Giving Up On Cybersecurity
Kristen E. Eichensehr

ABSTRACT

Recent years have witnessed a dramatic increase in digital information and connected devices, but constant revelations about hacks make painfully clear that security has not kept pace. Societies today network first, and ask questions later.

This Essay argues that while digitization and networking will continue to accelerate, cybersecurity concerns will also prompt some strategic retreats from digital dependence. Individuals, businesses, and governments will “give up” on cybersecurity by either (1) adopting low-tech redundancies for high-tech capabilities or digital information, or (2) engaging in technological regression or arrest, foregoing capabilities that technology could provide because of concerns about cybersecurity risks. After cataloguing scattered examples of low-tech redundancy and technological regression or arrest that have occurred to date, the Essay critically evaluates how laws and regulations have fostered situations where giving up on cybersecurity is necessary. The Essay concludes by proposing ways that law can help to guide consideration of when to engage in low-tech redundancy or technological regression moving forward.

AUTHOR

Assistant Professor, UCLA School of Law. For helpful comments, I am grateful to participants in the Program on Understanding Law, Science, and Evidence (PULSE) conference on “Imagining the Legal Landscape: Technology and the Law in 2030.” Thanks to Andrew Brown for excellent research assistance.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>322</td>
</tr>
<tr>
<td><strong>I. Two Ways to Give Up on Cybersecurity</strong></td>
<td>323</td>
</tr>
<tr>
<td>A. Giving Up as a Response to Security Concerns</td>
<td>324</td>
</tr>
<tr>
<td>B. Giving Up So Far</td>
<td>327</td>
</tr>
<tr>
<td>1. Low-Tech Redundancy</td>
<td>327</td>
</tr>
<tr>
<td>2. Technological Regression or Arrest</td>
<td>330</td>
</tr>
<tr>
<td><strong>II. Law’s Push and Pull</strong></td>
<td>333</td>
</tr>
<tr>
<td>Conclusion</td>
<td>339</td>
</tr>
</tbody>
</table>
INTRODUCTION

Recent years have witnessed a dramatic escalation in digital information and connected devices. By some estimates, 90 percent of all data has been created in the last two years alone,¹ and the number of connected devices doubled between 2010 and 2015 and will double again or perhaps even quadruple by 2020.² The constant revelations about hacks of individuals, institutions, businesses, and governments, however, make painfully clear that security has not kept pace.³ Societies today network first, and ask questions later.

This Essay argues that while the next fifteen years will undoubtedly see the predicted dramatic expansions of digitization and networked technologies, they will also be marked by instances where cybersecurity concerns prompt some strategic retreats from digital dependence. Individuals, businesses, and governments will “give up” on cybersecurity by either (1) adopting low-tech redundancies for high-tech capabilities or digital information, or (2) engaging in technological regression or arrest, choosing to forego capabilities that technology could provide because of security concerns. Scattered examples of giving up on cybersecurity are occurring now, and they will and should become more frequent going forward.

³ ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 49 (2016) (“The history of cyberspace and cyber conflict is short, but the pace of history is rapidly accelerating. Whereas years or months once separated notable cyberattacks, now they come almost weekly, if not sometimes daily.”).
Law often stands on the sidelines as technology charges ahead, intervening only after a significant delay, and that is certainly part of the story of the last fifteen years. But sometimes law has pushed the adoption of technologies and digitization of information in circumstances where it now appears that giving up on cybersecurity may be a better option. Law’s role in pushing toward digital dependency suggests that it may also have a role to play in pulling back and guiding consideration of when to adopt low-tech redundancy or technological regression.

Part I of this Essay first defines “low-tech redundancy” and “technological regression or arrest.” Part I.A explains how these concepts respond to concerns about the confidentiality, integrity, and availability of information. Part I.B catalogues examples of low-tech redundancy and technological regression or arrest that have occurred so far. Part II then critically evaluates how laws and regulations have fostered situations where giving up on cybersecurity is necessary and proposes ways that law can help to guide consideration of when to engage in low-tech redundancy or technological regression moving forward.

I. Two Ways to Give Up on Cybersecurity

The concept of “giving up” on cybersecurity captures two distinct phenomena spurred by cybersecurity concerns. The first is “low-tech redundancy.” Low-tech redundancy involves deliberate decisions to retain low-tech or no-tech versions of capabilities or nondigital versions of content. The strategy of low-tech redundancy is not necessarily limited to the cybersecurity context. The New York Times recently reported that to address security concerns posed by drones, European officials are considering using trained eagles to intercept drones that appear to threaten, for example, airports or public gatherings—“a low-tech solution for a high-tech problem.” Stephen Castle, Dutch Firm Trains Eagles to Take Down High-Tech Prey: Drones, N.Y. TIMES (May 28, 2016), http://www.nytimes.com/2016/05/29/world/europe/drones-eagles.html?_r=2 [https://perma.cc/2MJV-A6RW] (quoting Sjoerd Hoogendoorn, the co-founder of the eagle program company, Guard From Above). The drone-hunting eagle program may be an example of low-tech redundancy: Dutch police detective chief superintendent Mark Wiebes explained to the Times that “subject to a final assessment,” eagles are “likely to be deployed soon in the Netherlands, along with other measures to counter drones,” such as “jamming drone signals.” Id.
rendered inaccessible, inoperable, or untrustworthy. When that occurs, the low-tech alternatives ensure resilience.\textsuperscript{5} They function as a failsafe, allowing continued operations and perhaps restoration of high-tech capabilities. Until cybersecurity fails, the high-tech and low-tech mechanisms proceed in parallel.\textsuperscript{6}

The second phenomenon is “technological regression or arrest.” Technological regression involves walking back from technological capabilities because of concern about the inability to properly secure the technology. Technological arrest is similar, capturing the deliberate decision not to proceed with developing a technical capacity because of security concerns. Technological arrest occurs when the security concerns are appreciated ex ante; technological regression occurs when the security implications are recognized only after the technology has been developed or deployed. Technological regression and arrest give up on cybersecurity in the sense that they assess that cybersecurity will fail and that the implications of that failure are sufficiently dire that the best course of action is to forego a technological capability entirely.

A. Giving Up as a Response to Security Concerns

Low-tech redundancy and technological regression and arrest respond to concerns about the confidentiality, integrity, and availability of data, which information security specialists often call the “CIA triad.”\textsuperscript{7}

A confidentiality problem involves access to data by individuals or entities that the owner of the data does not intend.\textsuperscript{8} Data breaches are confidentiality problems: criminals hack a business’s payment card system and obtain information, such as credit card numbers, that the business and individual


\textsuperscript{6} “High-tech” and “low-tech” are, of course, relative terms. As newer, more sophisticated technologies are developed, today’s high-tech will become the future’s low-tech. Today’s cars are high tech as compared to the Model T, which was high-tech as compared to horse-drawn carriages, but today’s cars will be low-tech when assessed against the future’s driverless cars.


\textsuperscript{8} See SINGER & FRIEDMAN, supra note 7, at 35 (discussing confidentiality).
card holders intend to keep confidential. Intellectual property theft is another example of a confidentiality problem: hackers steal trade secrets, whose very intellectual property protection depends on their status as confidential information.

Availability problems occur when data or systems are not accessible to authorized users when they are supposed to be. For example, in 2012 and early 2013, distributed denial of service (DDoS) attacks rendered the websites of numerous U.S. financial institutions inaccessible by flooding them with traffic and thereby preventing legitimate customers from accessing their accounts. Data or technological capabilities could also be rendered unavailable due to physical damage to technical systems. Imagine a physical attack that disables or destroys satellites used for the Global Positioning System (GPS).

Integrity problems may be even more pernicious than confidentiality and availability problems. Data integrity problems involve unauthorized changes to data. Integrity problems are particularly troubling because they are difficult to detect and once any integrity problem is discovered, it tends to cast doubt on the accuracy and reliability of all the other data on the system. The paranoia and time-consuming efforts to verify information that an integrity attack induces may be more damaging than the attack itself. Although attacks that compromise the integrity of data have been rarer than the widespread confidentiality and availability problems, they have occurred.

9. See id. (discussing availability).
11. See SINGER & FRIEDMAN, supra note 7, at 35 (discussing integrity).
12. Id. at 129 (arguing, in discussing attacks that compromise the integrity of military information, that “[u]nly a relatively small percentage of attacks would have to be successful in order to plant seeds of doubt in any information coming from a computer. Users’ doubt would lead them to question and double-check everything from their orders to directions. . . . The impact could even go beyond the initial disruption. It could erode the trust in the very networks needed by modern military units to work together effectively. . . .”).
One significant example occurred with the alleged U.S. and Israeli cyberattack against Iranian nuclear facilities. The operation, known as “Stuxnet,” infected Iran’s Natanz nuclear facility with malware and caused nuclear centrifuges to spin out of control, rendering them nonoperational. In addition to the physical damage, the code recorded the centrifuges’ normal operation, and then while the centrifuges spun out of control, it “sent signals to the Natanz control room indicating that everything downstairs was operating normally,” a feature that one U.S. official called “the most brilliant part of the code.” According to the New York Times, the Iranians became “so distrustful of their own instruments that they . . . assigned people to sit in the plant and radio back what they saw,” and they shut down entire “stands” of 164 centrifuges, looking for sabotage, when a few centrifuges failed. U.S. officials have recently begun sounding warnings about integrity attacks.

Low-tech redundancy primarily responds to concerns about availability and integrity. Governments, businesses, other organizations, and individuals may be forced to rely on redundant low-tech capabilities or paper backups where confidentiality, whereas denial-of-service operations and data deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.  


15. Id.

16. Id.

17. Id. Another example of an integrity attack occurred in 2007 when Israel bombed a Syrian nuclear facility. A cyber attack on Syrian air defense computer systems caused Syrian radar operators to see false images—one that did not reveal that Israeli planes had entered Syrian airspace—and “the air defense network never fired a shot.” Singer & Friedman, supra note 7, at 127.

18. See, e.g., James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Armed Serv. Comm., 114th Cong. 2 (2016), http://www.dni.gov/files/documents/SASC_Unclassified_2016ATA_SFR_FINAL.pdf [https://perma.cc/UD82-5G42] (“Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decisionmaking, reduce trust in systems, or cause adverse physical effects.”). Clapper, supra note 13, at 5 (warning about future attacks on data integrity); Katie Bo Williams, Officials Worried Hackers Will Change Your Data, Not Steal It, THE HILL (Sept. 27, 2015, 8:00 AM), http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it [https://perma.cc/9Y6Z-AXEY] (reporting on congressional testimony by National Security Agency Director Michael Rogers warning about future cyberattacks aimed at undermining the integrity of data).
when high-tech systems are unavailable due to a cyberattack or when cyber intrusions undermine confidence in the reliability of high-tech methods or digital data. Technological regression and arrest also respond to integrity concerns, and they may be used to address confidentiality problems as well. In circumstances where, for example, the accurate functioning of a particular device is crucial, fear that the device cannot be secured—that its data will not remain confidential and that hackers could manipulate the data—may prompt a decision that the device should not be networked or that it should not be used at all.

B. Giving Up So Far

Scattered examples of both low-tech redundancy and technological regression and arrest exist now and will become increasingly common in the coming years.

1. Low-Tech Redundancy

One striking example of low-tech redundancy has emerged from the U.S. Naval Academy. After a nearly twenty-year hiatus, the Academy has resumed teaching cadets to navigate by the stars due to concern about vulnerabilities in the systems that the U.S. Navy currently uses for navigation.\(^{19}\) The old-school navigation training will soon be expanded to enlisted personnel as well.\(^{20}\) The advent of GPS drove the abandonment of celestial navigation training in the 1990s.\(^{21}\) As Lieutenant Commander Ryan Rogers explained, the Navy “went away from celestial navigation because computers are great . . . The problem is . . . there’s no backup.”\(^{22}\) Knowledge about celestial navigation now serves as the backup. While experts have raised significant concerns about the security vulnerabilities of GPS,\(^{21}\) “you can’t hack a sextant.”\(^{24}\)

---


21. *Id.*

22. *Id.*

Another example of a shift to nondigital redundancy involves voting machines. In the wake of the controversy about “hanging chads” in the 2000 presidential election, jurisdictions across the United States moved to modernize their voting equipment, including by adopting electronic voting machines or direct record electronic machines.\(^{25}\) Almost immediately, computer scientists raised concerns about security vulnerabilities in electronic voting machines that could be exploited to tamper with election results.\(^{26}\) Some jurisdictions responded to the security concerns by establishing low-tech redundancy: a paper record of each vote cast electronically. In February 2003, Santa Clara County, which includes Silicon Valley, became the first U.S. county to purchase electronic voting machines that produce a voter-verified paper receipt.\(^{27}\) Later that same year, the California Secretary of State announced that beginning in July 2006, all electronic voting machines in California must produce a “voter verified paper audit trail.”\(^{28}\) Many other states have followed suit,\(^{29}\) adopting laws requiring a paper backup for ballots cast


26. See id. at 1734–36.


29. Some states have not engaged in low-tech redundancy (that is, paper backups), but instead have engaged in technological regression, abandoning electronic voting altogether in favor of a return to paper ballots. See, e.g., ELECTIONLINE.ORG, supra note 28, at 4 (discussing New Mexico’s return to paper ballots).
electronically. Some states have been slow to respond to security concerns: Only in 2015 did Virginia decertify WINVote touchscreen voting machines, which suffered from numerous severe security flaws and produced no paper backups. Other states still use vulnerable voting machines without paper backups. Concerns about hacking of voting machines have become increasingly urgent in light of the alleged Russian hacking of the Democratic National Committee and the release of stolen information in an apparent attempt to influence the presidential election.

A more quotidian example of low-tech redundancy is printing hard copies of important records or treasured photos. The last several years have seen a dramatic rise in ransomware—malicious software that encrypts a computer’s hard drive and renders the information on it permanently inaccessible unless the victim pays the attackers (often in Bitcoin) to restore access.


ware strikes not just individuals, but increasingly businesses, including hospitals,\textsuperscript{35} which have paid to restore access to electronic systems.\textsuperscript{36} Even Vint Cerf—one of the “Fathers of the Internet” and currently Google’s “Chief Internet Evangelist”\textsuperscript{37}—exhorted people to print important items. In a 2015 speech, he warned, “If there are pictures that you really really care about then creating a physical instance is probably a good idea. Print them out, literally.”\textsuperscript{38} The motivation for Cerf’s warning was not security so much as the march of technology and the possibility that future technology will lack the backwards compatibility necessary to read earlier file formats, effectively creating a digital “Dark Age” of inaccessible data.\textsuperscript{39} But the basic point is the same: low-tech redundancy in the form of paper copies of digital files as a way to mitigate the risks of inaccessibility or compromised integrity of digital files.

2. **Technological Regression or Arrest**

Examples of technological regression or arrest also run the gamut from issues of national security to corporate and consumer contexts.

In the wake of Edward Snowden’s revelations, Russia’s Federal Guard Service (FSO), which protects high-ranking Russian officials, reportedly ordered typewriters in an attempt to keep sensitive communications from being

---


\textsuperscript{38} Id.
electronically surveilled. An FSO source explained to the Russian newspaper Izvestiya that “the practice of creating paper documents will expand.” The technological regression may not be limited to Russia. A German member of parliament who heads a parliamentary inquiry into National Security Agency activities said in an interview that “he and his colleagues were seriously thinking of ditching email completely,” and when asked whether they considered typewriters, he replied, “As a matter of fact, we have—and not electronic models either.”  

Technological regression goes beyond communications technologies. The rapid increase of a wide range of networked devices as part of the “Internet of Things” is prompting cybersecurity concerns related to everything from medical devices to children’s toys to cars. One example of technological regression came to light in a 2013 60 Minutes interview with former Vice President Dick Cheney. Cheney disclosed that “his doctor ordered the wireless functionality of his heart implant disabled due to fears it might be hacked in an assassination attempt.” Cheney’s revelation shows technological regres-

41. Id. (quoting a source inside the Federal Guard Service).
sion for one medical device, but regression on a broader scale might occur as a result of regulation or in the wake of an incident of patient harm from hacking of a medical device.

Similarly, consumers may drive demand for regression in some instances. For example, German researchers in March 2016 released a study showing that twenty-four different models of cars from nineteen manufacturers are vulnerable to a “radio ‘amplification attack’ that silently extends the range of unwitting drivers’ wireless key fobs to open cars and even start their ignitions,” greatly facilitating car theft. 47 Although consumers undoubtedly enjoy the convenience of keyless entry and ignition, cybersecurity concerns might push at least well-informed consumers to demand old school, physical car keys. 48

While technological regression involves undoing a technological capability in response to security concerns, examples of technological arrest are characterized by a deliberate decision not to go high-tech—not to network a device, not to create a digital file—due to security concerns. 49 For example, in the wake of the 2014 cyberattack on Sony Pictures, Hollywood studios are working to improve their cybersecurity. 50 Some of the techniques involve using more sophisticated technology, like encryption, to secure digital copies of movie scripts, but other techniques involve technological arrest. According to reports, “[t]he most-coveted scripts are still locked in briefcases and ac-


48. As just one example, in response to an article about the radio amplification attacks, Shawn Henry, the president of cybersecurity firm Crowdstrike Services, tweeted, “My ignition key worked pretty well for the past 30 years. Maybe we don’t need to incorporate tech into EVERYTHING!” Shawn Henry (@Shawn365Henry), TWITTER (Mar. 23, 2016, 8:36 AM), https://twitter.com/Shawn365Henry/status/712619038531189876 [https://perma.cc/Z6TQ-AM32].

49. See, e.g., Darren Samuelsohn, GOP Shuns Electronic Ballots at Open Convention, POLITICO (May 1, 2016, 4:56 PM), http://www.politico.com/story/2016/05/gop-convention-ballots-technology-222472 [https://perma.cc/7VAZ-PH5W] (reporting that senior Republican party officials “ruled out a change to convention bylaws that would allow for electronic voting on” presidential and vice presidential nominees due in part to concerns about hacking); Schneier, supra note 33 (arguing against Internet voting due to cybersecurity concerns).

companied by bodyguards whose sole job is to ensure they don’t end up in the wrong hands.\textsuperscript{51}

The Apple-versus-FBI dispute over access to the iPhone of one of the San Bernardino shooters provides another technological arrest example. In February 2016, a magistrate judge in the Central District of California ordered Apple to assist the FBI in accessing the iPhone by writing software that would, among other things, override a feature of the phone that caused it to auto-erase after ten incorrect attempts to guess its passcode.\textsuperscript{52} Apple raised many legal and policy objections to the court’s order,\textsuperscript{53} and one is essentially an argument for technological arrest.\textsuperscript{54} Specifically, Apple argued that the court’s order would require “Apple to design, create, test, and validate a new operating system that does not exist, and that Apple believes—with overwhelming support from the technology community and security experts—is too dangerous to create.”\textsuperscript{55} Apple cited the risks that the code would be leaked or stolen by hackers as a reason for its refusal to write the code in the first place.\textsuperscript{56}

\textbf{II. LAW’S PUSH AND PULL}

Numerous drivers have pushed the digital revolution and increased dependence on technology. Businesses and governments adopt technology because it improves efficiency and gives them new capabilities. Customers

\textsuperscript{51} Id.
\textsuperscript{53} See Apple Inc’s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government’s Motion to Compel Assistance at 14-35, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Feb. 25, 2016) [hereinafter Apple Brief], https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-Apple-Motion-to-Vacate-With-Declarations.pdf.
\textsuperscript{54} Id. at 2.
\textsuperscript{55} Apple Inc.’s Reply to Government’s Opposition to Apple Inc.’s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search at 16, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Mar. 15, 2016) [hereinafter Apple Reply Brief], https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-CDCal-Apple-Reply.pdf; \textit{see also} Apple Brief, supra note 53, at 2 (arguing that the court’s order “compels Apple to create a new operating system—effectively a ‘back door’ to the iPhone—that Apple believes is too dangerous to build”).
\textsuperscript{56} Apple Reply Brief, supra note 55, at 19–20.
seeking convenience or just the coolest new device form a vast market for high-tech gadgets, mobile phones, and tech-dependent services. Companies seeking to capture pieces of these highly lucrative markets rush products onto (often digital) shelves, fiercely competing with similarly situated firms. Because of these interests, adoption of technologies often occurs before full consideration of their security implications. As the examples of low-tech redundancy and technological regression and arrest show, demands for efficiency, convenience, and greater capabilities often lead to adoption first, careful consideration later.

Law and regulation are at least complicit in this situation. Law often lags behind technology, only belatedly catching up to a technology’s implications and uses after the technology has been deployed. But in some circumstances, laws and regulations are partially to blame for creating the situation in which dependence on technology outpaces efforts to secure it. Government entities sometimes adopt technologies themselves without fully considering security problems. Consider, for example, the electronic voting machines that jurisdictions across the United States approved and purchased without appreciating that they could be hacked and compromise the integrity of elections and voter confidence in the electoral process. Another example is the federal government’s adoption of electronic processing of security clearance investigations, including electronic security clearance forms and digital fingerprints.57 This information was stored in a centralized database that China compromised in last year’s hack of the Office of Personnel Management.58


wake of the intrusion, the government reverted to hard copy security clearance applications, at least temporarily.\footnote{59}

Sometimes the government has also mandated or provided incentives for other entities to adopt technologies. One example is digitization of medical records. Passed as part of the American Recovery and Reinvestment Act of 2009,\footnote{60} the Health Information Technology for Economic and Clinical Health (HITECH) Act\footnote{61} “established incentive programs for eligible hospitals and professionals adopting and meaningfully using certified electronic health record . . . technology.”\footnote{62} Regulations issued under the Act provide for incentive payments under Medicare and Medicaid to health care providers that meaningfully use electronic health records, but the regulations also provide for decreased Medicare payments to providers who fail to meet electronic health record standards.\footnote{63} Although these laws were a well-intentioned attempt to improve efficiency and patient safety,\footnote{64} they have also pushed hospitals toward dependence on digital records that are now subject to hacks and ransomware attacks.\footnote{65}

On the upside, the fact that laws and regulations are partly responsible for pushing toward digital dependency suggests that they may also be able to play a constructive role in pulling back from it in narrowly tailored and strategic

\footnote{64}{See President Barack Obama & Vice President Joe Biden, Remarks by the President and Vice President at Signing of the American Recovery and Reinvestment Act, WHITE HOUSE (Feb. 17, 2009), https://www.whitehouse.gov/the-press-office/remarks-president-and-vice-president-signing-american-recovery-and-reinvestment-act [https://perma.cc/F5YW-9UWC] (explaining the American Recovery and Reinvestment Act as “an investment that will take the long overdue step of computerizing America’s medical records to reduce the duplication and waste that costs billions of health care dollars, and medical errors that cost thousands of lives each year”).}
\footnote{65}{See supra note 35 and accompanying text.}
ways. Setting aside legal regulation to improve cybersecurity and the debates that accompany it, law and regulations could help to require or incentivize giving up on cybersecurity via low-tech redundancy or technological regression.

Examples of laws mandating low-tech redundancy are easy to imagine and in some cases already exist. For example, the same jurisdictions that passed laws or ordinances requiring electronic voting machines could just as easily require all voting machines to produce a paper backup.\textsuperscript{66} Similarly, the laws and regulations that incentivize digitization of medical records could mandate or provide incentives for health care providers to produce periodic paper backups of at least some documents, for instance, patient allergy information. Laws could similarly incentivize individuals to maintain low-tech capabilities. Ownership of self-driving cars could be contingent on the owner obtaining a driver’s license for conventional cars. None of these legal moves would abandon the advantages of digitization or new technology, but they would preserve low-tech redundancy that could be drawn upon if the high-tech options were destroyed, made inaccessible, or rendered untrustworthy.

Laws and regulations could similarly foster consideration of technological regression. For industries that are already regulated, agencies could require a risk assessment for networked devices that would specifically evaluate whether the benefits of the networking outweigh the security risks. Forcing explicit consideration of cybersecurity risk could push companies toward technological regression. Examples in this category might be the Food and Drug Administration’s regulation of medical devices,\textsuperscript{67} and the National Highway Traffic Safety Administration’s regulation of motor vehicle safety.\textsuperscript{68}

In addition to federal government agencies, state laws and regulations might provide other avenues for prompting companies to consider technological regression explicitly. States and state attorneys general in particular have been active in protecting consumer privacy through mechanisms such as state data breach notification statutes.\textsuperscript{69} Many have consumer protection-focused mandates.

\textsuperscript{66} See supra notes 28 and 30 and accompanying text.


as well.\textsuperscript{70} States might issue guidance or provide incentives or mandates for consumer product companies that sell networked devices to consider device security. They might even require product manufacturers to preserve the ability to de-network consumer products and to disclose to consumers how to de-link devices from the Internet. To be sure, such a requirement would pose practical challenges, including how to provide the information to consumers and whether the information on de-linking the device could be communicated in a sufficiently understandable way for the average consumer to follow the instructions if he or she chose to do so.\textsuperscript{71}

Another way law could incentivize consideration of low-tech redundancy or technological regression is by incorporating such consideration into the standard of care for what constitutes reasonable cybersecurity. For the last decade,\textsuperscript{72} the Federal Trade Commission (FTC) has brought administrative actions against companies that demonstrate weak cybersecurity with respect to customer data. The FTC actions are based on Section 5 of the Federal Trade Commission Act’s prohibition on “unfair or deceptive acts or practices in or affecting commerce.”\textsuperscript{73} The Commission’s authority to regulate inadequate cybersecurity pursuant to Section 5 received a significant boost in 2015 when the Third Circuit Court of Appeals rejected a challenge to the FTC’s authority by Wyndham Hotels, which was the subject of an FTC enforcement action after three data breaches compromised credit card information of more than 619,000 customers and resulted in “at least $10.6 million” in fraudulent charges.\textsuperscript{74} Most of the FTC’s more than fifty enforcement actions


\textsuperscript{71} Some of these challenges occur with respect to privacy policies for connected devices, which do not even attempt to convey technical information about how to alter a device’s functions. See Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 TEX. L. REV. 85, 140–43 (2014).

\textsuperscript{72} For an overview of the FTC’s history of data security enforcement actions, see GINA STEVENS, CONG. RESEARCH SERV., THE FEDERAL TRADE COMMISSION’S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 7–8 (2014), http://fas.org/sgp/crs/misc/R43723.pdf (tracing the history of FTC data security enforcement actions beginning in 2006).


\textsuperscript{74} Fed. Trade Comm’n v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).
have resulted in settlements, and the settlements focus on companies’ failure to employ basic cybersecurity practices, such as requiring secure passwords and keeping software updated.

In the future, the FTC’s understanding of what counts as “unfair” practices could evolve to include maintenance of low-tech redundancy and consideration of technological regression. For example, in response to a wave of attacks that renders customer services unavailable—think inability to access personal health tracking data or travel reservations—the Commission could come to regard a company’s failure to maintain low-tech redundancy in the form of paper backups or other means for continued customer access to data as an unfair practice. In other words, the failure to maintain continuity of operations during a cyberattack—including through low-tech redundancy—could be understood to be an unreasonable cybersecurity practice and one that is unfair to consumers.

The FTC might also address technological regression as an extension of existing concerns about unnecessary collection of consumers’ data. The FTC already advises businesses to avoid collecting personal information they do not need and to retain consumers’ personal data only for as long as there is a legitimate business need for the data. The FTC has highlighted these “data minimization” best practices specifically in connection with the Internet of Things. The Commission gave an example of a wearable device that tracks a health condition and has the ability to monitor the wearer’s physical location. The Commission suggests that until the company needs the geolocation information for a future product feature that would allow users to find medical care near their location, the company should not collect the location data. The FTC’s example could be understood to push for consideration of technological regression: The wearable technology company would turn off a feature of the device absent a business need that would justify collecting data.

76. Id. at 4–5, 12.
77. Id. at 2.
79. Id. at 36.
80. Id.
and thereby putting it at risk of compromise.\textsuperscript{81} It is worth emphasizing that under the FTC’s current approach, the existence of a business need for data appears sufficient to justify its collection. A full embrace of consideration of technological regression, on the other hand, might change the analysis so that the mere existence of a business need for data is not necessarily sufficient; rather the reasonableness of a company’s practices could turn on a balancing between the cybersecurity risks of a technology and the benefits it provides to consumers.

CONCLUSION

The website of “I Am The Cavalry”—a “grassroots organization” focused on the intersection of computer security and public safety\textsuperscript{82}—notes that “[a]s the question around technology is less-and-less ‘can we do this’ we must more-and-more be asking ‘should we do this.’”\textsuperscript{83} As the examples of low-tech redundancy and technological regression suggest, sometimes that answer should be “no.” Going forward, legal institutions from executives to legislatures to regulatory agencies should consider whether low-tech redundancy should be maintained alongside high-tech capabilities and digital data and whether in limited circumstances, the convenience, efficiency, and other benefits of a technology might not overcome the cybersecurity risks that it poses.

Discussions of technological progression don’t often end in discussions of technological regression. But maybe they should.

\textsuperscript{81} Fed. Trade Comm’n, supra note 75, at 2 (highlighting security risk to unnecessarily collected and retained data); FTC Staff Rep., supra note 78, at 34-35 (explaining that collection and retention of unnecessary data increases security risk because “[l]arger data stores present a more attractive target for data thieves”).

\textsuperscript{82} Executive Summary, I Am The Cavalry, https://www.iamthecavalry.org/about/overview [https://perma.cc/8SCE-BPBC].

\textsuperscript{83} Id.