CYBERSECURITY AS A LEGAL PROBLEM

Josh A. Goldfoot*

August 2023

Cybersecurity isn't just a technical problem. It's a social problem as well. Law is the foundation of cybersecurity because law defines the "security" in cybersecurity, who is entitled to that security, and how human beings and governments should behave to guarantee cybersecurity.

Cybersecurity law has many silos. If a teenager's private photo is hacked from Google Drive, lawyers think about anti-hacking statutes like the Computer Fraud and Abuse Act. If the U.S. government seeks access to the same photo from the same account, lawyers think about the Fourth Amendment and criminal procedure rules like the Electronic Communications Privacy Act. If the British government seeks access to that photo, lawyers think about mutual legal assistance treaties and the CLOUD Act. If the Russian government accesses that photo, lawyers think about national security law. If Google were to launch a new social network that automatically shares its users' photos, lawyers would think about privacy policies and privacy statutes. Cybersecurity law is the intersection of all those silos; it is the law of who may control which computer.

Cybersecurity is both a technical problem and a social problem. Network defense is the technical half of cybersecurity, but law is the social half. While regulating how computers behave is an important part of cybersecurity, regulating how humans and governments behave is just as important. Law is the

* Principal Deputy Chief, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice; J.D., University of Virginia, 1999; B.A., Yale University, 1996. All statements of fact, opinion, or analysis expressed are mine and do not necessarily reflect the official positions or views of the Department of Justice or any other U.S. government agency. Nothing in the content should be construed as asserting or implying U.S. government authentication of information or agency endorsement of the author's views. I am grateful for being invited to the 2022 Cybersecurity Law and Policy Scholars Conference, where this paper received helpful feedback from many participants, including Steven Bellovin, Anne Boustead, Jeff Kosseff, Asaf Lubin, Riana Pfefferkorn, Alan Rozenshtein, Chinmayi Sharma, and Felix Wu.

foundation of cybersecurity because law defines the "security" in cybersecurity, who is entitled to that security, and how human beings and governments should behave to guarantee cybersecurity.

The first section of this paper explains how cybersecurity is a legal concept. Cybersecurity exists when the people who can control computers and information are the people that law says ought to control those computers and information. Computers are controlled by whoever succeeds in getting them to execute commands. Computers execute commands without regard to whether these commands are given by their owner, a government, a technology company, or a hacker. Law is used to depart from this technological default. While cybersecurity laws fall into several different disciplines—criminal prohibitions on hacking and privacy laws, for example—those laws nonetheless are similar in that they all reflect normative decisions to depart from the way technology by default orders who may control which computer. Often those normative decisions are motivated by moral values, principally the frequently competing values of *autonomy*, which values personal choice and freedom, and *collectivism*, which values the overall health and utility of the network.

The second section demonstrates these principles by analyzing cybersecurity between government and citizens—that is, civil liberties. How civil liberties protections apply to computers is a notoriously complex question. One cause of that complexity is that civil liberties questions are often also cybersecurity questions. The Supreme Court's 2018 *United States v. Carpenter* decision, about obtaining a defendant's location information from cell phone companies, demonstrates how some Fourth Amendment questions are cybersecurity questions, questions about when police may exercise control over computers and the information they contain. The majority in that case used the Fourth Amendment to bestow upon defendants a degree of legal control over mobile phone network computers, valuing personal autonomy. The dissenters, meanwhile, promoted a view of the Fourth Amendment that advanced a collectivist, technology-focused view of cybersecurity.

The third section analyzes cybersecurity between nations. Nations make different legal judgments about who ought to control which computer, and conflicts arise from those legal differences. It's even possible to measure a nation's cybersecurity by the strength of its law, but only if it can use its law to influence who accesses which computer. Nations use law not just to define cybersecurity but also to secure control over other nations' computers and to block foreign nations' control over their own computers. Democracies enjoy a cybersecurity advantage over other nations because their stronger, more trustworthy legal systems generate confidence in the cybersecurity of computers and information within their borders. One legal technique in particular—domestic online disruption operations—strikes at the heart of the competing moral values at the center of cybersecurity.

CYBERSECURITY AS A LEGAL PROBLEM

Cybersecurity Defined and Redefined

Ask professionals to define cybersecurity, and most will define it along the lines of the federal government's official definition: "the art of protecting [computers] from unauthorized access or criminal

use and the practice of ensuring confidentiality, integrity, and availability of information."[1] That's an incomplete definition. What access is "unauthorized," what use is "criminal," from whom should information be kept "confidential," and who decides if information has integrity or is sufficiently available? In short, who is entitled to control which computer? Any definition of cybersecurity depends on a shared understanding of rules that define ownership, authorization, and control. Those rules are laws.

With this appreciation for law's role in cybersecurity, we can redefine cybersecurity, without much simplification: ***Cybersecurity exists when the people who can control computers and information are the people that law says ought to control those computers and information.*** Cybersecurity problems occur whenever those two groups of people—those who can control, and those whom the law permits to control—are different.

Cybersecurity is as much a legal concept as it is a technical concept. Yes, when a hacker penetrates a bank, the bank has a cybersecurity problem: The law said only the bank gets to control its computer, but the reality was different. But Timothy Carpenter also had a cybersecurity problem.[2] Carpenter robbed stores while carrying a cell phone. His computer—that is, his phone—in concert with the phone company, generated information about his location, and Carpenter wanted to ensure that information's confidentiality. But the cell phone company, not Carpenter, had technological and physical control over that information. The police, in turn, took indirect control over that information using a court order but not a search warrant. Thus, Carpenter, similar to the bank, had a cybersecurity problem: From his point of view, the Fourth Amendment said police without warrants could not control his location information, but the reality was different. In deciding that the Fourth Amendment prohibited the police's access, the Supreme Court was defining what unauthorized access meant.

HiQ Labs also had a cybersecurity problem.[3] HiQ scraped public profiles from LinkedIn and analyzed that data for profit. HiQ's cybersecurity problem arose when LinkedIn blocked hiQ from scraping its site. LinkedIn used a technological measure (Internet Protocol address blocking) and legal measures (a cease-and-desist letter) to try to deny hiQ access to LinkedIn profiles. HiQ sued, claiming LinkedIn had violated California's unfair competition statutes. This, again, was a cybersecurity problem, because hiQ believed the unfair competition statutes said hiQ could access LinkedIn's computers, but the reality was different. Resolving that legal dispute requires resolving the cybersecurity question of whether hiQ is authorized to access LinkedIn's servers or not.

---

[1] Cybersecurity & Infrastructure Security Agency, "What Is Cybersecurity?" May 6, 2009, https://perma.cc/6GP5-S3L2.

[2] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[3] *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022).

Cybersecurity Orderings and Legal Patches

Technology, on its own, dictates one set of rules about who can control which computer. I call this set of rules the default cybersecurity ordering. A cybersecurity ordering is a set of rules about who controls which computer, and the default cybersecurity ordering is that those who can control a computer may do so. That is, the default cybersecurity ordering is the ordering defined by physics, computer code, and nothing else.

Identifying the default cybersecurity ordering requires disregarding legal rules concerning control over computers. Contract law is irrelevant: That a cloud computing provider has contracted with customers not to read their data does not change the technological fact there are no technological barriers to the provider doing just that. Property law is irrelevant: How law assigns ownership of a computer does not change the technological reality of who is able to control that computer. Physical possession is relevant, because possessing a computer does allow a good degree of control, but physical possession of a computer does not equate to being in total control. After all, control over a computer is in the hands of whoever can program or configure the computer; usually, that means power goes to manufacturers, operating system publishers, cloud computing services, application developers, and hackers, with whatever power that remains going to the computer's physical possessor. That many of those parties are prevented by law from controlling the computer, or are prevented by good business sense from exercising control unwisely, is irrelevant to the default cybersecurity ordering.

The default cybersecurity ordering is frequently undesirable. So policymakers adjust the rules that define ownership, authorization, and control to correct undesirable outcomes that technology, on its own, would otherwise dictate. Think of this as using law to patch the default cybersecurity ordering, creating a new cybersecurity ordering. The simplest example of a legal patch is an anti-hacking statute like the Computer Fraud and Abuse Act,[4] which prohibits certain actions that are made without authorization or exceeding authorized access.[5] Anti-hacking statutes reflect that network defense is imperfect; it's not possible or cost effective for computer owners to perfectly implement their intended authorization restrictions through technological means.[6] Anti-hacking statutes provide a second layer of prohibition: When the computer itself fails to stop an undesired access, the law can punish that access, and, knowing of the legal prohibition, those who are capable of making the undesired access will hopefully be deterred or at least punished. The law acts as a patch, preventing accesses that technology, on its own, would permit.

---

[4] 18 U.S.C. § 1030.

[5] See, generally, Justice Manual § 9-48.000(B), https://perma.cc/55R6-L2PX.

[6] Josh Goldfoot & Aditya Bamzai, "A Trespass Framework for the Crime of Hacking," *George Washington Law Review* 84 (2016): 1487.

Law also corrects situations when the default cybersecurity ordering would give owners or possessors of computers too much control. Sometimes, law offers the only protection against undesirable control. Users of cloud computing and many online services depend on computers that they do not own or possess. Technologically speaking, an Amazon Web Services user is completely at Amazon's mercy; Amazon can delete, forge, block, and often read whatever it likes, thanks to Amazon's total control of the Amazon servers, the software running on them, and the network attached to them. Law, however, provides a layer of protection. It permits Amazon to make credible, enforceable promises to its users that it will refrain from exercising its total technological control. Contracts like these are patches, just like anti-hacking statutes are patches: They create a new set of rules about who controls which computers and which data, rules that are dictated not by technology but by law.

Anti-hacking statutes and cloud service contracts are alike in that they patch the default cybersecurity ordering to disable access. But patches can also enable access when the default cybersecurity ordering provides someone with too little control. An example is the U.S. Court of Appeals for the Ninth Circuit's recent decision in *hiQ Labs, Inc. v. LinkedIn Corporation*, discussed above. The Ninth Circuit held that LinkedIn might have violated a California unfair competition statute when it used IP address blocking to prevent a competitor, hiQ, from accessing LinkedIn's website. Thus, according to the Ninth Circuit, California's unfair competition statute is an access-enabling patch: Technology, on its own, permitted LinkedIn to single out hiQ and block hiQ's IP address, but a statute modified that default ordering and gave hiQ the ability to access LinkedIn from its IP address, after all.

Legal rules that permit the police to control computers—or, at least, to indirectly access data stored on them—are also examples of patches that enable access. Legal rules that permit government investigators to hack computers, or to compel providers to produce stored data (as in *Carpenter*), or to compel providers to assist the government in implementing a wiretap or a pen trap are all rules that allow the government to control computers—control using law, rather than technology. Each of these legal rules reflects a policy decision that, in some circumstances, the default cybersecurity ordering doesn't permit the right people to control some computers. Compulsory process is a legal patch to the cybersecurity ordering: Although compulsory process does not put anyone in technological control of anyone else's computer, compulsory process can force targets to access their computers and produce information, or to assist the government in accessing it. Legal rules can also require product designs that enable access. In these ways, law redefines who may control a computer to access information stored on it.

Cybersecurity, then, is intertwined with normative judgments. The "security" in cybersecurity is a subjective question about which people might disagree. Network security concepts of information confidentiality, integrity, and availability depend on a point of view about law. From LinkedIn's point of view, the law permitted LinkedIn to block whomever it chose, so LinkedIn's servers were secure from hiQ when LinkedIn blocked hiQ. From hiQ's point of view, it had a legal right to access LinkedIn's servers and LinkedIn impaired their availability to hiQ. Similarly, from Carpenter's point of view, the Fourth Amendment protected his location information from government agents without search warrants. Cybersecurity, then, is more than network defense—that is, it is more than just an objective technical

question of whether a network owner has succeeded in achieving confidentiality, integrity, and availability. Instead, cybersecurity is a normative question about whether the right people have control.

Property, Reserved Control, and Product-Design Patches

In theory, owning a computer comes with the right to control it, much like owning a bicycle or a bank vault comes with the right to control. But controlling computers differs from controlling other property. Computers follow their programming, so they are controlled by their programmers and not necessarily by their owners. Owners have some say in what programs their computers run and in what commands are given to them, but owners nonetheless are forced, as a practical matter, to use software that other people wrote.

Whose software runs on a given computer, in turn, is a hard-fought battle. Companies compete to lash their preferred operating systems, cloud services, app stores, and application software to a given user's computer. The winner of that competition sometimes has control over the computer's most fundamental operations and access to all or most data that users store. The story of computers and consumer electronics over the past six decades can be told in terms of manufacturers, software publishers, and Internet companies jockeying against each other to capture as much control over—that is, to run their software on—as many computers as technology, the market, and law would allow. Hackers, meanwhile, also compete to get computers to run their instructions. Often, a hacker's goal is persistence, achieved by installing software that grants the hacker complete remote control over a computer. Network security professionals call such software "malicious software," although, in the default cybersecurity ordering, judgments about malice or benevolence don't matter; only control over a computer matters.

In the default cybersecurity ordering, computer owners have only whatever control over their computers that programmers allow them—that is, whatever control remains after operating system publishers, application developers, cloud service providers, and hackers have taken their share of control. The entities who design or program or hack computers and online services keep some control from the end user and reserve that control for themselves. How much control is reserved varies depending on which product the user chooses. Linux users have extensive control over their computers; they can access low-level computer hardware and sometimes even change minute behaviors of their Wi-Fi radios. Because the Linux source code is available to everyone under a free software copyright license, Linux users in theory can alter any aspect of Linux that they choose. By contrast, iPhone users can install only software that Apple permits, and Apple restricts what that software can do. For example, app developers can't write software that uses an iPhone's near-field communications capability to communicate with credit card payment terminals; only Apple's own Apple Pay software can do that. There is no technological reason why iPhones couldn't offer their users more control; Apple has simply chosen to reserve that control.

When the reserved control held by large American technology companies draws attention, the attention has been about antitrust and unfair competition, about privacy, and about platforms' choices about freedom of expression and content moderation. For example, the majority staff of the House Judiciary

Committee's Subcommittee on Antitrust, Commercial and Administrative Law alleged that Facebook, Google, Amazon, and Apple use their control over their websites, app stores, operating systems, and other products to (a) disadvantage potential competitors by preferring their own products, (b) collect competitive information about how consumers are using competitors' products, and (c) lock users into their ecosystems by making interoperability with competitors' products harder.[7] Companies' control over the mechanisms of publication and distribution, moreover, has put them in the position of deciding whether and how to censor some content, such as terrorist material.

Companies also use their control for other purposes. For example, Amazon used its control over its Echo smart speakers in 2021 to add functionality that shared Echo owners' Internet connections over Bluetooth with passersby—belatedly giving those owners a chance to opt out, but not asking for their affirmative permission.[8] Apple in 2022 modified how AirDrop, a technique for sending information from one Apple device to another without using the Internet, worked in China, removing users' option to leave AirDrop on permanently and instead requiring it to turn off after 10 minutes—a decision that seemingly cut off one means of communication used by anti-government protesters in China.[9] Firms sometimes also use reserved control to enforce moral judgments. In 2010, Apple prohibited pornography apps on the iPhone by disallowing them from its monopoly App Store. CEO Steve Jobs responded to a customer's complaint about that policy this way: "We do believe we have a moral responsibility to keep porn off the iPhone. Folks who want porn can buy an Android phone."[10]

What is common to each of these scenarios is *reserved control:* the ability of companies to treat competitors unfairly, to invade privacy, to censor, to borrow Internet connections, to enforce moral judgments, and to restrict usage of near-field radios only because companies have made design decisions that reserve to themselves a measure of control over the computers and online services that citizens use.

Who exercises this reserved control, and how, can be regulated by law. Most common are laws regulating *how* reserved control may be used. For example, privacy laws, like Europe's General Data Protection Regulation or the California Consumer Privacy Act, restrict how companies treat the user data that companies obtain through their control of cloud services and consumers' computers. Antitrust regulators in the United States and Europe argue that companies may not abuse their power for anticompetitive ends. Yet these are only examples of limiting how companies *use* control; regulators

[7] Majority Staff, Subcommittee on Antitrust, Commercial and Administrative Law, House Judiciary Committee, "Investigation of Competition in Digital Markets," Oct. 5, 2020, https://perma.cc/KU7B-S7Q2.

[8] See, generally, *Street v. Amazon.com Servs., LLC*, No. 2:21-CV-0912-BJR, 2022 WL 3683811, at *1 (W.D. Wash. Aug. 25, 2022).

[9] Mark Gurman, "Apple Limits iPhone File-Sharing Tool Used for Protests in China," *Bloomberg*, Nov. 9, 2022.

[10] Chris Matyszczyk, "Steve Jobs: If You Want Porn, Get an Android," *CNET*, April 20, 2010.

accept as a given that a few powerful companies will *reserve* control, and they seek to punish companies when they abuse that control.

In theory, law could go further and prohibit companies from retaining control at all—for example, by mandating interoperability, or by mandating open source and free software. In the United States, at least, this is uncommon. Instead, market forces are left as the chief regulator. The U.S. policy toward empowering consumers is an extension of Jobs's "folks who want porn can buy an Android phone": Folks who don't like one company's exercise of its control can do business with the competition instead. Shoppers choose among technological dictators, preferring the most benevolent.

Apart from limiting firms' ability to reserve control from users, governments might also patch the default cybersecurity ordering to appropriate reserved control for themselves. By giving industry legal obligations to adhere to legally mandated design standards, governments appropriate the reserved control industry has over users. An example is statutes that require telephone companies and other communications companies to have the technical ability to implement court-ordered wiretaps and to provide technical assistance to government agents.[11] Compulsory process laws also qualify as examples because they require companies to turn over user data.

Morals, Autonomy, and Collectivism

Behind every patch is a normative judgment—a decision that, although technology and physics would permit or deny some form of control, law should dictate a different outcome. Often these normative judgments are moral. Moral judgments are central to cybersecurity. Departing from the default cybersecurity ordering is sometimes counterintuitive and always difficult. Policymakers seek those departures only when something about the way technology and physics leaves things is objectionable, and moral values often motivate those objections.

Consider again the Computer Fraud and Abuse Act. Anti-hacking statutes were inspired by analogies to trespass law and a related Lockean notion that property owners should be able to exclude others (and the government) from using their property, whether that property is an acre of land or a file server. Without anti-hacking statutes, the rule would be that whoever *can* control a computer *may* control that computer. That default rule values network defense skills above all other values. Although some applications of anti-hacking statutes can be controversial, no serious voices call for the total repeal of anti-hacking

[11] See, e.g., 18 U.S.C. § 2518(4) ("An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider … shall furnish the applicant forthwith all … technical assistance necessary to accomplish the interception[.]"); 18 U.S.C. § 3124(a) ("[A] provider … shall furnish such investigative or law enforcement officer forthwith all … technical assistance necessary to accomplish the installation of the pen register[.]"); id. § 3124(b) (technical assistance for trap-and-trace devices); 50 U.S.C. § 1805(c)(2)(B) (technical assistance for electronic surveillance orders under the Foreign Intelligence Surveillance Act [FISA]); id. § 1842(d)(2)(B)(i) (technical assistance for pen traps under FISA).

statutes. Anti-hacking statutes are notable for being both long-standing and widespread. In the United States, an anti-hacking statute was first enacted just a few years into the personal computer revolution; even before then, during the age of microcomputers and mainframes, courts entertained the argument that general-purpose fraud statutes prohibited some unauthorized accesses of computers.[12] Anti-hacking statutes are far from an American peculiarity; the nations that have ratified or acceded to the Budapest Convention on Cybercrime have all agreed that their nations' criminal laws ought to prohibit "the access to the whole or any part of a computer system without right."[13]

That anti-hacking statutes are long-standing and widespread shows a long-standing global consensus, reflecting a moral judgment that, while computers as a technological matter can be controlled by many people, only some people ought to control them. This is the moral value of *autonomy.* Valuing autonomy means recognizing each person has a right to have a private sphere of computing, a set of computers or data over which that person has the exclusive right to determine control. That sphere mostly encompasses computers the person owns and possibly also includes computers the person does not own but depends on. Not unlike moral values favoring personal autonomy, bodily integrity, and property rights, the moral value of autonomy appreciates how important computing has become in society and, with that importance, the need to preserve human dignity. The autonomy value elevates personal choice, to promote the individual's independence from society and the state. The autonomy value also upholds property rights in computers, generally looking to property law (and maybe to contract law) to define the sphere of computing that an individual has the right to control. Autonomy sees ownership of a computer as carrying the complete, though assignable, right to control that computer. Autonomy is frequently in conflict with access-enabling legal patches and other interferences by the state in personal control, but autonomy frequently stands in favor of strict anti-hacking statutes and other access-prohibiting patches.

The consensus around anti-hacking statutes has deep support, beyond just the need to keep control over computers in the hands of those who would most benefit the economy and society. The support for anti-hacking statutes also comes from a moral judgment that human beings are entitled to a degree of control over their own computers, control sufficient for them to enjoy the benefits of computing despite its inherent vulnerabilities. When a family's computer is infected with malicious software, giving a hacker control over the computer sufficient to spy on everything the family does online, our outrage about that hacker's conduct springs not just from a concern over the possible harm to that family's bank account, but from a revulsion over how the family's choice and dignity were taken from them, and from dread about the ways the hacker might abuse the family in the future.

---

[12] See August Bequai, *Computer Crime* (Lexington, 1978).

[13] Budapest Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. 13174, E.T.S. No. 185, Art. 2, https://perma.cc/333D-52VR. According to the Council of Europe's website, 68 nations have ratified or acceded to the Budapest Convention. See Council of Europe, "Chart of Signatures and Ratifications of Treaty 185," https://perma.cc/9UVM-BWVE.

A different, often competing, moral value is also common in cybersecurity: *collectivism.* The value of collectivism is premised on the idea that the Internet is not merely an association of autonomous privately owned computers, but a collective, cooperative, mutually beneficial endeavor. Everyone, upon connecting their computer to the Internet, takes on a moral responsibility to others on the network. Collectivism values, most of all, preserving the collective utility that all Internet users derive from the Internet's interoperability. Like the value of autonomy, collectivism recognizes that individuals ought to have a private sphere of control, but collectivism looks to technology and the social understanding of network protocols to define that sphere. Collectivism tends to uphold technological rules embodied in code and math as the most important, because code and math are so much more determinative and predictable than judge-enforced laws. Individuals' permissible choices about withdrawing permission to access their computer must be expressed through collaboratively designed network protocols and prevailing norms of computer use. For example, someone who runs a server and opens port 80 ought to expect that anyone else on the network might send that computer an HTTP (web) request—including individuals whom the server owner did not personally invite, and including individuals whom the server owner, if asked, would not welcome. What matters is that the server owner participated in the HTTP protocol by opening port 80; from that point, who may control that server is defined by how the public understands the HTTP protocol and not necessarily by the server owner's personal preferences.

These two moral values of autonomy and collectivism can cohere, but they often compete. For example, suppose a person attaches his server to the Internet, runs a web server on it, and makes a file accessible through that web server. Hoping to protect it, the person gives the file a long, hard-to-guess web address; and he shares that address only with trusted parties. A journalist discovers the web address anyway and downloads the file. How one thinks about that scenario depends mostly on values. Those who value autonomy the most would uphold the server owner's intention that the file be kept secret; those who value collectivism would instead look at shared understandings about the web protocol and analyze whether the file was secured in a way that the community would accept as valid.[14]

A similar clash of moral values could be seen in cases involving peer-to-peer file sharing. Defendants, voluntarily running peer-to-peer file sharing programs such as LimeWire or Kazaa on their computers, downloaded illegal images of child exploitation. The file-sharing software then did what it was designed to do and automatically advertised the availability of those images for download to everyone else on the network. That advertisement made it possible for law enforcement agents to find offenders.[15] Defendants, valuing their autonomy, characterized law enforcement's conduct as a type of computer

[14] Orin S. Kerr, "Norms of Computer Trespass," *Columbia Law Review* 116 (2016): 1161–1163 (citing Internet Engineering Task Force "Request for Comments" documents as authoritative in concluding that "[a] person who connects a web server to the Internet agrees to let everyone access the computer much like one who sells his wares at a public fair agrees to let everyone see what is for sale").

[15] See, e.g., *United States v. Hoeffener*, 950 F.3d 1037, 1044 (8th Cir. 2020); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009).

intrusion, while government attorneys, valuing collectivism, defended law enforcement's conduct as consistent with the rules of the network that the defendants joined.

CYBERSECURITY BETWEEN GOVERNMENT AND CITIZENS

Civil liberties are legal rights that citizens may assert against their government. How civil liberties apply to computers and telecommunications is a notoriously complex question. The underappreciated cause of that complexity is that civil liberties disputes involving computers and telecommunications are also cybersecurity problems. These disputes at their core involve normative judgments about the government's exercising control over computers.

The Default Cybersecurity Ordering of Service Providers

Most citizens use computers that generate information that, thanks to reserved control and cloud computing, is entirely outside their technological control. The Supreme Court's *Carpenter* case was one of hundreds of possible illustrations. Carpenter robbed stores while carrying a cell phone. The default cybersecurity ordering left Carpenter's phone company with total control over his location information, of which it saved at least 127 days' worth. That location information sat on the phone company's computers, and neither Carpenter nor the officers investigating his crimes could control those computers or access that information. Assuming no hackers had access to the systems and that all insider employees with access to the data were trustworthy, what happened to that location information was entirely up to the phone company.

The *Carpenter* majority noted that phone companies might sell location records to data brokers. The majority wrote, however, that companies sold only "aggregated" records "without individual identifying information."[16] In retrospect, that was not entirely correct. Less than a year after the *Carpenter* opinion was published, an investigative journalist published an article whose headline tersely summarized the reality: "I Gave a Bounty Hunter $300. Then He Located Our Phone."[17] The article revealed that AT&T, Sprint, and T-Mobile's customers' location information was available for sale, and bounty hunters were buying it. About two years after the *Carpenter* opinion, the Federal Communications Commission (FCC) fined T-Mobile for making its customers' location information available to two "aggregators": companies that are generally in the business of buying data about persons. One reseller of the information was "reselling access to T-Mobile customer location information to bail bonding and similar companies to track the location of T-Mobile customer devices without customer consent."[18]

Location information gleaned from cell phone networks is the product of cell phone companies' reserved control. But other companies also have reserved control that allows them to collect location

[16] *Carpenter,* 138 S. Ct. at 2212.

[17] Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone," *Vice,* Jan. 8, 2019.

[18] *In re T-Mobile USA, Inc.*, 35 FCC Rcd. 1785, 1795 (2020).

information from other sources. When location information is captured by apps or phone operating systems through GPS, rather than by cell phone companies through network solutions, the FCC's regulations don't apply, and it's unclear whether any federal law restricts the sale of that information. Consider, for example, that "Google collects detailed location data on 'numerous tens of millions' of its users," collecting "sweeping, granular, and comprehensive" data that "serves Google's advertising business."[19] A Department of Homeland Security agency reportedly "bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border enforcement."[20] A mobile-advertising company was for years selling to its clients "bulk phone-movement data that included many Grindr users," data that was "in some cases detailed enough to infer things like … workplaces and home addresses."[21] In 2021, journalists used Grindr data, apparently obtained from ad networks, to report on the app's usage by officials in the Catholic Church.[22]

Location information is one example of information placed outside user control; online services and cloud computing are another. Using online services like Facebook or Google Drive means using those companies' computers and therefore giving those companies total technological (though not legal) control. Bitter reminders of that reality occur when stories emerge of employees inside those companies abusing their access, such as a Google employee accessing the communications of 15-year-old boys "to goad them and impress them with his level of access and power,"[23] a Twitter employee accepting bribes from a foreign government in exchange for selling personal user information,[24] and Meta employees accused of "taking over user accounts, in some cases allegedly for bribes."[25]

---

[19] *United States v. Chatrie,* No. 3:19CR130, 2022 WL 628905, at *3 (E.D. Va. Mar. 3, 2022).

[20] Byron Tau & Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *Wall Street Journal*, Feb. 7, 2020.

[21] Byron Tau & Georgia Wells, "Grindr User Data Was Sold Through Ad Networks," *Wall Street Journal*, May 2, 2022; see id. ("Grindr in 2019 said it was the world's largest social-networking app for gay, bi, trans and queer people, with 'millions of daily users who use our location-based technology in almost every country in every corner of the planet.'").

[22] See Liam Stack, "Catholic Officials on Edge After Reports of Priests Using Grindr," *New York Times*, Aug. 20, 2021.

[23] Kim Zetter, "Ex-Googler Allegedly Spied on User E-mails, Chats," *Wired*, Sept. 15, 2010.

[24] U.S. Department of Justice, "Former Twitter Employee Found Guilty of Acting as an Agent of a Foreign Government and Unlawfully Sharing Twitter User Information," Aug. 10, 2022, https://perma.cc/YE4E-KSQY.

[25] Kirsten Grind & Robert McMillan, "Meta Employees, Security Guards Fired for Hijacking User Accounts," *Wall Street Journal*, Nov. 17, 2022.

Some lawyers attach great importance to individuals' lack of technological control over service providers' computers. The Kennedy, Thomas, and Alito dissents in *Carpenter* are illustrative. Those dissents rely heavily on cybersecurity concepts. Emphasizing Carpenter's lack of "control," Justices Anthony Kennedy, Clarence Thomas, and Samuel Alito would let the default cybersecurity ordering stand. Phrasing the argument in terms of what Carpenter "owned" and whether records were "his," these three dissenters found it decisive that no legal authority patched the default cybersecurity ordering and granted Carpenter control over the location information. Thomas, for example, noted that "[n]either the terms of [Carpenter's] contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint."[26] Kennedy wrote much the same thing when he noted that "the cell phone customer, either from a legal or commonsense standpoint" had no basis to think "the law would deem" the location records as "owned or controlled by him."[27]

With that lack of legal patching established, these three dissenting justices wrote that Carpenter's lack of control should have been decisive. Alito devoted a paragraph to Carpenter's lack of control and its implications:

> Carpenter did not create the cell-site records. Nor did he have possession of them; at all relevant times, they were kept by the providers. Once Carpenter subscribed to his provider's service, he had no right to prevent the company from creating or keeping the information in its records. Carpenter also had no right to demand that the providers destroy the records, no right to prevent the providers from destroying the records, and, indeed, no right to modify the records in any way whatsoever (or to prevent the providers from modifying the records). Carpenter, in short, has no meaningful control over the cell-site records, which are created, maintained, altered, used, and eventually destroyed by his cell service providers.[28]

Thomas, dissenting, was more concise: Carpenter "did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them."[29]

These dissenting opinions are notable for their implicit reliance on collectivism as the most important value. "Once Carpenter subscribed to his provider's service," Alito writes, Carpenter lost the ability to control the data that his phone, in conjunction with the network, generated about his location. The dissenting justices' emphasis on the technological reality of Carpenter's situation, and on how that reality was the consequence of his decision to subscribe to a service and thus participate in the ordinary operation of a network, values those facts above Carpenter's individual preference about how his phone and the data it generates ought to have been controlled.

---

[26] *Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting).

[27] *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting).

[28] *Carpenter*, 138 S. Ct. at 2257 (Alito, J., dissenting).

[29] *Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting).

Legal Patching and Super-Patching

Those three dissenting justices, in describing how Carpenter "did not create the records," did not "maintain them," and did not "control them," accurately described the default cybersecurity ordering that Carpenter faced. They were less direct, however, in confronting another aspect of the default cybersecurity ordering: While it is true that Carpenter did not create, maintain, or control the location records, it was also true that the officers investigating him did not create, maintain, or control those records. Officers obtained control over those records solely because of the operation of a statute.

In fact, several legal rules—patches—led to the officers obtaining the location records. To start, there is a principle, going back to English common law, that a grand jury "has a right to every man's evidence" and may subpoena evidence unless other, limited, legal protections apply.[30] In the case of online records, a statute, the Electronic Communications Privacy Act (ECPA), limits the use of grand jury subpoenas but permits court orders or search warrants to compel providers to produce data to the government.[31] That same statute limits providers' authority to voluntarily disclose their customers' data, although its only meaningful limitation on disclosing non-content data is that it cannot be disclosed "to any governmental entity."[32] Another statute requires telecommunications providers to keep confidential their customers' location information.[33] An FCC requirement, additionally, requires that cellular service providers have the capability to identify the location of a phone making a 911 emergency call.[34]

The cybersecurity controversy underlying *Carpenter*, then, was about whether statutes gave the government more control over the phone company's computers and location data than the Fourth Amendment allows. Absent legal rules, Carpenter's location information likely would never have entered the government's control; in fact, absent the FCC's E911 location requirements, Carpenter's phone company might not have collected 127 days of location information in the first place. The entire controversy in *Carpenter* arose because the default cybersecurity ordering had been modified by these legal rules, both rules that required products to be designed to collect location information and rules that enabled police to access that location information.

---

[30] *United States v. Nixon*, 418 U.S. 683, 709 (1974).

[31] 18 U.S.C. § 2703; see, generally, Magistrate Judges Executive Board, *Carpe Data: A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information,* 3rd ed. (2017), 6–11, https://perma.cc/8LHN-EUQY.

[32] 18 U.S.C. § 2702(a)(3).

[33] 47 U.S.C. § 222(c), (h)(1); *In the Matter of T-Mobile USA, Inc.*, 35 FCC Rcd. 1785, 1799–1800 (2020) (finding that 47 U.S.C. § 222 required T-Mobile to keep subscribers' location information confidential).

[34] See, e.g., *Wireless E911 Location Accuracy Requirements,* PS Docket No. 07-114, Fourth Report and Order, 30 FCC Rcd. 1259 (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf.

In cybersecurity Fourth Amendment cases like *Carpenter*, the Fourth Amendment could be playing two, nonexclusive and potentially overlapping, roles: anti-patching and super-patching.

Anti-patching. The Fourth Amendment might play the role of guarding the default cybersecurity ordering from patches that benefit the government to the citizen's detriment. In this role, the Fourth Amendment restrains government by requiring a warrant, or at least a reasonableness justification, whenever a government action, statute, or other sub-constitutional authority patches the default cybersecurity ordering in a way that benefits an investigation. That is, if the way that citizens would have arranged their cybersecurity absent government interference would have succeeded in keeping evidence out of the government's control, then the Fourth Amendment regulates the government's use of patches to the cybersecurity ordering to obtain that evidence.

All compulsory process regimes—such as ECPA, or the common-law subpoena power of grand juries—could be evaluated under the Fourth Amendment's anti-patching role. When the U.S. Court of Appeals for the Sixth Circuit faulted ECPA for permitting the government to obtain the contents of an e-mail account without a search warrant, it was employing the Fourth Amendment in this anti-patching role.[35] However, if the default cybersecurity ordering permits government access to a computer, the Fourth Amendment would, under this anti-patching role, not stand in the way. For example, if the Fourth Amendment's only role is anti-patching, then none of the following situations would run afoul of the Fourth Amendment: when an inspector general in a government agency obtains information from the government agency's own computer, when a criminal investigator downloads from a defendant's computer material the defendant was sharing through peer-to-peer file sharing software, or when a government agent accesses a defendant's computer thanks to the defendant's failure to install security updates. In all of those examples, the default cybersecurity ordering enabled the government's conduct.

Super-patching. Whereas anti-patching courts scrutinize legal patches to the default cybersecurity ordering, super-patching courts scrutinize the default cybersecurity ordering. No matter how technology leaves things, super-patching courts might wield the Fourth Amendment as a final super-patch, holding that it requires the government to refrain from doing some things that technology nevertheless permits. For example, when the default cybersecurity ordering allows government investigators to access a defendant's computer remotely, courts might nonetheless wield the Fourth Amendment to patch that cybersecurity ordering.

If acting as a super-patch, the Fourth Amendment is being deployed in the service of some policy goal that the default cybersecurity ordering does not support. As explained above, all patches to the default cybersecurity ordering are motivated by a normative judgment that the unpatched cybersecurity ordering is undesirable; for example, anti-hacking statutes recognize that even though a teenager has a poorly secured iCloud account, it's undesirable to allow stalkers to access it. If it is playing a super-patch role,

[35] *United States v. Warshak,* 631 F.3d 266, 288 (6th Cir. 2010) ("[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'").

then the Fourth Amendment, too, must be motivated by some normative judgment. Policymakers and judges have a large menu of normative judgments to choose from, as the recent history of the Fourth Amendment and academic debates surrounding it have illustrated. Does the Fourth Amendment govern how much data the government gathers, or does it govern any use of technology with the capacity for indiscriminate surveillance?[36] Are the Fourth Amendment's protections defined by a concern to protect privacy,[37] or are they defined by positive law?[38]

Some anti-patching role for the Fourth Amendment, at least as applied to the content of communications, now seems uncontroversial. True, when the Fourth Amendment was first being applied to communications technologies, a vigorous minority pointed out that neither the amendment's history nor text permitted the conclusion that it regulated 20th-century technologies. Justice Hugo Black, for example, dissented from a holding that the Fourth Amendment regulated electronic eavesdropping, writing that the Fourth Amendment's reference to "persons, houses, papers, and effects" referred only to physical things, and that the words "searches and seizures" similarly meant the Fourth Amendment applies only to tangible things and not to conversations: "It simply requires an imaginative transformation of the English language to say that conversations can be searched and words seized," Black wrote.[39] Today, most Fourth Amendment lawyers have that imagination. Even modern textualists, such as Justice Neil Gorsuch, tend to read into "papers" modern forms of data storage and transmission, and even assert that "few doubt that e-mail should be treated much like the traditional mail it has largely supplanted."[40]

The *Carpenter* majority used the Fourth Amendment as a modest anti-patch. The majority opinion in *Carpenter* held that the government violated the Fourth Amendment by using a court order, rather than a search warrant, to compel the phone company to produce Carpenter's location records. The cybersecurity effect of the opinion was that the Court shrank the set of officers entitled to control the phone company's computers to those officers who could obtain search warrants. In shrinking the set of authorized officers, the majority used the Fourth Amendment to patch the part of ECPA that permitted officers to obtain records with a court order.

---

[36] David Gray & Danielle Citron, "The Right to Quantitative Privacy," *Minnesota Law Review* 98 (2013): 71–72.

[37] For example, Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," *Southern California Law Review* 75 (2002): 1086–1087.

[38] *Carpenter*, 138 S. Ct. 2206, 2268 (Gorsuch, J., dissenting) (citing William Baude & James Y. Stern, "The Positive Law Model of the Fourth Amendment," *Harvard Law Review* 129 (2016): 1852).

[39] *Berger v. New York*, 388 U.S. 41, 78 (1967) (Black, J., dissenting).

[40] *Carpenter*, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) (also calling data "your modern-day papers and effects").

Outwardly, the *Carpenter* majority opinion was concerned with familiar Fourth Amendment formalities and abstractions, such as whether the acquisition of the records was a "search," whether Carpenter had a "reasonable expectation of privacy" in them, the "third-party doctrine," and so on. The way that the Court manipulated those abstractions aroused great excitement,[41] earning Justice Alito's dissenting criticism that the opinion was "revolutionary" and prompting the observation that a majority of the Court now seemed motivated by Fourth Amendment policy concerns that were dramatically different from where the William H. Rehnquist Court's criminal procedure counter-revolution had left things.[42] Indeed, the majority invoked several normative judgments, among them an expectation by "society" that the government cannot "secretly monitor and catalogue every single movement of an individual […] for a very long period;" "basic Fourth Amendment concerns about arbitrary government power;" and "ensur[ing] that the 'progress of science' does not erode Fourth Amendment protections."[43]

Within the majority's invocation of concern for personal privacy in the face of "society," it's possible to detect impatience for the collectivist cybersecurity values advanced by three dissenters. Instead, the majority opinion seemingly values a limited form of autonomy for cell phone users like Carpenter. Yet the majority was not willing to advance that value of autonomy very far; its opinion was not revolutionary, but reactionary. The Court did not, in fact, disrupt a cybersecurity ordering in which entities "secretly monitor and catalogue every single movement of an individual." It left that cybersecurity ordering in place, only now requiring the government to use a search warrant supported by "probable cause" rather than a court order supported by "reasonable grounds to believe" before it may read from that catalogue.

Adapting a phrase used by Justice Louis Brandeis almost a century ago, the majority wrote that they were obligated "to ensure that the 'progress of science' does not erode Fourth Amendment protections."[44] However, "the progress of science" is not charted solely by scientists but also by the society that demands and makes use of scientific innovations. That society demands that its scientists (and engineers) behave morally and legally. "Science" is therefore not exogenous to law; when scientific innovations occur, legislatures, regulators, and courts have a say in how those innovations will affect society. It wasn't just "science" that led to a phone company having 127 days of Carpenter's movements sitting on a hard drive; it was also legal choices that required or permitted the phone company to

---

[41] See Alan Z. Rozenshtein, "Fourth Amendment Reasonableness After Carpenter," *Yale Law Journal Forum* 128 (2019): 944 n.2 (citing commentary).

[42] For example, Paul Ohm, "The Many Revolutions of Carpenter," *Harvard Journal of Law & Technology* 32 (2019): 388–389.

[43] *Carpenter,* 138 S. Ct. at 2217, 2222, 2223.

[44] *Carpenter,* 138 S. Ct. at 2223 ("As Justice Brandeis explained in his famous dissent, the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections.").

exercise that control. Legal rules can influence those technological choices, but the *Carpenter* court found fault only with a legal rule that allowed the government to appropriate the companies' reserved control too easily. Had it been in a revolutionary mood, the Court could have decided to subject private actors' decisions about computer code to constitutional review—a step some commentators have been advocating for decades.[45] But the Court left reserved control alone. In that sense, the *Carpenter* court did not launch a revolution, but rather suppressed one: The Court enabled private-sector surveillance by noting and leaving in place phone companies' reserved control. There will still be a "catalogue of every single movement of an individual" compiled by a private actor, but the Fourth Amendment makes it slightly harder for public actors to see it.

CYBERSECURITY BETWEEN NATIONS

Cybersecurity is a source of international conflict, and law both describes and shapes that conflict. Initially, it might appear that cybersecurity between nations is lawless, a brutal dystopia where only network defense and attack matter. But cybersecurity is about more than technology. As this section explains, law, and the moral choices behind law, both describe what cybersecurity is on an international scale and shape the contours of international conflict.

This section (a) extends the first section's definition of cybersecurity to an international context, showing how law can helpfully describe nations' relative strength and weakness, (b) explains how nations use law to increase their control over other nations' computers and data, and (c) explores how a nation's cybersecurity strategy requires choices between competing moral values.

Conflicts of Patches

As defined in the first section of this paper, cybersecurity is a state in which the people who can control computers and information are the people that law says ought to control those computers and information. But two nations might each define cybersecurity in contradictory ways. For example, the United States's anti-hacking statute generally prohibits Americans from hacking foreign computers, but it contains an exception stating that "lawfully authorized" intelligence activity conducted by U.S. intelligence agencies is not illegal.[46] Yet most foreign nations consider that U.S. intelligence agency activity a crime when it involves hacking computers within their borders. Reciprocally, many nations permit their intelligence agencies to hack computers in the United States, and the United States considers *that* activity to be a crime.

---

[45] See, e.g., Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999), 217–218 ("If code functions as law, then we are creating the most significant new jurisdiction since the Louisiana Purchase, yet we are building it just outside the Constitution's review."). For an opposing view, see Orin S. Kerr, "The Problem of Perspective in Internet Law," *Georgetown Law Journal* 91 (2003): 369–370.

[46] 18 U.S.C. § 1030(f).

It may seem formalistic to use criminal laws to characterize hostile conduct by foreign nations. Ordinarily, characterizing hostile foreign conduct as a crime yields few benefits. When British military forces burned the Capitol building and the White House in 1814, their conduct violated American laws against arson[47] but, presumably, was consistent with British law. That legal observation, however, does not lead to any helpful insights about the nature of the international conflict at the time. But law is far more important in understanding computer intrusions—so-called cyberattacks—because nations welcome some remote access of their computers by foreigners and oppose others. While British soldiers bearing lit torches will categorically never be welcome at the White House, situations where foreigners access, control, and otherwise affect U.S. computers are sometimes welcomed, and sometimes not. Law, frequently, is the only way to define those contours. When two nations both try to patch the default cybersecurity ordering in contradictory ways, that conflict of law describes the cybersecurity conflict.

These "conflicts of patches" situations point to a possible way to define cybersecurity at a national scale. If cybersecurity is the state in which the people who can control computers and information are the people that law says ought to control those computers and information, then a nation's cybersecurity is measured by the extent to which it is able to use law to patch the cybersecurity ordering in that nation's jurisdiction. Put another way, a nation's cybersecurity is intact if that nation can enact and enforce laws that accurately describe the nation's preferred cybersecurity ordering.

That might tempt one to see national cybersecurity as a rivalry, to measure national cybersecurity by counting how many computers one's own nation controls and measuring that against how many computers competing nations control. But national cybersecurity doesn't have to be rivalrous. Like-minded nations can align their laws by incorporating international agreements and norms into domestic law. For example, in 2021, all United Nations member states agreed on a framework for responsible state behavior in cyberspace.[48] The 2001 Budapest Convention on Cybercrime[49] also stands as a monumental achievement in the international law of cybersecurity. The nations that joined that convention agreed to roughly similar definitions of cybercrime and to help each other investigate and prosecute it.

Thus, international laws defining cybersecurity are possible. If all nations respect an international legal rule that, for example, prohibits hacking the computers of other nations, then that international legal rule serves as a patch to the cybersecurity ordering. Theoretically, international law—were it enforceable and obeyed by all nations—could be a foundation for every nation's cybersecurity, much as international law is a foundation for every nation's security against invasion. But work in formalizing international

[47] Were it not for combatant immunity. See Rymn J. Parsons, "Combatant Immunity in Non-international Armed Conflict, Past and Future," *Homeland & National Security Law Review* 1 (2014): 5–6.

[48] James Andrew Lewis, "Creating Accountability for Global Cyber Norms," Center for Strategic and International Studies, Feb. 23, 2022, https://perma.cc/88KW-LUY6.

[49] Supra note 13.

laws and norms against cyberattacks is incomplete.[50] Meanwhile, faith in international law as a source of stability and defense has been in decline, punctuated by Russia's blatantly illegal war against Ukraine.

Domestic criminal law, also, has known limitations in deterring foreign actors. As described above, the United States uses its criminal law to prohibit the members of foreign militaries and intelligence services from attacking U.S. computers. The U.S. government has criminally indicted military officers and other foreign nationals, working on behalf of the governments of China, Russia, Iran, and North Korea, for violations of the U.S. anti-hacking statute.[51] While it is possible to enforce anti-hacking laws by arresting and imprisoning foreign hackers, doing so is difficult and rare. Arrests do happen, but the resulting deterrent effect has not stopped international hacking.

Absent criminal law, and absent tools generally held only by wealthy and influential nations (like threatening economic sanctions or diplomatic consequences for hacking), the default cybersecurity ordering that whoever *can* control a computer *may* control a computer would prevail internationally. In such a world, a nation's strength is measured by how many foreign computers it can control and by how many domestic computers foreigners can control. Nations must weigh not only the number of soldiers in their army or the number of aircraft carriers in their navy, but also the number of zero-day vulnerabilities their hackers know how to exploit. Yet, even in this state of lawless international rivalry, network defense and attack are not everything. The concept of reserved control—and who may exercise that reserved control—is also important and, significantly, determined by law.

Reserved Control as a Tool of National Cybersecurity

Reserved control—the power that technology companies retain over computers and data—is a national cybersecurity battleground. No matter where in the world a computer is located, if its software or hardware allows a technology company to send it commands, then the computer is at least partially under the control of that company. Governments might appropriate that reserved control and, theoretically, order any companies that obey their laws to wiretap communications, to turn over stored

[50] See, e.g., Michael P. Fischerkeller, "A Cyber Persistence Way to Norms," *Lawfare*, June 29, 2022.

[51] Press Releases, U.S. Department of Justice, China: "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," July 19, 2021, https://perma.cc/4L3L-EKPZ; Russia: "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," Oct. 4, 2018, https://perma.cc/T3KZ-7BSY https://perma.cc/T3KZ-7BSY https://perma.cc/T3KZ-7BSY; Iran: "Iranian Hackers Indicted for Stealing Data from Aerospace and Satellite Tracking Companies," September 17, 2020, https://perma.cc/BC79-Y88T; North Korea: "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," Feb. 17, 2021, https://perma.cc/F4KW-VPTU.

data, to send remote software updates, or to use any other technological means available to advance that nation's self-interest.

From the viewpoint of national cybersecurity, software vulnerabilities and reserved control are rough equivalents. Both concern whether the technological reality of who controls a computer matches whom a nation would prefer to control that computer. This equivalency is why a Russian government hacker's installation of malicious software on a victim's computer can be just as concerning as that victim's installing "antivirus" software published by a Russian company that must obey the Russian government. This equivalency is why a Chinese government hacker's penetration and exploitation of a telecommunications network could potentially lead to the same result as that telecommunications network incorporating network hardware that is designed and controlled by a Chinese company obligated to obey the Chinese government. This equivalency is also why the United States's dominance in consumer operating systems and its strong but contested lead in social networking and cloud computing is a source of concern for other nations.

Concerns about reserved control motivate data localization and data transfer restrictions. Russia in 2016 banned LinkedIn, purportedly for not storing information about Russians on servers inside Russia.[52] China in 2017 effectively forced Apple to store the iCloud data of Chinese citizens on servers located in China and owned by a Chinese company.[53] The European Union generally prohibits firms from "transferring" data out of countries whose privacy laws the EU approves of and into countries it disapproves of,[54] and French law now requires the French government and French critical infrastructure companies to use for cloud storage only French servers run by French firms.[55] At bottom, all of these policies or laws are aimed at maximizing the power of a nation to use its laws to define its own preferred cybersecurity ordering. Russia's Roskomnadzor agency, for example—nominally a telecommunications agency but, functionally, an intelligence agency—exerts control over local Russian computers and networks to surveil computers in Russia.[56] Data localization also, of course, minimizes foreign nations'

[52] Olga Razumovskaya & Laura Mills, "Court Upholds Decision to Ban LinkedIn in Russia," *Wall Street Journal*, Nov. 10, 2016.

[53] Paul Mozur, Daisuke Wakabayashi, & Nick Wingfield, "Apple Opening Data Center in China to Comply With Cybersecurity Law," *New York Times*, July 12, 2017.

[54] Sam Schechner, "Meta Fined $1.3 Billion Over Data Transfers to U.S.," *Wall Street Journal*, May 22, 2023.

[55] Nigel Cory, "France's 'Sovereignty Requirements' for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation," Information Technology & Innovation Foundation, May 10, 2022.

[56] Paul Mozur, Adam Satariano, Aaron Krolik, & Aliza Aufrichtig, "'They Are Watching': Inside Russia's Vast Surveillance State," *New York Times*, Sept. 22, 2022.

ability to use appropriated control to surveil domestic data; the EU's rule, for example, protects against EU companies placing data within Roskomnadzor's clutches.

Foreswearing the use of reserved control is also a national security strategy. Nations ultimately advance their cybersecurity when they appropriate reserved control sparingly, predictably, and transparently. The popularity of a nation's software, hardware, and cloud services is connected to the extent to which a nation can credibly guarantee that its law bestows on customers an acceptable level of cybersecurity. Few customers, given the choice, would intentionally choose to trust their data and their computers to a company beholden to an authoritarian state. Democratic nations with a tradition of rule of law, which respect their companies' autonomy and invade it only as authorized by narrow and well-justified statutes, therefore enjoy a significant cybersecurity advantage. They can use their legal systems to credibly forswear from appropriating reserved control, except in defined and justifiable circumstances; and they can erect around those legal promises court systems and procedural guarantees. Nations compete, essentially, by defining cybersecurity orderings, and customers take them into consideration when shopping for services. Counterintuitively, nations that credibly bar themselves from appropriating reserved control end up with more reserved control. Those nations find that their superior legal regimes lead to more domestic data and computers, located there not because of mandatory localization requirements but because of the rational preference of individuals and firms that approve of the nation's definition of cybersecurity.

Autonomous and Collectivist Approaches to National Cybersecurity

Autonomy and Externalities

Autonomy—recognizing that each person has a right to have a private sphere of computing, a sphere that generally coincides with property rights—has traditionally predominated in cybersecurity policy.[57] An autonomous view of cybersecurity sees cybersecurity as guaranteeing the continued freedom of a nation's citizens to control their own computers, free from the interference of their fellow citizens, the interference of their government, and the interference of foreign governments. This way of thinking aligns with the Jeffersonian argument that governments are formed to secure rights and also aligns with the related notion that armies and territorial defense forces are chiefly useful because they protect the legal rights of citizens from the consequences of foreign attack and invasion. To bring about this vision of autonomous cybersecurity, governments have assisted the private sector in protecting its networks the same way that it has protected any private property: by defining a concept of trespass (here, computer intrusion) and credibly threatening to punish it as a crime, thus deterring potential offenders. More recently, governments have devoted attention to collecting information that network defenders would find useful and sharing it with them. But the choice about whether to use that information, and about whether and how to protect one's computers, is traditionally left to whoever owns that computer.

[57] See Jason Healy, "Twenty-Five Years of White House Cyber Policies," *Lawfare*, June 2, 2023.

Computers are private property, under this view, and the ultimate responsibility to protect them lies with their owners.

This traditional autonomous view of cybersecurity has recently come under significant pressure. Part of the pressure comes from how hacking can produce physical damage outside of the hacked computer. Consider the introduction to the report issued by the Cyberspace Solarium Commission, a congressionally chartered group chaired by members of Congress that was charged with making policy recommendations to improve the United States's national cybersecurity. That report's introduction began with a small work of speculative fiction, in which a beleaguered Senate staffer looks across Washington, D.C., and sees the Potomac River polluted by chemicals released from hacked water treatment plants, hacked delivery drones crashing into civilians, and refugees from Baltimore camping in all available open spaces after a hack of a railroad caused a toxic accident that rendered their home city uninhabitable.

The state's interest in regulating the computers controlling chemical plants and railroads is precisely as strong as the state's interest in regulating those chemical plants and railroads themselves, and whatever autonomy interest the owner of those computers (or chemical plants or railroads) might have is easily overridden by society's need for safety. If the autonomous decisions of the owners of water treatment plants, delivery drones, and railroads result in a malicious adversary's control over their computers, that control can cause disastrous physical consequences outside of computer networks, consequences that will harm the autonomy of many other people. Another challenge to the traditional autonomy view of cybersecurity is cloud computing: If Yahoo's autonomous decisions result in its losing control over its e-mail servers, that injures not only Yahoo's autonomy but also the autonomy of Yahoo's millions of users. Another challenge is botnets and other mass-hacking. For example, a 2016 Department of Justice indictment charged defendants with hacking vulnerable web servers and then using those web servers to launch distributed denial-of-service attacks on U.S. bank websites.[58] The vulnerable web servers were "running versions of popular website content management software that had not been updated to address certain known security vulnerabilities."[59] Those unaddressed vulnerabilities meant that the defendants could control the servers by installing malicious software that obeyed their commands.

What unites the challenges posed by physical threats, cloud computing, and botnets is negative externalities. In each case, the autonomous decisions of computer owners led to those computers being controlled by an adversary, who then turned the computers into weapons against others. While the water treatment plant, Yahoo, and web server owners all suffered blows to their autonomy, the residents of the city, Yahoo's users, and banks all suffered worse blows to their interests.

---

[58] Indictment in *United States v. Fathi et al.*, 16-CRM-48 (S.D.N.Y. March 24, 2016), https://perma.cc/K2TU-7JLS. The indictment is only an accusation, and all defendants are presumed innocent unless proven guilty in a court of law.

[59] Id. at 7.

Policing negative externalities leads to a reassessment of autonomous cybersecurity and the need to promote collective cybersecurity. As discussed before, the value of collectivism is premised on the idea that the Internet is a collective, cooperative, mutually beneficial endeavor, and not merely an association of autonomous privately owned computers. In line with this view, governments have gradually begun to exercise small degrees of control over their lawful citizens' computers, in some cases countermanding citizens' demonstrated wishes. Governments might try to mandate network defense measures; to deter poor network defense by imposing liability; to outlaw unacceptably insecure or un-securable products, like "antivirus" software controllable by Russia or 5G routers controllable by China; or, as described below, to go even further and take direct technical control over citizens' computers for the purpose of making them more secure.

Domestic Online Disruption Operations

In 2021, a serious vulnerability in Microsoft Exchange e-mail server software permitted hackers to install their own software on those servers. That software, a web shell, awaited future commands from the hackers. The Exchange vulnerability was exploited for the first two months of 2021, and then, in March, Microsoft published a software patch that corrected the vulnerability. Microsoft and government agencies published tools to remove web shells. By mid-April, however, "although many infected system owners successfully removed the web shells from thousands of computers, others appeared unable to do so, and hundreds of such web shells persisted unmitigated." This was a danger to everyone: The web shells "could have been used to maintain and escalate persistent, unauthorized access to U.S. networks." The Justice Department, acting through the FBI, deleted the shells. The technical ability to delete them came from the web shells themselves: "The FBI conducted the removal by issuing a command through the web shell to the server, which was designed to cause the server to delete only the web shell." [60]

Online disruption operations occur when governments or private firms exercise control over computers that they do not own in order to stop, remediate, or prevent unauthorized use of those computers. That is, a disruptor takes some control over a computer and uses that control to disrupt someone else's past, ongoing, or planned use of that computer. Many of these disruption operations to date involve botnets—networks of thousands or millions of compromised computers that stand ready to obey commands sent them by a criminal "bot herder" through a command-and-control server. For example, in 2011, the FBI's seizure of domain names allowed it to take over control of the Coreflood botnet, control that the FBI then used to try to liberate as many computers as possible. In 2017, the FBI and the Justice Department disrupted the Kelihos botnet, whose bots communicated largely peer-to-peer rather than through

[60] U.S. Department of Justice, "Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities," April 13, 2021, https://perma.cc/58QU-UTGC. *A disclosure:* I supervised attorneys who provided legal advice regarding this operation.

centralized servers, by sending "peer lists" and "job messages" to multiple infected machines.[61] The 2021 Microsoft Exchange operation also fits into this category. Disruption operations aren't solely the province of governments, either: Microsoft, in particular, has used court process to address criminal misuse of computers.[62]

Whether through disruption operations or through regulation, when governments seek to control law-abiding individuals' computers, they surface a contradiction between two moral values: autonomy, which would uphold individuals' rights to control their own computers and make decisions about how they are configured; and collectivism, which holds that the interconnected and cooperative nature of the Internet imposes moral obligations and rights on network users. Disruption operations like the 2021 Microsoft Exchange operation provide a helpful illustration. On the one hand, disruption operations uphold the autonomy of computer users. The operations liberate computers from the control of hackers and restore control to owners. They also, not incidentally, remove from malicious actors a powerful—perhaps even crucial—weapon, and thus save others from violations of their autonomy. At the same time, the web shell removal operation violated autonomy; the disruptors seized control of the infected computers and used that control to make changes to the computers, all either without permission or, at best, with only implied or inferred permission. Doing so reduces lawful computer owners' capacity to control their own property. On this reading, the disruption operation seemed to value collectivism more than autonomy; it advanced the collective health of the network at the expense of impairing computer owners' autonomy. In fact, the Exchange disruption operation seemed to value not just collectivism but one of the strongest statements of collectivism possible: that the collective health of the network so outweighs individuals' autonomy that the ultimate decision about how to configure one's own computer does not belong to the individual, but to the government or some other entity acting on behalf of the common good.

Resolving those tensions requires refining the moral judgment surrounding who ought to have control over computers. Here, the concept of reserved control is helpful. While the moral intuition of autonomy seems to value a total prohibition on outsiders modifying those computers, computer owners do not, in fact, have or for the most part seek out complete control over their devices. Instead, computer owners surrender important decisions to others, mostly to manufacturers and software publishers. To give one example of this user surrender, a positive, welcomed feature of modern operating systems and application software is automatic security updates: Without the user having to do much more than the occasional restart of the computer, modern software downloads software patches from its publisher and applies them to fix vulnerabilities. Automatic security updates promote network security, but at the cost of considerable control; with automatic update mechanisms, publishers can make all sorts of changes,

---

[61] United States' Memorandum of Law in Support of Motion for Temporary Restraining Order, *United States v. Levashov,* Case No. 3:17-cv-00074 (D. Alaska Apr. 4, 2017), https://perma.cc/B6Q4-M949.

[62] See Janine S. Hiller, "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets," *Santa Clara High Technology Law Journal* 31 (2015): 186.

including changes the user might not like. Another example of user surrender comes from the very decision to buy locked-down computers, such as the iPhone. Apple retains so much reserved control over the iPhone that users aren't even allowed root access—that is, administrator-level access—to their own computers. While that means users cannot customize the computers fully, it also means that users generally do less damage if they are tricked or fooled into installing malicious software. Buying locked-down computers is like Odysseus ordering his crew to tie him to the mast so that he could resist the calls of the Sirens: It is a voluntary choice to forego the ability to make future choices.

These are the two paradoxes of the value of autonomy. First, autonomy can be self-defeating. There is a moral judgment in favor of autonomy, but autonomy means that computer owners will sometimes make decisions that ultimately compromise their technological ability to control their own computers. Second, autonomy is often unwelcome: Computer security is hard, and considerable evidence now exists that most computer owners would prefer to surrender control over their computers to software publishers and other trusted parties.

CONCLUSION

Cybersecurity debates are difficult in large part because they are, ultimately, normative debates. The very thing that defines computers—that they obey commands—puts into question who ought to be commanding them. That difficult question underlies not just computer anti-hacking statutes but also laws about surveillance, technology regulation, privacy, and even competition. While each area of law comes with considerations that are independent of cybersecurity, all are also, ultimately, similar in that they demand a choice between autonomy and collectivism.

The Digital Social Contract paper series is supported by funding from the John S. and James L. Knight Foundation and Meta, which played no role in the selection of the specific topics or authors and which played no editorial role in the individual papers.