skeptics cite serious risks to privacy that must be addressed.[23] In a January 2015 report, the Federal Trade Commission (FTC) exhorted businesses to take concrete steps to help protect consumers' privacy.[24] The FTC report further noted that there are currently over 25 billion connected devices around the world and the number of these devices, including cars, is expected to rise exponentially.[25]

Most people know to guard their pin while accessing an ATM; it is common sense to protect a bank account from prying eyes. Yet what happens when connecting to the IoT or interacting with someone across the world through the medium of virtual reality becomes mundane? The issue of digital complacency arises when people are not adequately guarded against the new possibilities for intrusion they face in an increasingly electronic existence. The capacity to intrude on peoples' lives is increasing. Target's now-infamous use of Big Data helps illustrate the point.[26] The best time for retailers to get customers to commit to a new chain is at the moment of a major life change, such as a

F. 61, 63 (2016).

[22] Amelia R. Montgomery, *Just What the Doctor Ordered: Protecting Privacy Without Impeding Development of Digital Pills*, 19 VAND. J. ENT. & TECH. L. 147, 148 (2016).

[23] *Id.*

[24] Anthony Jones, *Autonomous Cars: Navigating the Patchwork of Data Privacy Laws That Could Impact the Industry*, 25 CATH. U.J.L. & TECH. 180, 195 (2016); FTC, *Internet of Things: Privacy and Sec. in a Connected World* 12-13 (2015).

[25] *Id.*

[26] Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 350 (2015).

child's birth.[27] Several years ago, Target used Big Data to market baby goods to pregnant women. The tricky part was identifying which women were pregnant. Thanks to data analytics, Target was able to compare its massive database of customer purchases with public birth listings and in-store baby shower registries to identify about two dozen items that pregnant women often bought in the months before giving birth – items such as unscented body lotion, calcium supplements, and hand sanitizers.[28] Target then took this profile of a pregnant customer and applied it to its database of current customers. If a woman had recently purchased a number of items on the list, Target assigned her a high "pregnancy prediction score" and delivered baby-related advertisements and coupons.[29] Remarkably, Target's intrusive practices came to light when a father became aware that his high school aged daughter was pregnant when the retailer sent her numerous coupons for baby-related items.[30] As one Target statistician told the *New York Times*, data analytics is a powerful tool that must be wielded softly even in lawful arenas to avoid consumer backlash: "If we send someone a catalog and say, 'Congratulations on your first child!' and they've never told us they're pregnant, that's going to make some people uncomfortable…. We are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy."[31]

---

[27] *Id.*
[28] *Id.* at 350-51.
[29] *Id.* at 351.
[30] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?.
[31] *Id.*

B. Sacrificing Privacy

Privacy intrusions do not merely arise from the profit motive. Everyday consumers willingly engage in privacy-sacrificing behaviors.[32] For instance, whenever a user logs on to more than one Google service (e.g., Gmail, Google Maps, or YouTube), Google monitors and aggregates the user's searches and activity.[33] In regard to the IoT devices, consumers purchase them with little knowledge, or, perhaps more worrisome, with little care about to whom the devices may disclose data.[34]

Three problems may be exacerbated when consumers exchange their privacy rights for IoT device convenience. First, companies producing IoT devices could become like Google or Target and use customers' private data to create specialized advertisements.[35] Despite being lawful, Big Data analytics create an environment where companies have an almost unrestricted insight into customers' lives. Second, there are myriad data security risks whenever personal data is available on the internet. Hackers have repeatedly shown that they have the capability to compromise IoT devices and have broken into online video cameras and baby monitors.[36] Third, companies have shown

---

[32] Melissa W. Bailey, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1024 (2016).

[33] *Id.*

[34] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEXAS L. REV. 85, 140-43 (2014) (explaining how difficult it is to locate the privacy policies of various IoT manufacturers).

[35] Bailey, *supra* note 32, at 1025.

[36] *Id. See generally Home, Hacked Home*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606420- perils-connected- devices-home-hacked-home [http://perma.cc/8MKC-

an eagerness to sell data to buyers. A particularly egregious example are "data brokers:" entities that aggregate consumer profiles that "may reveal where consumers live; how much they earn; and their race, health conditions, and interests."[37] Indeed, the FTC has already revealed that some mobile apps transmit information to third parties "about consumers' workouts, meals, or diets."[38] And the data exposures are not limited to third-party data brokers; for example, Fitbit has expanded its market to include sales to employers. While Fitbit insists that it does not sell individualized data to employers without the consumer's permission, its privacy terms allow it to sell "de-identified data" without consumer consent.[39]

C. Divergent Privacy Views

Broadly speaking, normative views of privacy fall

4QH9].

[37] Bailey, *supra* note 32, at 1025.

[38] Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 210-11 (2014).

[39] *See* Parmy Olson & Aaron Tilley, *The Quantified Other: Nest and Fitbit Chase a Lucrative Side Business*, FORBES (Apr. 17, 2014), http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest- and-fitbit-chase-a- lucrative-side- business [http://perma.cc/4QFN-JLNC] ("Fitbit is selling companies the tracking bracelets and analytics services to better manage their health care budgets, and its rival Jawbone may be preparing to do the same."); Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance [http://perma.cc/645Y-UCHJ] (detailing how "Fitbit's sales to employers are now one of the fastest growing parts of its business").

into two camps – behaviorist and consequentialist.[40] The behaviorist perspective looks to actors' actions rather than the consequences of those actions (i.e., a behaviorist might suggest that individuals have the right to engage in a specific type of data flow or to prevent that information flow from occurring).[41] The First Amendment provides an illustrative model: the press has the right to publish personal information without the subject's consent and regardless of the consequences.[42] On the other hand, the consequentialist model looks to the outcome of a given action and its effects on privacy rather than to the underlying actions. For example, certain police media guidelines prohibit the release of information about some sexual offenses or crimes involving children because it would tend to identify the victims.[43] Importantly, therefore, the consequentialist model factors unintended consequences into its assessment of whether information should be released. In short, conceiving of privacy as a set of consequences of information flows rather than a set of rights enjoyed by information subjects makes it easier to design policies that produce desirable privacy consequences.

If the consequentialist model is the best approach to protect privacy in the era of Big Data because it takes into account consequences, even those that are unintended, a complication is that statutory reform is slow compared to the rapid pace of technology. The Fourth Amendment protects citizens against unreasonable searches and seizures, a protection that includes warrantless searches of digital

---

[40] Roger Allan Ford, *Unilateral Invasions of Privacy*, 91 NOTRE DAME L. REV. 1075, 1104 (2016).
[41] *Id.*
[42] *Id.*
[43] *Id.*

data.[44] Although the Fourth Amendment has significant implications for the interplay between government and private entities that hold consumer data, it does not protect individuals from *voluntary* interactions with companies.[45] Congress has passed several sectoral statutes that protect discrete types of data that may be in the possession of private entities. For example, the Fair Credit Reporting Act protects consumer credit information, the Family Educational Rights and Privacy Act protects students' educational records, and the Health Information Portability and Accountability Act (HIPAA) protects patient medical information.[46] Overall, however, these laws cover limited types of information in certain situations. The medical information contained in a FitBit or Apple Watch is not covered by HIPAA because that statue only covers certain entities like hospitals or health insurance companies and not user-generated health information.

Given the realities of the digital age, the U.S. might benefit from adopting Britain's approach to privacy solutions. Indeed, Britain (and in large measure the European Union as well) has followed a consequentialist-omnibus approach to privacy wherein data is protected regardless of the type of entity holding the data or the precise type of data at issue.[47] This more holistic view of a "right to

---

[44] U.S. Const. amend. IV.

[45] Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 787 (2016).

[46] *Id. See generally* Fair Credit Reporting Act, 15 U.S.C. §1681 (2012); Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012); Health Information Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

[47] Lipman, *supra* note 45, at 788; *See also* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966, 1975 (2013).

privacy" affects how entities view customer obligations. For its UK website, the giant data broker Acxiom has a privacy policy page that states in part "Acxiom Ltd respects the right of individuals to privacy."[48] The equivalent U.S. webpage begins with "Acxiom respects the privacy of every individual about whom we either process information or maintain information within Acxiom's information products."[49] Besides being much more legalistic and difficult to parse, the U.S. version does not contemplate any individual "right" to privacy, and it mirrors the U.S. sectoral approach by carefully defining whose privacy it will respect.[50]

D. Coding Privacy

1. Privacy by Design

For some researchers, the solution to digital privacy lies in code, taking privacy into account at the forefront of the engineering lifecycle by culturally perpetuating privacy at all levels of an organization.[51] In the Privacy by Design (PbD) framework, managers and creators are encouraged to think about the data and concomitant privacy interests at the start of the design process rather than being simply an

---

[48] Acxiom, *UK Privacy Policy*, http://www.acxiom.com/about-acxiom/privacy/uk-privacy-policy (last visited Mar. 1, 2017).
[49] Acxiom, *US Products Privacy Policy*, http://www.acxiom.com/About-Acxiom/Privacy/US-Products-Full-Privacy-Policy/ (last visited Mar. 1, 2017).
[50] Lipman, *supra* note 45, at 788.
[51] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, IAB (2009), *https://www.iab.org/wp-content/IABuploads/2011/03/fred_carter.pdf.*

afterthought in the development lifecycle.[52] PbD is the notion that online platforms should be designed from the ground up with privacy in mind.[53] Refinement of PbD has yielded seven core tenets called the foundational principles: 1) proactive; 2) privacy as the default setting; 3) privacy embedded into design; 4) full functionality; 5) full lifecycle protection; 6) transparency; and 7) respect for user privacy.[54]

PbD enables creators to specially architect environments and systems with considerations of data use for implementation at the onset, which will directly tie to business or operational processes once the solution is promoted into a live production status.[55] In essence, PbD is a fluid and evolving framework with applicability to the continual advancement of data collection, storage, and use.[56] The design and implementation of privacy requirements in systems is a continually vexing problem and requires a multi-various approach to include the translation of complex social, legal, and ethical concerns into systems requirements.[57] Perhaps most significant, PbD is an opportunity to foster a privacy-first culture that extends from organizational governance and leadership to design concepts that over time will help define brand reputation.[58] After all, if PbD proves successful, it may assist the symbiotic relationship between privacy and the helpful aspects of Big Data: as former FTC chairwoman Edith Ramirez recently

---

[52] *Id.*
[53] Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193, 226 (2016).
[54] Cavoukian, *supra* note 75.
[55] Eric Everson, *Privacy by Design: Taking Ctrl of Big Data*, 65 CLEV. ST. L. REV. 27, 29 (2016).
[56] *Id.*
[57] *Id.*
[58] *Id.*

remarked, "[t]here is a risk we won't really be able to innovate, we won't really be able to make full use of big data … unless we really do make sure that consumers feel that they have control."[59]

2. Privacy Engineering

In 2017, the National Institute of Standards and Technology (NIST) developed An Introduction to Privacy Engineering and Risk Management in Federal Systems (PRM). The novel framework is a new approach to assessing and managing risks to privacy and is focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes personally identifiable information (PII).[60] Whereas PbD involves approaching the entire design of a system or product from a positive sum, proactive viewpoint, and using privacy as the default choice in system design, privacy engineering takes a more granular approach and recognizes the boundaries and overlap between privacy and security.[61]

---

[59] Anita L. Allen, *Protecting One's Own Privacy in A Big Data Economy*, 130 HARV. L. REV. F. 71, 78 (2016).

[60] Brooks et al., *NISTIR 8062 – An Introduction to Privacy Engineering and Risk Management in Federal Systems*, iv (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. Office of Management and Budget defines "personally identifiable information" as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual," in Circular A-130, "Managing Federal Information as a Strategic Resource" (2016), https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[61] Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L.J. 251, 303 (2016). *See also* Brooks et

As pertains to information security, the security objectives commonly known as the "CIA Triad" – Confidentiality; Integrity; and Availability are a means of categorizing capabilities and controls to achieve security outcomes.[62] Confidentiality is about how information is kept private; Integrity means neither systems nor data have been improperly altered or changed without authorization; and Availability means that systems function as anticipated, systems are prompt, and services are accessible when authorized users attempt to access them.[63] Significantly, the PRM realizes that privacy concerns may develop even when a system is properly adhering to CIA protocol. Accordingly, the PRM fashioned three privacy engineering objectives meant to compliment but in no way supplant the three traditional CIA security information objectives.

The first privacy engineering objective, Predictability, means designing systems so that stakeholders are not surprised by the handing of personally identifiable information (PII).[64] Put another way, Predictability is the foundation upon which stable, trusted relationships between systems and individuals can be built. The second objective, Manageability, is viewed as a system property that enables several of the Fair Information Practice Principles (FIPPs).[65] The FIPPS were first established by an advisory committee to the Secretary of Health, Education, and Welfare and were the basis of the Privacy Act of 1974, which governs federal

al., *supra* note 60, at 8.

[62] Brooks et al., *supra* note 60, at 10.

[63] Eric P. Roberson, *"Adequate" Cybersecurity: Flexibility and Balance for A Proposed Standard of Care and Liability for Government Contractors*, 25 FED. CIRCUIT B.J. 641, 652 (2016).

[64] Brooks et al., *supra* note 60, at 18.

[65] *Id.* at 19.

agencies' collection and use of personal information.[66] In 1980 the FIPPs were revised by the Organization for Economic Co-operation and Development and became an internationally recognized set of privacy principles.[67] The principles are laudable from an objective privacy standpoint and include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[68] Using the PRM model, if an entity cannot administer individuals' information with sufficient granularity, it cannot be confident that inaccurate information can be identified and corrected, obsolete information disposed of, only necessary information is collected or disclosed, and that individuals' privacy preferences about uses of their information are implemented and maintained.[69] Disassociability, the third PRM objective, captures an integral element of privacy-preserving systems – that the system actively protects or "blinds" an individual's identity or associated activities from exposure.[70]

Even more than PbD, privacy engineering has vast potential ramifications for the protection of PII because its Disassociability objective may prevent or forestall the effects of new technologies aimed at re-identifying "anonymized" data. For instance, the concept behind the smart grid is, among other things, to upgrade the existing national electrical grid to allow for the greater use of modern technologies that provide two-way communication between

---

[66] J. Frazee, M. Finley, JJ Rohack, *Mhealth and Unregulated Data: Is This Farewell to Patient Privacy?,* 13 IND. HEALTH L. REV. 384, 401 (2016).
[67] *Id.*
[68] *Id.*
[69] Brooks et al., *supra* note 60, at 19.
[70] *Id.* at 20.

energy producers and energy customers, eliminate vulnerabilities to cyberattacks, reduce power outages, promote the efficient use of electricity, and reduce customer costs.[71] Presently, in most areas of the country, utilities only learn of a power outage when a customer calls to report it.[72] The smart grid enables utilities to identify outages, their cause, and the customers affected as soon as they occur.[73] This allows utilities to employ resilient solutions such as quickly rerouting electricity to customers ti reduce the impact of an outage.[74] Advanced smart grid technology also allows utilities to monitor the health of the grid proactively, allowing them to repair pending faults in advance.[75] Traditionally, personal data is organized into three categories: (1) customer-specific data, (2) customer-specific de-identified data, and (3) aggregated data representing community level information.[76] To be sure, customer-specific data generate the greatest privacy concerns because that data set contains personal information that can be traced back to specific individuals and households and therefore should be afforded the most protection.[77] For this reason, in

---

[71] Robert B. McKinstry Jr., Thomas D. Peterson, Steven Chester, *Unlocking Willpower and Ambition to Meet the Goals of the Paris Climate Change Agreement (Part Two): The Potential for Legal Reform and Revision*, 47 ENVTL. L. REP. NEWS & ANALYSIS 10135, 10148 (2017).

[72] Samuel J. Harvey, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. REV. 2068, 2072-73 (2014).

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] Megan McLean, *How Smart Is Too Smart?: How Privacy Concerns Threaten Modern Energy Infrastructure*, 18 VAND. J. ENT. & TECH. L. 879, 902 (2016).

[77] *Id.*

Colorado, a utility may not disclose customer data to third party entities, to include government agents, unless the customer first submits a signed "consent to disclose customer data form."[78] Accordingly, government agents cannot access consumer data without a warrant, subpoena, or court order.[79] The rationale behind the precautionary rule is because customer-specific de-identified data is customer-specific usage information that was stripped of PII yet still indicates single home usage. The problem is current limits of digital privacy protection make it impossible to discern whether a given piece of data was sufficiently de-identified to preclude the ability to re-identify it. Additionally, technological ability to manipulate data is constantly changing, which creates a genuine concern that data sufficiently de-identified today may be re-identifiable tomorrow.[80] Consequently, Colorado takes the sensible position that recognizes de-identified data presents the same threat to privacy as customer data and treats it identically.[81] The precautionary steps Colorado implements to prevent anonymized data from being re-identified could be helped by imbedding the PMR's Disassociability objective into the smart grid code.

III. DEVELOPMENTS IN CYBERSECURITY

A. Breaches

Computer networks constitute the nerve system of modern society. States, organizations, corporations, and

---

[78] 4 COLO. CODE REGS. § 723-3:3031.
[79] McLean, *supra* note 100, at 903.
[80] *Id.*
[81] *Id. See also* 4 Colo. Code Regs. § 723-3:3026(a).

individuals depend on information infrastructures for myriad uses to include commerce, communication, emergency services, energy production and distribution, mass transit, military defenses, and health services.[82] The centrality of digital technology in all facets of modern life coupled with the vulnerability of the selfsame technologies and infrastructures to threats and damage necessitates close attention to issues of cybersecurity broadly understood. As a recent study observed, cybersecurity incidents intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services people take for granted such as water, healthcare, electricity or mobile services.[83] Threats are diverse and can have different origins including criminal, politically motivated, terrorist or state-sponsored attacks, as well as natural disasters and unintentional mistakes.[84]

It is no surprise that the number and magnitude of data breaches continue to rise.[85] The Global State of Information Security Survey reports that the compound annual growth rate of detected breaches increased by 66% in the six years prior to 2015.[86] While the public may find an occasional data breach understandable, the actual prevalence

---

[82] Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 482 (2015).
[83] *Id.*
[84] *Id.*
[85] Open Security Foundation, *Data Loss Statistics*, DataLossDB, http://datalossdb.org/statistics (last visited Mar. 1, 2017) (data begins from 2007).
[86] *Security Incidents Continue to Rise in Cost and Frequency While Budgets Decrease, according to PwC, CIO and CSO's The Global State of Information Security® Survey 2015*, PWC, http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html (last visited March 1, 2017).

is surprisingly high and approximately one of five organizations will likely succumb to a material data breach in the next two years.[87] A brief survey of recent hacking events is eye-raising as hackers compromised the confidential account and financial information of 145 million eBay records; 130 million Heartland records; 76 million JPMorgan Chase client records; 80 million Anthem records; 77 million Sony records; 70 million Target records; and 56 million Home Depot records.[88]

The Federal Information Security Management Act of 2002 (FISMA) created a cybersecurity framework for federal information systems, with an emphasis on risk management, and required implementation of agency-wide information security programs.[89] Pursuant to FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing security standards for federal computer systems (aside from national security systems).[90] Each federal agency is responsible for complying with those standards and they report annually on the status of their information security to the Office of Management and Budget, which then reports to Congress.[91]

Given splashy news headlines about hacking results, it is perhaps not surprising that many consumers believe companies are not taking sufficient measures to prevent data breaches. By one estimate, 90% of the data breaches that happened in 2014 could have been prevented had the compromised entity followed industry "best practices."[92]

---

[87] Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get over It!*, 19 SMU SCI. & TECH. L. REV. 3, 12 (2016).
[88] *Id.*
[89] 40 U.S.C. §11331 (2012).
[90] *Id.*
[91] 44 U.S.C. §§3544-3545.
[92] *Id.*

And yet the tremendous increase in data breaches is coexistent with the fact that the amount of money spent protecting and securing data has consistently increased over the years.[93] In fact, global expenditure on information security is projected to reach over $100 billion by 2018.[94] Despite the spending increases, however, industry experts almost universally concede that throwing money at information security will not cure the pandemic because "data security systems are complex beasts, with multiple vulnerabilities and points of attack."[95]

B. Protecting Critical Infrastructure

Cyberattacks are occurring at a furious pace; from Sony to JP Morgan and the U.S. Office of Personnel Management, Saudi Aramco to the Ukraine crisis, cybersecurity is increasingly taking center stage in the diverse arenas of geopolitics, international economics, security, and law.[96] Yet despite the increasing proliferation of cyber events, the field of international cybersecurity law and policy remains relatively immature. For example, although there has been a relative abundance of scholarship exploring the contours of the law of cyberwarfare, less attention is paid to defining a law of cyber peace applicable

---

[93] *Id.*

[94] *Id.*

[95] *Id. See generally* Robert W. Hahn & Anne Layne-Farrar, *THE LAW AND ECONOMICS OF SOFTWARE SECURITY*, 30 HARV. J.L. & PUB. POL'Y 283, 288 (2006) (discussing the many different routes for attacking computers or networks).

[96] Scott J. Shackelford, J.D., Scott Russell, J.D., Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 3 (2016).

below the armed attack threshold at which point the law of armed conflict is activated.[97] As underscored by the International Court of Justice in the oft-cited *Nicaragua* case, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[98] Accordingly, cyber hostilities directed against

---

[97] *Id. See e.g.*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICATION TO CYBER WARFARE 17 (Michael N. Schmitt ed., 2013) (discussing when a cyberattack could trigger the right of self-defense); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 127 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009); David Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 17 J. CONFLICT & SECURITY L. 279 (2012); Emily Crawford, *VIRTUAL BATTLEGROUNDS: DIRECT PARTICIPATION IN CYBER WARFARE*, 9 J.L. & POL'Y FOR INFO. SOC'Y 1 (2012); Michael N. Schmitt & Sean Wattset, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 TEX. INT'L. L.J. 189 (2015); LTC Dean L. Whitford et al., JUDGE ADVOCATE GENERAL'S LEGAL CTR. & SCH., U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 29 (LTC William J. Johnson & LCDR David H. Lee eds., 2016); Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569 (2011); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010); Eric Talbot Jensen, *Future War and the War Powers Resolution*, 29 EMORY INT'L L. REV. 499 (2015).

[98] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. Rep.14, ¶ 202 (June 27)The case involved U.S. assistance to Nicaraguan guerrillas known as the Contras and the mining of Nicaraguan harbors. The case provided helpful jurisprudence on the scope of the prohibition on the use of force. The court reasoned "[t]here appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to

cyber infrastructure located on another state's territory, whether government owned or not, constitute a violation of that state's sovereignty.[99] Yet a critical unanswered question with respect to these sovereign rights and responsibilities is whether cyber operations that do not cause damage nor amount to an intervention nevertheless violate the targeted state's sovereignty.[100] Given the paucity of guidance in this critical arena, the U.S. has turned to strengthening its cyber defenses for critical infrastructure.

In 2009, President Obama declared Critical Infrastructure (CI) to be a "strategic national asset," though a fully integrated U.S. cybersecurity policy has yet to be established.[101] In 2013, Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity" provided for the creation of the NIST Cyber Security Framework, a voluntary set of standards in best security practices for critical infrastructure.[102] CI is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[103] In Framework Draft Version 1.1, released in January 2017, the authors explain

---

amount to" (*inter alia*) an actual armed attack conducted by regular forces, "or its substantial involvement therein." This description, contained in Article 3, paragraph g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. *Id.* at 14, ¶ 195.

[99] Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 274-75 (2014).

[100] *Id.* at 275.

[101] President Obama, *Remarks by the President on Securing our Nation's Cyber Infrastructure (*May 29, 2009).

[102] Exec. Order No. 13,681, 79 Fed. Reg. 63,491 (2014).

[103] *Id.*

that cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems and thus place the Nation's security, economy, public safety and health vectors at risk.[104] Extending the Framework's viability beyond CI, the authors posit that similar to financial and reputational risk, cybersecurity risk affects a company's bottom line as it can drive up costs, impact revenue, harm an organization's ability to innovate and to gain and maintain customers.[105]

C. Toward a Standard of Care

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of an organization's risk management processes.[106] The Framework consists of three components: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles.[107] Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.[108] The Tiers provide a mechanism for organizations to view and understand the characteristics

---

[104] Cybersecurity Framework, Draft Version 1.1, NAT. INST. OF STAND. & TECH., https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1.pdf
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*

of their approach to managing cybersecurity risk.[109]

The NIST Framework is important, in part, because even though its critics argue that it helps solidify a reactive stance to the nation's cybersecurity challenges, it is in fact spurring the development of a standard of cybersecurity care in the U.S. that plays into discussions of due diligence.[110] The NIST Framework harmonizes industry best practices to provide a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of CI in assessing and managing cyber risk. Although the NIST Framework is still relatively new, some private-sector clients are already receiving advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[111] In the relative near future, the NIST Framework has the potential not only to shape a standard of care for domestic critical infrastructure organizations but also to harmonize global cybersecurity best practices for the private sector writ large, given active NIST collaborations with a number of nations, including the U.K., Japan, Korea, Estonia, Israel, and Germany.[112]

---

[109] *Id.*

[110] Shackelford, *supra* note 120, at 27. *See* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. J. INT'L L. 287 (2015).

[111] Shackelford, *supra* note 120, at 27. *See also Why the NIST Cybersecurity Framework Isn't Really Voluntary*, Info. Sec. Blog (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

[112] Shackelford, *supra* note 120, at 27.

D. The Plight of Corporations

Corporations that are victims of cyberattacks perpetuated by a state actor have little options under domestic law. A state actor conducting hostile cyber operations against a corporation indeed violates the sovereignty of the host nation.[113] It matters not whether these activities were physically destructive as long as they were unlawful and detrimental.[114] A host state has multifarious options to respond to the aggressor state depending on whether the activity is an armed attack or something that falls beneath the level of an armed attack.[115] Yet, if states have options, what options might private entities possess? A state reacting to cyber hostilities will look to international law to regulate its response; in contrast, a corporation can only rely upon domestic law to justify its actions.[116] In addressing the immediate hostile cyber event, a corporation may only use protective measures that do not cause destruction or death to a hostile state actor's cyber agents or

---

[113] Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for A Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827, 1849 (2016). *See also* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 274-75 (2014) ("[H]ostile cyber operations directed against cyber infrastructure located on another state's territory, whether government owned or not, constitute, *inter alia*, a violation of that state's sovereignty...."); *see also* Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, Just Security (Dec. 17, 2014, 9:29 AM), http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea. For example, North Korea's cyber hostilities directed at Sony violated the sovereignty of the United States.

[114] Garrie, *supra* note 137, at 1850-51.

[115] *See generally* Schmitt, *supra* note 137.

[116] Garrie, *supra* note 137, at 1851.

infrastructure.[117] Further, the corporation must exercise caution and not pierce the sovereignty of the hostile state, an exercise in precision which can prove difficult in the borderless nature of cyberspace, since this would also be a violation of international law.[118] In other words, a state has the latitude to even preempt a cyberattack and has internationally-recognized authority to engage the hostile state in self-defense. On the other hand, a private entity's actions must be limited to the defensive rather than anticipatory or preemptive spheres and its response is capped at stopping the hostile state's cyber hostilities without violating international law.[119] In the end, private entities have few legal options that are consistently effective against

---

[117] *Id. See* U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT, at 4 (2010) (discussing the difficulties of cyberspace); Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, WINTER 2008-09, AT 60, 70 ("[I]nternational laws of war are...fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns.").

[118] Garrie, *supra* note 132, at 1851. Interestingly, the lack of meaningful national borders in cyberspace could lead to the theoretical situation where a private entity acts in self-defense against a hostile state actor's agents in cyberspace and the result is death or destruction in the host nation. As the use of force in self-defense is an exclusive right of state actors, the corporation would be in violation of the U.N. Charter's general prohibition on the use of force. *See* U.N. Charter art 2, ¶ 4. As a perverse result, under the law of state responsibility, the United States would be responsible for the corporation's violation of the hostile state's sovereignty. *See* G.A. Res. 56/83 (Jan. 28, 2002) (Responsibility of States for Internationally Wrongful Acts) This is the same result if a corporation is acting in self-defense and their response damages a third nation's cyber infrastructure or personnel. *Id.*

[119] *See generally* Dever & Dever, *Making Waves: Refitting the Caroline Doctrine for the Twenty-First Century*, 31 QUINNIPIAC L. REV. 165 (2013) (historical investigation into the norms of anticipatory self-defense of nations).

the variety of threats that they face.[120] Criminal enforcement is complicated by the lack of a consistently enforced international paradigm, complex jurisdictional issues, and the vexing problem of identifying an attacker in a manner specific enough to support criminal prosecution.[121] Civil litigation is similarly of questionable utility for two reasons: (1) the problem of anonymity in cyberspace and (2) the low likelihood of holding third parties liable in tort.[122]

IV. E-REPUBLIC

A. A Lively Past

In 1815 John Adams said to Thomas Jefferson, "What do we mean by the Revolution? The war? That was no part of the Revolution; it was only an effect and consequence of it. The Revolution was in the minds of the people . . . before a drop of blood was shed at Lexington."[123] If the Revolution had ideological origins when the original patriot Crispus Attucks fell during the Boston Massacre, the question of who has the right to vote continues to be a painful chapter in the history of the American experiment.[124] When surveyed about what rights are most valued under the Constitution, Americans invariably include the right to

---

[120] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J.L. & Tech. 429, 442 (2012).
[121] *Id.*
[122] *Id.*
[123] BERNARD BAILYN, THE IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION 1 (KNOPF 1967).
[124] Kevin Brown, Foreword: President Barack Obama Law & Policy Symposium, 35 T. MARSHALL L. REV. 1, 7 (2009).

vote.[125] As the Founders understood, an advantage of federalism is its parochial qualities because state and local governments draw voters into the political process.[126] Local, accessible government allows individuals to participate actively in governmental decision making and trains citizens in the techniques of democracy, fosters accountability among elected officials and enhances voter confidence in the democratic process.[127]

History can sometimes be a comfort because 2016 was not the first bruising, contentious American presidential election. Consider the election of 1800 between Thomas Jefferson and John Adams; the outcome of the contest was so bizarre that America had to amend its Constitution to make sense of new political realities.[128] Prior to ratification of the 12th Amendment, electoral college members each had two votes for president and whoever garnered the most votes was president while second place took the vice presidency.[129] When Jefferson and his Democratic-Republican running mate, Aaron Burr, tied with 73 votes, Federalist Party founder Alexander Hamilton famously sneered, "Mr. Burr loves nothing but himself –thinks of nothing but his own aggrandizement," which ultimately turned favor against Burr in the House and Representatives and led Jefferson to become president.[130] As fans of the

---

[125] Joshua A. Douglas, *Is the Right to Vote Really Fundamental?*,18 CORNELL J.L. & PUB. POL'Y 143, 145 (2008)
[126] Deborah Jones Merritt, *The Guarantee Clause and State Autonomy: Federalism for A Third Century*, 88 COLUM. L. REV. 1, 7 (1988).
[127] *Id.*
[128] Eliott C. McLaughlin, *10 of the Most Bizarre Elections in American History*, CNN Politics (March 4, 2016 8:26 AM), http://www.cnn.com/2015/10/30/politics/interesting-u-s-elections/).
[129] *Id.*
[130] *Id.*

smash hip-hop Broadway musical "Hamilton" know all too well, the antipathy between Hamilton and Burr continued for three more years until Burr killed Hamilton in a duel.[131]

Or consider the 1876 presidential campaign when Rutherford B. Hayes defeated his Democrat opponent Samuel J. Tilden by one electoral vote.[132] In a manner that presaged our modern salacious-driven news cycle, Hayes scorched Tilden with a series of broadsides calling him everything from a briber to a thief and drunken syphilitic.[133] Suspicion of voter fraud in Republican-controlled states was rampant while Jim Crowe-era marauders suppressed voter turnout in the South.[134] Consequently, Florida, Louisiana and South Carolina were deemed too close to call, and Tilden remained one electoral vote short of the 185 required to win. With 165 electoral votes tallied for Hayes, all he needed to do was capture the combined 20 electoral votes from those three contested states to win the presidency.[135] An ensuing crisis unfolded, starting with threats of a second civil war and ending with a backroom deal, the Compromise of 1877, that delivered the presidency to Hayes in exchange for the removal of federal troops from the South and the effective end of Reconstruction.[136]

---

[131] Chris Isidore, 'Hamilton' has best week ever for a Broadway show, CNN (November 30, 2016 1:12 AM), http://money.cnn.com/2016/11/29/media/hamilton-box-office-record/.
[132] John Copeland Nagle, *How Not to Count Votes*, 104 COLUM. L. REV. 1732 (2004).
[133] Gilbert Kin, *The Ugliest, Most Contentious Presidential Election Ever*, Smithsonian.com (September 7, 2012), http://www.smithsonianmag.com/history/the-ugliest-most-contentious-presidential-election-ever-28429530/.
[134] *Id.*
[135] *Id.*
[136] *Id. See generally* Nathan L. Colvin & Edward B. Foley, *Lost Opportunity: Learning the Wrong Lesson from the Hayes-Tilden*

In recent memory, the contest between George W. Bush and Al Gore in 2000 was a source of bitterness and anguish for many. As two scholars succinctly summarized in 2001, "[w]e live in extraordinary times. In the past year the Supreme Court of the United States has decided an election and installed a president."[137] On election night every major broadcast and cable news channel – ABC, NBC, CBS, CNN, MSNBC, and Fox News – all made and withdrew projections of Florida for both Bush and Gore.[138] At 3 a.m. on November 8, Gore conceded when Bush pulled 50,000 votes ahead and broadcasters put Florida's 25 electoral votes into Bush's win column.[139] But within two hours of Gore's concession, Bush's Florida lead had shrunk and the small margin triggered an automatic recount under Florida law.[140] Almost immediately, concerns about voting irregularities emerged in places like Palm Beach County, where a punch-card ballot with a format that was easily misread resulted in many disqualified votes.[141] A scant few days after the election, The New York Times ran a piece that explained what "chads" were to an anxious electorate:

Dispute, 79 FORDHAM L. REV. 1043, 1045 (2010).

[137] Jack M. Balkin & Sanford Levinson, *Understanding the Constitutional Revolution*, 87 VA. L. REV. 1045 (2001).

[138] Peter Marks & Bill Carter, The 2000 Elections: The Network Predictions; Media Rethink an Urge to Say Who's First, N.Y. TIMES (November 9, 2000), http://www.nytimes.com/2000/11/09/us/2000-elections-network-predictions-media-rethink-urge-say-who-s-first.html.

[139] Samantha Levine, Hanging Chads: As the Florida Recount Implodes, the Supreme Court Decides Bush v. Gore, US NEWS (January 17, 2008 5:00 PM), https://www.usnews.com/news/articles/2008/01/17/the-legacy-of-hanging-chads.

[140] *Id.*

[141] *Id.*

> The leadership of the free world may be decided by chads[,] . . . tiny bits of cellulose that, under the pressure of a citizen wielding his voting franchise and a metal stylus, are supposed to detach sharply from a punch-card ballot. The rectangular hole is interpreted as a vote by an electronic reader, while all unpunched holes are considered nonvotes. The problem with chads is that they often do not fully detach . . . Then they're called 'hanging chads,' and the computers can interpret them in various ways each time they are run through. The issue is significant in Florida because thousands of ballots were read by voting machines as having no vote in the presidential column. Democrats hope that when the paper cards are reviewed one by one, many will be seen to have partly punched holes next to Mr. Gore's name.[142]

For 36 days, who won the presidency was in limbo, as Bush and Gore were separated by a razor-thin margin, complicated by the "hanging chad" difficulties in Florida. On November 26, Florida Secretary of State Katherine Harris, who doubled as Bush's state campaign co-chair, certified voting results that gave Bush a minute 537-vote lead.[143] On December 12, the United States Supreme Court rendered its decision in a 5-to-4 vote which allowed the Harris vote certification to stand and delivered the presidency to Bush.[144] As one scholar noted, a delicious irony that surely John Marshall would have enjoyed emerged from the Court's decision in *Bush v. Gore*: we moved from a world in which the interpretive authority of the political

---

[142] Ford Fessenden, *Counting The Vote: The Ballots; After Cards are Poked, The Confetti Can Count*, N.Y. TIMES (Nov. 12, 2000), http://www.nytimes.com/2000/11/12/us/counting-the-vote-the-ballots-after-cards-are-poked-the-confetti-can-count.html.

[143] Levine, *supra* note 193.

[144] *Bush v. Gore*, 531 U.S. 98 (2000).

branches was clear and that of the Supreme Court questionable and uncertain, to one in which the Court's authority stood relatively unchallenged while that of everyone else is under siege.[145] Even years after the election, people were still dumbfounded with what to do with the punch cards [t]he contested . . . election has largely faded into people's hazy memories of pre-9/11 America. But the Florida ballots are still there, nearly six million punch cards and their chads, stowed in boxes, stacked on pallets, wrapped in plastic."[146]

B. E-Voters

In 1955, Isaac Asimov penned a short story that turned out to be less fantastic than his usual fare; in the not-so-distant-future, an advanced computer holding "trillions of items" of information determined the outcome of the 2008 presidential election.[147] In 2002, after the debacle of the "hanging chad," and with growing awareness of the limitations of digital technology to disrupt or upend an election, Congress passed the Help America Vote Act (HAVA), which was designed to help overhaul the nation's

---

[145] Larry D. Kramer, *The Supreme Court 2000 Term Foreword: We the Court*, 115 HARV. L. REV. 4, 15 (2001).

[146] Dana Canedy, *Florida Ponders Fate of Historic 2000 Ballots*, N.Y. TIMES (February 16, 2003), http://www.nytimes.com/2003/02/16/us/florida-ponders-fate-of-historic-2000-ballots.html?rref=collection%2Ftimestopic%2FPresidential%20Election%20of%202000&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=287&pgtype=collection.

[147] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 862 (2014).

election system in the wake of the 2000 election.[148] The HAVA seeks to promote the efficiency and accuracy of federal elections.[149] It establishes minimum standards for "voting systems" for federal elections and mandates that those systems generate a paper record of each vote that may be used in case of a recount.[150] Lastly, HAVA also requires each state to establish a central "computerized statewide voter registration list" to "serve as the official voter registration list" for all "elections for Federal office.

Perhaps because voting is essential to American democracy, many people have a false sense of security when it comes to the purported infallibility of e-voting. In truth, the technologists who designed the current generation of e-voting computers "weren't thinking about … system security . . . [Most machines] are a decade or older. Most . . . [run] Windows XP, for which Microsoft hasn't realized a security patch since April 2014 . . . [M]any of them are susceptible to malware, or equally if not more alarming, a well-timed denial of service attack."[151] When people think

---

[148] Tom Zeller, *Ready or Not, Electronic Voting Goes National*, N.Y. TIMES, September 19, 2004, http://www.nytimes.com/2004/09/19/politics/campaign/ready-or-not-electronic-voting-goes-national.html?_r=0. *See also* Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (2002) (codified as amended at 52 U.S.C. §§ 20901-21145).

[149] Michael T. Corely, *Dismantling the Unitary Electoral System? Uncooperative Federalism in State and Local Elections*, 111 NW. U. L. Rev. 103, 111 (2017).

[150] *Id.*

[151] Brian Barret, *America's Electronic Voting Machines are Scarily Easy Targets*, WIRED (August 2, 2016, 9:17 AM), https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election.

about hacking and e-voting, they usually imagine a switching results scenario, but hackers can do far less and still cause havoc; if machines are not working, or working slowly, that could create a host of problems and prevent individuals from casting a ballot.[152] To be clear, there is a host of new, more secure e-voting computers available than the machines most states bought in bulk a decade or more ago, but only a handful of states and municipalities such as Rhode Island, Washington D.C. and parts of Wisconsin upgraded their equipment in the year prior to the current election.[153] One e-voting expert explained why the states have failed to upgrade their machines: "[t]he money's not there right now. . . . [E]lection officials told us what they are hearing from their state legislators [who will not] be funding this type of equipment . . . they say come back to us after there's some kind of crisis. Perhaps this latest election cycle pushed the state of equipoise in favor of purchasing more secure equipment to protect the integrity of American democracy.

Yet no matter whether e-voting security measures are improved, nothing can guarantee a hack-free election. For this reason, it is important to consider what national policy should be in the face of international hacking. In the weeks after the 2016 election, a declassified report authored by the CIA, FBI, and NSA declared that the president of Russia, Vladimir V. Putin, personally "ordered an influence campaign in 2016 aimed at the U.S. presidential election," and turned from seeking to "denigrate" Hillary Clinton to developing "a clear preference for President-elect Trump."[154] Furthermore, the report did not back up claims

---

[152] *Id.*
[153] *Id.*
[154] David Sanger, *Putin Ordered 'Influence Campaign' Aimed at U.S.*

by the Trump campaign that the Russian-sponsored hacking activity had no effect on the election because "[w]e did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election," the report concluded, saying it was beyond its responsibility to analyze American "political processes" or public opinion.[155] The intelligence agencies did conclude "with high confidence" that Russia's primary military intelligence unit, the GRU, created a "persona" called Guccifer 2.0 and a website, DCLeaks.com, to release the e-mails of the Democratic National Committee and of the chairman of the Clinton campaign, John D. Podesta.[156]

By November 23, 2016, the Clinton campaign was urged by a number of premier computer scientists to call for a recount of vote totals in Wisconsin, Michigan and Pennsylvania.[157] The scientists thought they discovered evidence that vote totals in three states may have been manipulated or hacked.[158] Essentially, the researchers believed they a questionable trend of Clinton performing worse in counties that relied on electronic voting machines compared to paper ballots and optical scanners.[159] And while the group had not found any evidence of hacking, the unusual voter pattern warranted an independent review.[160]

Election, Report Says, N.Y. TIMES (January 6, 2017), https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.

[155] *Id.*

[156] *Id.*

[157] Dan Merica, *Computer Scientists Urge Clinton Campaign to Challenge Election Results*, CNN politics (November 23, 2016, 4:43 PM), http://www.cnn.com/2016/11/22/politics/hillary-clinton-challenge-results/.

[158] *Id.*

[159] *Id.*

[160] *Id.*

On January 7, 2017, President-elect Trump conceded that Russia and other countries were in fact trying to meddle in the election:

> "While Russia, China, other countries, outside groups and people are consistently trying to break through the cyber infrastructure of our governmental institutions, businesses and organizations including the Democrat [sic] National Committee, there was absolutely no effect on the outcome of the election including the fact that there was no tampering whatsoever with voting machines. There were attempts to hack the Republican National Committee, but the RNC had strong hacking defenses and the hackers were unsuccessful."[161]

Ultimately, Russian interference in the 2016 election may set the stage for a "new normal" of international interference. As the Intelligence community recently warned, "[w]e assess Moscow will apply lessons learned from its campaign aimed at the U.S. presidential election to future influence efforts in the United States and worldwide, including against U.S. allies and their election processes."[162] In a similar vein, the German government warned "there might be a Russian cyberattack on the federal election in Germany" this upcoming fall, based on the U.S. 2016 campaign troubles, and cautioned that the Bundestag itself

---

[161] *2016 Presidential Campaign Fast Facts*, CNN, January 9, 2017 1:52 PM, http://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/.

[162] David Ignatius, *Russia's Assault on America's Elections Is Just One Example Of A Global Threat*, WASHINGTON POST (February 23, 2016), https://www.washingtonpost.com/opinions/global-opinions/russias-assault-on-americas-elections-is-just-one-example-of-a-global-threat/2017/02/23/3a3dca7e-fa16-11e6-9845-576c69081518_story.html.

was "the focus of Russian intelligence interest."[163]

C. New Challenges

On February 27, 1968 renowned CBS news anchor Walter Cronkite, recently back from witnessing the destruction caused by the Tet Offensive in Vietnam, predicted on national television that the war would continue for years and end not in victory but rather a bloody stalemate.[164] President Johnson was stunned by Cronkite's pronouncement and declared "If I've lost Walter, I've lost middle America."[165] Putting aside the often cantankerous relationship between the current administration and large segments of the media, it is improbable, given the explosion of digital media in the past two decades, that a sitting president will ever again divine policy through the medium of a single albeit respected journalist.

The digital age has flattened communication; today the "Twitter in Chief" bypasses traditional news outlets and speaks out directly via his Twitter account.[166] Yet flattened communication is no panacea for a republic that requires well-informed citizens. Approximately 88% of Millennials get their news from Facebook, and due to the methodology of the Facebook newsfeed algorithm, users tend to receive more new stories similar to ones they clicked on in the

---

[163] *Id.*

[164] Peter W. Morgan, *The Undefined Crime of Lying to Congress: Ethics Reform and the Rule of Law*, 86 NW. U. L. REV. 177, 232 (1992).

[165] *Id.*

[166] See generally Amanda Wills and Alysha Love, *All the President's tweets*, CNN (February 26, 2017 6:42 AM), http://www.cnn.com/interactive/2017/politics/trump-tweets/.

past.[167] Unfortunately, this limited algorithm is built to please users; individuals only encounter biased "news" with which they are predisposed to agree. Ultimately, greater numbers of Millennials are consuming news in an "echo chamber," and that does not bode well for democracy. Many of the Founders – Jefferson, Madison, and Adams – believed a well-informed citizenry was essential for perpetuation of the American experiment.[168] In today's world, *Federalist 10* would appear on some newsfeeds but not others; Millennials, and indeed all generations, deserve better. A study of digital news consumers before the 2016 election revealed Democrats were more likely to visit left-leaning outlets like Daily Kos and The Huffington Post while Republicans visited conservative-aligned outlets like Fox News and Breitbart far more often than Democrats.[169]

The global village that was once the Internet has been replaced by digital islands of isolation that are grouping certain users while driving other users farther apart.[170] From parochial newsfeeds to tailored experiences on Google Search, the user experience is becoming increasingly personalized and the Internet a community of self-segregators.

---

[167] Anna Johansson, *5 Ways Millennial Social Media Habits Will Change In 2017*, FORBES, (November 29, 2016 2:36 PM), https://www.forbes.com/sites/under30network/2016/11/29/5-ways-millennial-social-media-habits-will-change-in-2017/#5f7f43be3219.
[168] Sandra Day O'Connor, *The Rule of Law and Civic Education Foreword* 67 SMU L. REV. 693, 699 (2014).
[169] Brendan Nyhan, Relatively Few Americans Live in Partisan Media Bubble, but They're Influential, N.Y. TIMES September 7, 2016, https://www.nytimes.com/2016/09/08/upshot/relatively-few-people-are-partisan-news-consumers-but-theyre-influential.html.
[170] Mostafa M. El-Bermawy, *Your Filter Bubble Is Destroying Democracy*, WIRED, (November 18, 2916 5:45 AM), https://www.wired.com/2016/11/filter-bubble-destroying-democracy.

V. CONCLUSION

There is a certain irony to be found in the fact that the internet, which allows almost unlimited access to information, has in practicality come to be utilized in a fashion where the users very often simply inhabit echo chambers of like-minded thought. In some ways, this may be because the sheer amount of information available is overwhelming and therefor unwieldy. Effectively sifting through the internet to correctly identify reputable sources representing diverse points of view is very difficult and requires time and a certain level of sophistication.

The 2000 and 2016 elections are apt bookends for an investigation into how the digital world has changed what it means to be an informed citizen. For all the concern about "Y2K," the world of the 2000 election was largely analog. Put differently, 2000 was as much ancient regime as it was a harbinger of things to come. From the perspective of 2017, technology offers so much to both the nation and the peoples of the world. It is no mere platitude to say the future is here but it is not equally distributed. How long would dictators remain enthroned in North Korea if the average inhabitant had unfettered access to the Internet? How might the Grameen Bank become widely digitized and help millions escape the bonds of poverty? Closer to home, citizens should not be blithely unaware of the dramatic changes technology has brought to their lives. It is unfortunate to see a family at a restaurant, together but not communing, the head of each member bent over a device and thumbs busily tapping out work e-mails or clicking on the latest viral YouTube video. Technology can sometimes be too ever-present. Most importantly, citizens must remember that the connected world has definite currents that tend to bind some groups and isolate others. For the Republic to stand, users must

reorganize the Internet to some degree according to principles of responsible citizenship. It is insufficient to protect e-votes from hacking; ballots must be cast from an informed position.