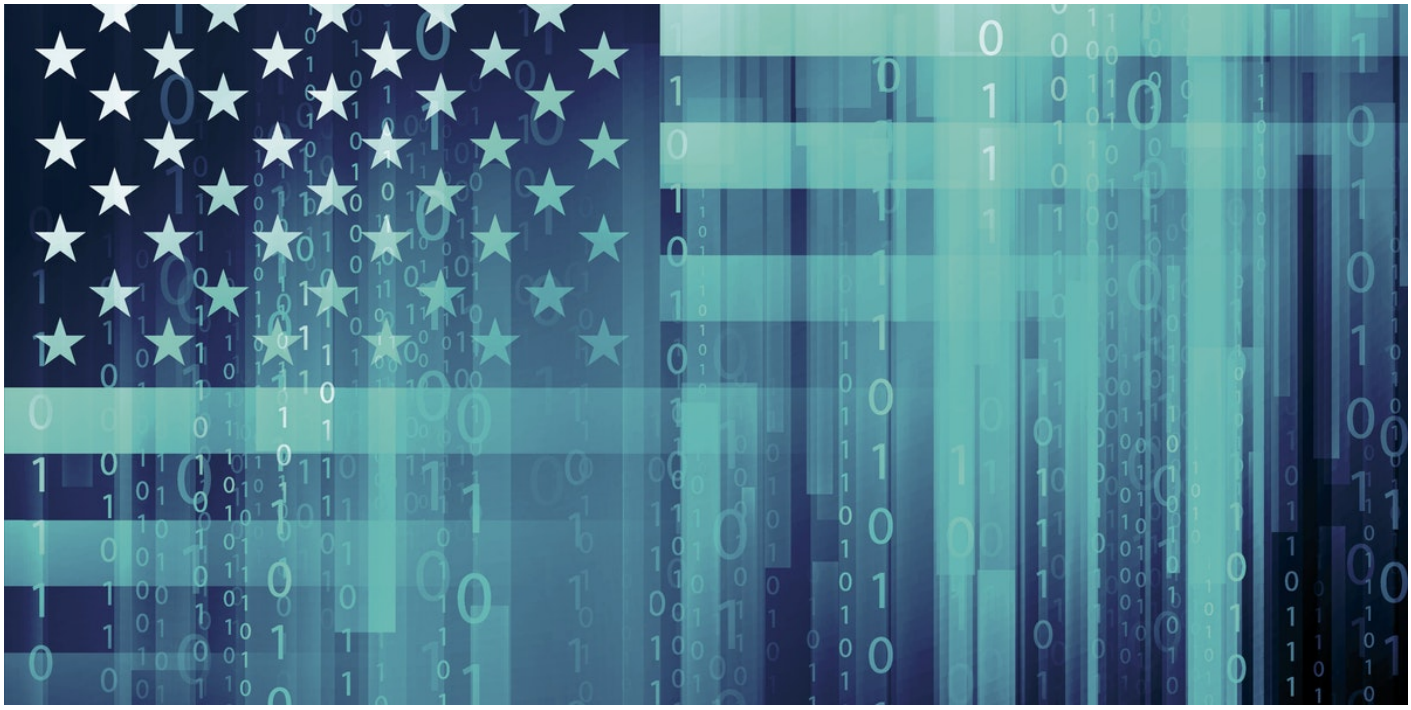
THE CENTURY FOUNDATION | 1919 2019



REPORT SURVEILLANCE & PRIVACY

Data Protection Federalism

Opportunities for State Executive Leadership on Cybersecurity and Consumer Privacy

AUGUST 15, 2018 — JONATHAN MAYER

During the Obama administration, prospects for federal regulation of cybersecurity and consumer privacy were dim. The administration recognized the need for action, but it struggled to advance even half-measures[1] and repeatedly got bogged down with ineffective working groups.[2] Officials were torn between acknowledging the pervasive market failures associated with cybersecurity and consumer privacy (which they were hesitant to articulate) and promoting economic progress in the exploding technology sector.[3] Dozens of bills languished in Congress, and what little progress occurred was primarily attributable to independent regulatory agencies—especially the Federal Trade Commission (FTC), which reinvented itself as a tech-savvy regulatory enforcer,[4] and the Federal Communications Commission (FCC), which attempted a similar feat through both enforcement[5] and rulemaking.[6]

Now, in the Trump administration, meaningful federal legislation and regulation are nonstarters. The administration moved quickly to repeal the FCC's broadband security and privacy rules.[7] The White House Office of Science and Technology Policy, which previously played a leading role on cybersecurity and consumer privacy, lacks a director, a chief technology officer, and most of its staff.[8] Even completely voluntary efforts, such as National Telecommunications and Information Administration (NTIA) projects to address Internet of Things security and botnet mitigation, are struggling to make progress.[9] Meanwhile, on Capitol Hill, the current congressional leadership has not demonstrated much appetite for meaningful cybersecurity or consumer privacy legislation—even as the Facebook-Cambridge Analytica and Russian hacking scandals continue to dominate headlines.[10]

In this federal vacuum, the states have become—and foreseeably will remain—the primary venue for regulating cybersecurity and consumer privacy in the United States. This federalism twist on technology policy is not entirely new; requirements for privacy policies,[11] data breach notification,[12] reasonable data security,[13] and secure data disposal[14] are already (mostly) creatures of state law. State legislatures are dabbling in new types of security and privacy legislation—but, owing to firm opposition, bills that incorporate a regulatory component have mostly stalled.[15] Perhaps the highest-profile examples have been in California. At the end of last year, a push to enact broadband privacy legislation—with support from a majority of the Assembly and Senate—fell short at the end of the legislative session.[16] And this year, an ambitious ballot initiative that attempted comprehensive cybersecurity and consumer privacy protections resulted in watered-down legislation that will have negligible impact on security and likely little immediate impact on the most pressing privacy issues.[17] As Joanne McNabb explained in a recent Century Foundation report, state legislation holds immense potential as a mechanism for addressing data security and privacy concerns.[18] But, at least in the near term, progress will be inconsistent and incremental.

This report is motivated by the current political landscape on cybersecurity and consumer privacy regulation. It focuses on a narrow and challenging question: If the federal government will not act, and if state legislatures will be slow, modest, and piecemeal in acting (when they act at all), what policy instruments are available to the executive

components of state governments?

The report offers three recommendations for the states. First, it proposes that state attorneys general strengthen their data security and privacy enforcement, both through internal organizational improvements and multistate collaborations. Second, it suggests that states can substantially reinstate the FCC's broadband security and privacy rules, either by conditioning state contracts or by issuing interpretive guidance on state communications privacy law. Third, it recommends that state executive components take action to implement cybersecurity safeguards for critical infrastructure, both by incorporating baseline requirements into state contracts and by leveraging sector-specific regulatory agencies.

Strengthening Investigation and Enforcement Capabilities

State attorneys general play an increasingly prominent role in data security and privacy regulation.[19] Dozens of states have now participated in at least one security or privacy case, and it is routine for state attorneys general to investigate data breaches, privacy intrusions, and other technology-related consumer protection matters in parallel with federal regulatory agencies.

The primary security and privacy enforcement tools for state attorneys general are unfair competition laws,[20] similar to the FTC's Section 5 unfairness and deception authority.[21] All fifty states have an unfair competition law, though specifics differ significantly.[22]

In many states, the enforcement authorities that are available to the attorney general are broader than those available to the FTC. As of 2018, all fifty states require companies to notify their affected consumers in the event of a data breach, and can take enforcement action if notice is delayed or inadequate. Thirteen states authorize the attorney general to bring enforcement actions against businesses that maintain deficient data security safeguards. Three states require businesses to affirmatively disclose their privacy practices, and again authorize enforcement for noncompliance. All of these important consumer protections are presently absent at the federal level, with the exception of specific regulated sectors.

TABLE 1

State Cybersecurity and Consumer Privacy Laws		
	Cybersecurity	**Consumer Privacy**

	Data Breach Notification Requirement	Data Security Standard	Privacy Policy Requirement	Consumer Data Rights
Alabama	X			
Alaska	X			
Arizona	X			
Arkansas	X	X		
California	X	X	X	X
Colorado	X			
Connecticut	X			
Delaware	X		X	
Florida	X	X		
Georgia	X			
Hawaii	X			
Idaho	X			
Illinois	X			
Indiana	X	X		
Iowa	X			
Kansas	X	X		
Kentucky	X			

Louisiana	X			
Maine	X			
Maryland	X	X		
Massachusetts	X	X		
Michigan	X			
Minnesota	X			
Mississippi	X			
Missouri	X			
Montana	X			
Nebraska	X			
Nevada	X	X	X	
New Hampshire	X			
New Jersey	X			
New Mexico	X	X		
New York	X			
North Carolina	X			
North Dakota	X			
Ohio	X			
Oklahoma	X			

Oregon	X	X		
Pennsylvania	X			
Rhode Island	X	X		
South Carolina	X			
South Dakota	X			
Tennessee	X			
Texas	X	X		
Utah	X	X		
Vermont	X			
Virginia	X			
Washington	X			
West Virginia	X			
Wisconsin	X			
Wyoming	X			

Some state attorneys general are also authorized to impose greater penalties than the FTC. Under current law, the FTC usually cannot assess a monetary penalty for a business's initial security or privacy violation.[23] Instead, it must issue an order prohibiting future violations, and then can seek monetary penalties for violations of the order. (Some observers refer to this unusual enforcement restriction as a "two-strikes rule.")

Against this backdrop of significant state authority, this report offers two directions for attorneys general to make more effective use of their enforcement tools. First, the report suggest how attorneys general could make internal improvements to their offices to more effectively leverage their authorities. Second, the report recommend ways in which the state attorneys general could combine their authorities to collectively maximize their regulatory potential.

State-by-State Improvements

State attorneys general traditionally have broad discretion in how they prioritize enforcement areas, organize their offices, and retain experts. These (admittedly bureaucratic) tools provide an opportunity for more informed and effective policymaking on data security and consumer privacy.

As a first step, state attorneys general can designate security and privacy as priority issue areas. In my experience collaborating closely with several state law enforcement agencies, because of the limited prosecutorial resources that are available, the priorities that are communicated from leadership can have an outsized impact. The simple act of circulating a memorandum to line-level attorneys directing that they should be on the lookout for data security and privacy cases, and that they should vigorously enforce state law in those cases, can have a dramatic effect on the scale and sophistication of regulatory activity.

The law enforcement agencies of larger states can go a step further, by establishing units dedicated to investigating and pursuing data security and consumer privacy cases. This structural shift—again, an admittedly bureaucratic maneuver—can radically increase an agency's regulatory capacity. By becoming repeat players, these dedicated units gain expertise in the substantive law and litigation norms associated with security and privacy; they gain credibility with the private sector and courts; they gain valuable connections to similar units at the state and federal levels (especially the FTC's Division of Privacy and Identity Protection) and to researchers who develop investigative leads; and they gain a soft-power ability to influence the private sector without bringing enforcement actions.

In California, for example, the attorney general's office includes a (small) Privacy Enforcement and Protection Unit that works exclusively on data security and privacy matters.[24] In New York, the attorney general's office includes an (also small) Bureau of Internet and Technology that handles most technology-related matters.[25] In New Jersey, before establishing a dedicated unit earlier this year, the attorney general had several line attorneys who focused on security and privacy without a formal structure. Each of these organizational approaches has tradeoffs.[26] But, at present, the norm in most states is to only occasionally participate in multistate enforcement actions brought by other states.[27] Any of these institutional structures would be a significant improvement.

A third way in which state attorneys general can leverage their organizational authorities to become more effective at data security and privacy policymaking is to bring in technical expertise. A small number of states have hired technologists to assist with security and privacy matters; a larger number have retained consultants for specific matters. Both are positive developments. But the states could do more: at the federal level, several agencies have appointed

outside experts as term-limited chief technologists, significantly improving the quality and quantity of their technology-related policymaking. No state attorney general has yet emulated the chief technology officer (CTO) model, but at least the large states easily could and should.

Multistate Collaborations

State law enforcement agencies often act alone when pursuing regulatory actions. The tendency is understandable—coordination between states is logistically challenging, cases can involve highly sensitive commercial information, and elected state attorneys general can prioritize the political upside of a successful enforcement action. (Not coincidentally, the National Association of Attorneys General is often dubbed the National Association of Aspiring Governors among consumer protection counsel.) But in some areas of law, where the issues are complex or the legal violations are inherently interstate, attorneys general have worked together. This trend is especially common in data security and privacy cases, where dozens of states can collaborate on a single investigation and settlement.[28]

These multistate collaborations follow a fairly predictable pattern. News breaks that a company has suffered a data breach or invaded consumer privacy. Attorneys in several state law enforcement agencies will begin preliminary inquiries, and some state attorneys general may announce that they have launched investigations. Additional states reach out to the first movers, expressing interest in collaboration and offering varying degrees of support. The states then establish a multistate investigation, by drafting and signing a memorandum of understanding and tapping several states to lead a "steering committee." The states on the committee conduct discovery and enter settlement negotiations with the investigation target, while in parallel other states join the multistate effort. Finally, a settlement is reached; all the participating states rush to declare victory; credit primarily goes to the large states and the states on the steering committee.

This current process—while an improvement over individual state investigations—is deeply flawed. Multistate investigations move at a snail's pace, because they require starting from square one on every case (adopting a new agreement and selecting a steering committee), and because every decision about investigation and settlement is a decision by committee. In my experience working on parallel federal and multistate regulatory investigations (from both the federal and state sides), these state investigations tend to move at a half to a third of the pace of comparable federal investigations.

The present approach to multistate investigations also misses an important upside of combining state capabilities. Each state attorney general's office differs in its substantive legal authorities (that is, when it can hold a business accountable for a security or privacy incident), investigative processes (that is, when, how, and how quickly it can procure documents

and testimony), and internal capacity. These variations provide an opportunity for investigative arbitrage, where a multistate collaboration can leverage the state best positioned for each investigative task.[29] In a data breach case, for example, the state that compels disclosure of business records should likely be a state that has a data safeguard law (assuring a clear scope of discovery related to the breach), that can quickly issue subpoenas, and that has the e-discovery capacity to handle a large influx of responsive documents. In the status quo, by contrast, tasks are distributed among the steering committee states in a mostly ad hoc fashion. In my experience, assigning just one investigative task to the wrong state—which is regrettably common—can set back a multistate enforcement action by months.

The current multistate model also inhibits professionalization of state regulatory action on cybersecurity and consumer privacy. Because the steering committee differs for each case, the participating attorneys do not consistently gain subject matter expertise and credibility as repeat players. My experience has been that attorneys working on multistate steering committees are often consumer protection generalists rather than security and privacy specialists.

Furthermore, the current steering committee structure tends to omit technical expertise—the states on the committee usually lack a technologist, and the committee usually lacks the authority, budget, or initiative to hire an outside expert.[30] My experience working on parallel federal and multistate regulatory actions has been that, too often, state law enforcement agencies are compelled to rely on federal technologists (and occasionally attorneys) for their analysis of evidence and liability. This reliance dynamic is especially problematic in today's climate of waning federal regulatory action and technical expertise.

What would a better model for multistate collaboration on security and privacy investigations look like? In the near term, the state attorneys general that are making institutional commitments to security and privacy should establish a procedural framework for collaboration. Reinventing the multistate steering committee for every enforcement action is unnecessary and an inefficient use of limited resources. These states should enter into a memorandum of understanding that sets clear ground rules and expectations for future multistate security and privacy enforcement actions.

In the long term, institutionalization is a promising path forward. The states should develop an overarching agreement on multistate cybersecurity and consumer privacy cases, then embody that agreement in a new organization. The agreement and institution should address matters of leadership (perhaps infrequently rotated or elected state attorneys general), personnel (authorizing the hiring of technical experts and establishing a career path for state regulatory attorneys to specialize in security and privacy), and credit (perhaps a commitment to acknowledge all the participating states). Institutionalizing multistate collaborations could address the key flaws in the current model—slow starts, inefficient tasking, and insufficient professionalization—while building a powerful state-level companion to the federal regulatory agencies.[31]

Replacing the FCC Broadband Privacy Rules

Broadband service providers play a unique role in the internet ecosystem. They are essential onramps for accessing online content; they have the technical capability to collect and analyze a customer's activity across all the online services they use, and to link a customer's online activity to their identity; they encounter limited competition (especially for residential service); they have a trusted, fiduciary-like role in handling a customer's communications; they have historically declined to monetize customer communications other than by charging for service; and they are directly compensated by consumers (unlike Google, Facebook, and other popular online services that are predominantly supported by advertising).

In recognition of these attributes, during the final year of the Obama administration, the FCC proposed and adopted strong data privacy rules for internet service providers.[32] At the core of those data privacy rules was a requirement that, if an internet service provider sought to repurpose a customer's online activity for its own business gain, it first had to obtain the customer's affirmative, opt-in consent.[33] The opt-in provision was a high-water mark for federal privacy policy, and though it was repealed by the Trump administration in spring 2017, the concept of opt-in privacy protections has generated renewed and bipartisan interest in the wake of the Facebook-Cambridge Analytica debacle.[34]

There are at least two ways that state officials could recreate the core of the FCC's broadband privacy rules without making any change to state statutory law: leveraging state contracts and issuing interpretative guidance on state communications privacy law.

Conditioning State Contracts by Executive Order

In response to the FCC's repeal of the Obama-era net neutrality rules, the governors of Montana, New York, and New Jersey issued executive orders prohibiting their respective states from contracting with any internet service provider that declines to make an enforceable commitment to key net neutrality principles. While no state has yet followed a similar approach for replacing the FCC's privacy rules, the legal mechanism would be identical: forbidding state contracts to ISPs unless they make strong privacy commitments.

The upside to these contracting conditions is that they are fast—governors can usually issue them with the stroke of a pen. The downside is that these conditions are of limited efficacy, for two reasons.

First, these contracting conditions are unlikely to have much impact in the residential internet service market. States, like many large or mid-size businesses, tend not to procure wired internet service from the same ISPs that provide service to ordinary residences. Instead, states usually enter contracts with enterprise service providers with customized

plans.[35] As a result, the residential ISPs that are most concerning from a consumer security and privacy perspective would likely not be regulated by these contract conditions.

Another drawback is that these contracting conditions might be easily circumvented. If an ISP wants to continue participating in the government market, it could consolidate its government services into a new corporate subsidiary, then have only the subsidiary commit to honoring privacy and security commitments.

On the whole, conditioning state contracts to protect broadband privacy is a worthwhile effort—especially in the wireless market, where (at least for now) states enter contracts with the same major carriers that serve consumers. But the contract conditioning approach is inherently limited in its efficacy and possibly susceptible to circumvention.

Issuing Interpretive Guidance on State Communications Law

Some states have a much stronger alternative available: they can use their established communications privacy law to recreate the FCC's broadband privacy protections.

In a pair of seminal 1967 cases, *Berger v. New York* and *Katz v. United States*, the U.S. Supreme Court paved a clear avenue for law enforcement agencies to use wiretapping and eavesdropping in criminal investigations.[36] As a result, both federal and state communications privacy laws—which had previously been a mess, to the extent they existed at all[37]—were rapidly modernized. As of today, there is a comprehensive federal statutory scheme that regulates communications privacy (the Electronic Communications Privacy Act, or ECPA), and all fifty states have their own communications privacy laws.[38]

ECPA currently offers ambiguous protection against ISP privacy intrusions, because of how courts have interpreted the consent exceptions in the statutory scheme.[39] If an ISP repurposes the content of a customer's online communications, that is likely a wiretap—but a customer's agreement to a terms of service provision may be sufficient to establish consent.[40] Similarly, if an ISP repurposes metadata (for example, hostnames, IP addresses, and possibly parts of URLs), that is also prohibited—but terms of service may again be sufficient to establish consent, and the consent of the subscriber is sufficient even if the person currently using the internet connection does not consent.

As a practical matter, ECPA has become a paper tiger for ISP privacy because of how Congress drafted its enforcement provisions. ISPs have primarily sought to leverage metadata (rather than content) on an opt-out basis, and ECPA only provides for criminal misdemeanor enforcement against metadata interception. It is difficult to believe that the Department of Justice, especially in the Trump administration, would seriously consider criminally prosecuting ISPs for their iffy privacy practices.

State communications privacy law, however, can offer greater privacy protections. Perhaps the best-known example is the rule for consensually recording a telephone call; ECPA includes a one-party consent provision, while eleven states require two-party consent.[41] If a state wanted to enact a strong opt-in requirement for content or metadata interception, similar to the FCC's broadband privacy rules, plainly it could.

But what if a state already had these opt-in requirements on the books? That appears to be the case, or at least plausibly the case, in some states.

In New York, for example, there is a unified communications privacy law that prohibits interceptions of both content and metadata. The law includes a consent exception, like ECPA—but New York courts have consistently interpreted the exception to only cover actual knowledge of and assent to an interception (that is, opt-in consent).[42] Furthermore, under New York's law, consent for metadata interception must be obtained from a party to the communication (that is, the current user) rather than from a subscriber.[43] Thus, if a New York ISP repurposes any broadband activity (content or metadata) for any monetization purpose (including advertising practices), and the ISP only buries notice in its terms of service, it likely commits a felony that the attorney general or a district attorney can prosecute.

Even in the states where communications privacy law more closely parallels ECPA, state law can expand the enforcement tools that are available to regulators. In California, for example, the attorney general can bring a civil suit to enforce ECPA's prohibition on metadata interception—and can receive a monetary penalty of up to $2,500 per affected resident.[44] (And remember that California has tens of millions of residents.) The option to file in a civil rather than criminal proceeding makes the threat of regulatory enforcement more credible, since criminal cases involve heightened procedural requirements and evidentiary burdens.

Attorneys general do not need to take any formal legal action to effectively leverage these substantive and procedural advantages to state communications privacy law. Instead, they could issue enforcement advisories, announcing that they interpret state communications privacy law to require opt-in consent before repurposing a customer's internet activity and that they will vigorously enforce against any ISP that violates the opt-in consent requirement. The advisories would have a significant market disciplining effect, by boxing ISPs into the pro-consumer trilemma of either adhering to an opt-in requirement, flouting the law (risking backlash and penalties), or launching litigation challenging the requirement (also risking backlash and stalling adoption of concerning business practices).

Leveraging a creative reinterpretation of existing state data privacy law is not an unprecedented regulatory maneuver. In 2011, the California Department of Justice informed app stores that it would construe the state's privacy policy requirement for websites to also apply to mobile apps. Within just a year, every major app store had taken steps to bring developers into compliance and had signed onto an enforcement agreement with the office.[45]

Protecting Critical Infrastructure

The discussion in this report thus far has emphasized how state executive agencies can regulate to address consumer protection concerns. This section takes up a different regulatory responsibility—protecting state residents from cybersecurity risks to critical infrastructure.

As foreign powers increasingly leverage vulnerabilities in America's electronic infrastructure to their advantage—for example, Russia's attacks on election systems[46] and energy infrastructure[47]—the federal government has lagged in providing adequate assistance and protection. For the foreseeable future, states will be on the frontlines of defending their residents against hostile nations.

This report offers two recommendations for how the states can better secure critical infrastructure without new legislation: conditioning state contracts (similar to the suggestions above on broadband privacy) and leveraging established sector-specific regulatory agencies.

Conditioning State Contracts by Executive Order

States often contract with the private sector to deliver critical services. Systems involved in water treatment, emergency services, and election administration, for example, are often operated by businesses on behalf of state or local government agencies.[48]

Governors and mayors could leverage these contracts to ensure implementation of cybersecurity best practices. They could insist on a range of baseline requirements, such as data breach notification, routine security auditing by independent experts, encryption for data at rest and in transit, strong authentication, and routine updates. They could also establish new financial incentives for cybersecurity, such as by providing bonus payments to vendors that go without an incident or withholding payments from service providers that suffer a breach.[49]

A version of this concept already exists at the federal level. Both the Department of Defense and the General Services Administration have long required contractors to adhere to data security requirements, and they are currently updating their standard contract provisions to reflect best practices recommended by the National Institute of Standards and Technology.[50] Some states have also begun to incorporate security requirements into their contracts, albeit in a much more inconsistent fashion.[51] Implementing contract conditions by executive order would ensure clarity and uniformity in guidance, and it would send a powerful signal to state critical infrastructure contractors that they are obligated to prioritize cybersecurity.

Sector-Specific Regulatory Agencies

State governments include a diverse array of sector-specific regulatory agencies, and many of these agencies have existing statutory authority to promulgate rules related to critical infrastructure security, safety, or reliability. Those broad authorities usually encompass security considerations—including cybersecurity—but, thus far, state sector-specific agencies have been slow to take action in the area.

There is one notable exception: the New York Department of Financial Services (NYDFS). In 2017, NYDFS adopted baseline cybersecurity requirements that apply to all regulated financial services in New York—which, in practice, means all financial services. While the rules initially sparked a degree of controversy out of concern that states could adopt duplicative or inconsistent regulation, those concerns have largely subsided, and the financial sector has moved (relatively) quickly to ensure compliance.

States could adopt a similar approach for other areas of critical infrastructure. In California, for example, the Public Utilities Commission is authorized to promulgate reliability rules for power generation. The agency could draw on that authority to set standards for energy sector cybersecurity in the state.[52] In fact, all fifty states have a utility regulatory agency; while the specific authorities and sectors differ, all have at least a partial capability to protect the state's residents through cybersecurity rules for critical infrastructure.

Conclusion

Until the White House has a new occupant, the prospects for federal regulation on data security and consumer privacy remain dim. But there is cause for optimism at the state level—attorneys general, governors, and regulatory agencies have actionable policy options. By strategically reorganizing, reinterpreting the law, and leveraging existing authorities, states can make meaningful progress on data security and consumer privacy, starting today.

Notes

1. “We Can’t Wait: Obama Administration Unveils Blueprint for a ‘Privacy Bill of Rights’ to Protect Consumers Online,” The White House Office of the Press Secretary, February 23, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.
2. “Privacy Multistakeholder Process: Mobile Application Transparency,” U.S. Department of Commerce, National Telecommunications and Information Administration, November 12, 2013, https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency; “Multistakeholder Process: Unmanned Aircraft Systems,” U.S. Department of Commerce, National Telecommunications and Information Administration, June 21, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems; “Privacy Multistakeholder Process: Facial Recognition Technology,” U.S. Department of Commerce, National Telecommunications and Information Administration, June 17, 2016, https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology.
3. Commission on Enhancing National Cybersecurity, “Report on Securing and Growing the Digital Economy,” U.S. Department of Commerce, National Institute of Standards and Technology, December 1, 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
4. “Enforcing Privacy Promises,” Federal Trade Commission, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises; Daniel J. Solove and Woodrow Hartzog, “The FTC and the New Common Law of Privacy,” *Columbia Law Review* 114, no. 3 (January 31, 2011),https://columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/.
5. “FCC Settles Verizon ‘Supercookie’ Probe, Requires Consumer Opt-In for Third Parties,” Federal Communications Commission, March 7, 2016, https://www.fcc.gov/document/fcc-settles-verizon-supercookie-probe.
6. “FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency, and Security for Their Personal Data,” Federal Communications Commission, October 27, 2016, https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.
7. S.J.Res.34, “A Joint Resolution Providing for Congressional Disapproval under Chapter 8 of Title 5, United States Code, of the Rule Submitted by the Federal Communications Commission relating to ‘Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,’” 115th Congress, 2d. sess., 2017, https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34.
8. Tony Romm, “Here’s who could become one of Trump’s top science and tech advisers,” *Washington Post*, March 15, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/03/15/heres-who-could-become-one-of-trumps-top-science-and-tech-advisers/.
9. “A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats,” U.S. Department of Commerce and U.S. Department of Homeland Security, May 22, 2018, https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf; “Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching,” U.S. Department of Commerce,

National Institute of Standards and Technology, November 7, 2017, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

10. Kristine Phillips, “Zuckerberg Is About to Face Congress—But Facebook Scandal May Be Out of His Control, Lawmaker Says,” *Washington Post*, April 8, https://www.washingtonpost.com/news/business/wp/2018/04/08/zuckerberg-is-about-to-face-congress-but-facebook-scandal-may-be-out-of-his-control-lawmaker-says/.

11. “State Laws Related to Internet Privacy: Privacy Policies and Practices for Websites or Online Services,” National Conference of State Legislatures, March 26, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#CollectPI.

12. “Security Breach Notification Laws,” National Conference of State Legislatures, March 29, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

13. “Data Security Laws: Private Sector,” National Conference of State Legislatures, December 5, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

14. “Data Disposal Laws,” National Conference of State Legislatures, December 1, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

15. “Cybersecurity Legislation 2017,” National Conference of State Legislatures, December 29, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx.

16. Jazmine Ulloa, “Closely watched California Internet privacy bill dies in final minutes of legislative session,” *Los Angeles Times*, September 16, 2017, http://www.latimes.com/politics/essential/la-pol-ca-essential-politics-updates-california-internet-privacy-bill-1505542611-htmlstory.html.

17. California A.B. 375, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

18. Joanne McNabb, “Can Laboratories of Democracy Innovate the Way to Privacy Protection?” April 5, 2018, https://tcf.org/content/report/can-laboratories-democracy-innovate-way-privacy-protection/.

19. Danielle Keats Citron, “The Privacy Policymaking of State Attorneys General,” *Notre Dame Law Review* 92, no. 2 (2016), http://ndlawreview.org/wp-content/uploads/2017/02/NDL205.pdf.

20. “Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes,” National Consumer Law Center, February 2009, http://www.nclc.org/images/pdf/udap/report_50_states.pdf.

21. 15 U.S.C. § 45, https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap2-subchapI-sec45.pdf; “A Brief Overview of the Federal Trade Commission’s Investigative and Law Enforcement Authority,” Federal Trade Commission, July 2008, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

22. “Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes,” National Consumer Law Center, February 2009, http://www.nclc.org/images/pdf/udap/report_50_states.pdf.

23. 15 U.S.C. § 45, https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap2-subchapI-sec45.pdf.

24. “Privacy Enforcement and Protection,” California Department of Justice, https://oag.ca.gov/privacy.

25. “Bureau of Internet and Technology (BIT),” New York Office of the Attorney General, https://ag.ny.gov/bureau/internet-bureau.

26. Danielle Keats Citron, “The Privacy Policymaking of State Attorneys General,”*Notre Dame Law Review* 92, no. 2 (2016), http://ndlawreview.org/wp-content/uploads/2017/02/NDL205.pdf.

27. Ibid.

28. Ibid.

29. Daphna Renan has made a similar observation about how federal regulatory agencies can combine their authorities. Daphna Renan, “Pooling Powers,” *Columbia Law Review* 115, no. 2 (March 2015), https://columbialawreview.org/content/pooling-powers/.

30. This model also has a pernicious second-order effect—it diminishes the incentive for any particular state attorney general to retain a technologist, because either the hire would be wasted (if the state did not regularly participate on steering committees) or the upside of the hire would be diffusely shared with many other states (those participating in the multistate action).

31. There is, to be sure, nothing quite like this type of interstate regulatory pact or institution today. The most similar development is the Multistate Information Sharing and Analysis Center (MS-ISAC), which facilitates collaboration among state Chief Information Officers and Chief Information Security Officers on data security matters. MS-ISAC plays no regulatory role, though, and it primarily functions as an information conduit.

32. “FCC Releases Rules to Protect Broadband Consumer Privacy,” Federal Communications Commission, October 27, 2016, https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy.

33. The precise policy framework for this opt-in requirement shifted between the FCC’s proposed and final rules. The proposed rules set an opt-in requirement for repurposing any data; the adopted rules set an opt-in requirement for repurposing sensitive data, but then defined all customer online activity as sensitive.

34. S.J.Res.34, “A Joint Resolution Providing for Congressional Disapproval under Chapter 8 of Title 5, United States Code, of the Rule Submitted by the Federal Communications Commission relating to ‘Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,’” 115th Congress, 2d. sess., 2017, https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34.

35. These enterprise providers can be corporate relatives of consumer ISPs, but they are nevertheless different businesses.

36. 388 U.S. 41 (1967), https://scholar.google.com/scholar_case?case=7370572188907228701; 389 U.S. 347 (1967), https://scholar.google.com/scholar_case?case=9210492700696416594.

37. “The Challenge of Crime in a Free Society,” Commission on Law Enforcement and Administration of Justice, 1967, https://www.ncjrs.gov/pdffiles1/nij/42.pdf.

38. “Reporter’s Recording Guide: State-by-State Guide,” Reporters Committee for Freedom of the Press, https://www.rcfp.org/reporters-recording-guide/state-state-guide.

39. Orin Kerr, “The FCC’s broadband privacy regulations are gone. But don’t forget about the Wiretap Act.,”*The Volokh Conspiracy*, April 6, 2017,https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/04/06/the-fccs-broadband-privacy-regulations-are-gone-but-dont-forget-about-the-wiretap-act/. Some ISPs have also argued that ECPA’s “ordinary course of business” exception is sufficient to exempt advertising and other traffic monetization practices. That argument

has not fared as well in court. In re Google Inc. Gmail Litigation, No. 13-MD-02430-LHK (N.D. Cal. Sept. 26, 2013), https://scholar.google.com/scholar_case?case=17557746320195805060.

40. In re Yahoo Mail Litigation, 7 F. Supp. 3d 1016 (N.D. Cal. Aug. 12, 2014), https://scholar.google.com/scholar_case?case=11543818315680297453; *Kirch v. Embarq Mgm't Co.*, No. 10-2047-JAR, (D. Kan. Aug. 19, 2011), https://scholar.google.com/scholar_case?case=13501618191771077863; *Deering v. CenturyTel, Inc.*, No. CV-10-63-BLJ-RFC (D. Mont. May 16, 2011), https://scholar.google.com/scholar_case?case=16367374844624649196; *Mortensen v. Bresnan Comm'n*, No. CV 10-13-BLG-RFC (D. Mont. Dec. 13, 2010), https://scholar.google.com/scholar_case?case=15661381237661199768.

41. "Reporter's Recording Guide: State-by-State Guide," Reporters Committee for Freedom of the Press, https://www.rcfp.org/reporters-recording-guide/state-state-guide.

42. *People v. Ross*, 989 N.Y.S.2d 548, 550 (Sup. Ct. App. Div. 2014), https://scholar.google.com/scholar_case?case=540787928007980376; *People v. Koonce*, 974 N.Y.S.2d 207, 209 (Sup. Ct. App. Div. 2013), https://scholar.google.com/scholar_case?case=15391160672546439819.

43. *Pica v. Pica*, 417 N.Y.S.2d 528, 529-30 (Sup. Ct. App. Div. 1979), https://scholar.google.com/scholar_case?case=9212401898816516082.

44. California Business and Professions Code §§ 17200, 17206, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=7.&chapter=5.&part=2.&lawCode=BPC.

45. Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications," California Department of Justice, February 22, 2012, https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

46. *United States v. Netyksho*, Indictment, No. 1:18-cr-00215-ABJ (July 13, 2018 D.D.C.), https://www.justice.gov/file/1080281/download.

47. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S. Department of Homeland Security, United States Computer Emergency Readiness Team, March 15, 2018 https://www.us-cert.gov/ncas/alerts/TA18-074A.

48. For a current list of sectors that the Department of Homeland Security deems to be critical infrastructure, see Presidential Policy Directive 21, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

49. State laws differ on whether these types of ancillary incentives are permissible in routine contracts.

50. "Unified Agenda of Federal Regulatory and Deregulatory Actions," General Services Administration, 83 Federal Register 1940, https://www.federalregister.gov/documents/2018/01/12/2017-28236/unified-agenda-of-federal-regulatory-and-deregulatory-actions; Defense Federal Acquisition Regulation Supplement 252.204-7012, U.S. Department of Defense, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm.

51. Sachin Bhatt and Michael Meinl, "Cybersecurity Terms and Conditions," July 26, 2016, https://www.ncmahq.org/docs/default-source/default-document-library/presentations/wc16/wc16—f11—cybersecurity-terms-and-conditions.pdf.

52. California Public Utilities Code § 761.3,https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PUC&sectionNum=761.3.; General Order No. 167, California Public Utilities Commission, November 28, 2008, http://docs.cpuc.ca.gov/PUBLISHED/GENERAL_ORDER/108114.htm.

Jonathan Mayer, Contributor

Jonathan Mayer is assistant professor of computer science and public affairs, Princeton University. Mayer is the 2017 winner of the Janice Nittoli “Forward Thinking” Award.