2016

The Privacy Policymaking of State Attorneys General

Danielle Keats Citron
University of Maryland School of Law, dcitron@law.umaryland.edu

THE PRIVACY POLICYMAKING OF STATE ATTORNEYS GENERAL

*Danielle Keats Citron**

* Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law; Affiliate Scholar, Stanford Center on Internet & Society; Affiliate Fellow, Yale Information Society Project; Senior Fellow, Future of Privacy Forum. This Article received the *International Association of Privacy Professionals* Best Paper award at the 2016 Privacy Law Scholars Conference. I owe special thanks to Chris Hoofnagle, Neil Richards, and Daniel Solove for commenting on several drafts and to Chris Wolf for his wisdom. This Article benefited from the insights of California Attorney General (AG) Kamala Harris, former Maryland AG Douglas Gansler, Connecticut AG George Jepsen, Illinois AG Lisa Madigan, and Indiana AG Greg Zoeller; current and former AG staff Nathan Blake, Sara Cable, Linda Conti, Justin Erlich, Matt Fitzsimmons, Deborah Hagan, Susan Henrichsen, Erik Jones, Ryan Kriger, Taren Langford, Travis LeBlanc, Michele Lucan, Kathleen McGee, Joanne McNabb, Steve Ruckman, Paula Selis, Melissa Szozda Smith, Matt Van Hise, and Christian Wright; privacy practitioners Julie Brill, Tanya Forsheit, Jim Halpert, Erik Jones, Michelle Kisloff, Jeff Rabkin, Divonne Smoyer, and Kurt Wimmer; colleagues Jessica Bulman-Pozen, Ryan Calo, Julie Cohen, Neal Devins, Andrew Ferguson, Susan Freiwald, Don Gifford, Mike Greenfield, James Grimmelmann, Woodrow Hartzog, Hosea Harvey, Leslie Meltzer Henry, David Hoffman, Margot Kaminski, Orin Kerr, Pauline Kim, Lee Kovarsky, David Law, Tom Lin, Kevin Linskey, William McGeveran, Deirdre Mulligan, Frank Pasquale, Priscilla Regan, Gilad Rosner, Paul Schwartz, Cathy Sharkey, Nancy Staudt, David Super, Peter Swire, Omer Tene, and Felix Wu; privacy advocates Dissent Doe, Claire Gartland, Bob Gellman, Caitriona Fitzgerald, Beth Givens, Jules Polonetsky, Marc Rotenberg, and Jeramie Scott; participants in the Future of Privacy Forum Roundtable, Cardozo Law School's Data Security Conference, DePaul Law School's Clifford Symposium on Data Breaches and Corporate Responsibility, 2016 Privacy Law Scholars Conference, Electronic Privacy Information Center's Big Ideas session, Washington University School of Law's faculty workshop, Temple University School of Law's faculty workshop, and the 2016 Privacy and Security Forum. The Future of Privacy Forum kindly gave me a home during my 2015–2016 sabbatical. Camilla Tubbs, Jenny Rensler, Frank Lancaster, Kristen Bertch, Hector DeJesus, Dan Kaprow, Cassie Mejias, David Maher, and Alex Stern provided indispensable research assistance. Susan McCarty, as always, lent her keen editing eye and citation expertise. Dean Donald Tobin, Associate Dean Max Stearns, and Associate Dean Barbara Gontrum supported this project. I am ever grateful to Audrey Beck, Jeffrey Schmidt, and the editorial staff of the *Notre Dame Law Review*.

ABSTRACT

Accounts of privacy law have focused on legislation, federal agencies, and the self-regulation of privacy professionals. Crucial agents of regulatory change, however, have been overlooked: the state attorneys general (AGs). This Article is the first in-depth study of the privacy norm entrepreneurship of state attorneys general. Because so little has been written about this phenomenon, I engaged with primary sources by examining documentary evidence received through Freedom of Information Act (FOIA) requests submitted to attorney general offices around the country and interviewing state attorneys general and current and former career staff.

Much as Justice Louis Brandeis imagined states as laboratories of the law, offices of state attorneys general have been laboratories of privacy enforcement. State attorneys general have been nimble privacy enforcers whereas federal agencies have been more constrained by politics. Local knowledge, specialization, multistate coordination, and broad legal authority have allowed AG offices to fill in gaps in the law. State attorneys general have established baseline fair-information protections and expanded the frontiers of privacy law to cover sexual intimacy and youth. Their efforts have reinforced and strengthened federal norms, further harmonizing certain aspects of privacy and data security policy.

Although certain systemic practices enhance AG privacy policymaking, others blunt its impact, including an overreliance on weak informal agreements and a reluctance to issue closing letters identifying data practices that comply with the law. This Article offers ways state attorneys general can function more effectively through informal and formal proceedings. It addresses concerns about the potential pile-up of enforcement activity, federal preemption, capture, and the dormant Commerce Clause. It urges state enforcers to act more boldly in the face of certain shadowy data practices.

INTRODUCTION

Accounts of privacy law have focused on legislation,[1] federal agencies,[2] and the self-regulation of privacy professionals.[3] Crucial agents of regulatory change, however, have been neglected: the state attorneys general. This Article fills that void with the first in-depth study of the privacy policymaking of state attorneys general.

The privacy norm entrepreneurship of state attorneys general is ripe for assessment. In the past fifteen years, attorneys general have devoted significant time and energy to privacy and data security enforcement. State attorneys general have worked on privacy and data security issues individually,

1 *See, e.g.*, Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 LEWIS & CLARK L. REV. 595 (2016); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009) [hereinafter Schwartz, *Preemption and Privacy*]; Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY 324 (Beate Roessler & Dorota Mokrosinska eds., 2015) [hereinafter Schwartz, *The Value of Privacy Federalism*].

2 *See, e.g.*, CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015) [hereinafter Hartzog & Solove, *Scope and Potential*]; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) [hereinafter Solove & Hartzog, *New Common Law of Privacy*].

3 *See, e.g.*, KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 21 (2015); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249–50 (2011).

collectively, and through the National Association of Attorneys General (NAAG).[4] The Privacy Working Group, coordinated by NAAG, has enabled offices to share expertise and resources.[5] Some offices have led the charge;[6] others have played a supporting role by joining multistate efforts.[7]

State attorneys general have been on the front lines of privacy enforcement since before the intervention of federal agencies.[8] In the 1990s, while the Federal Trade Commission (FTC) was emphasizing self-regulation, state attorneys general were arguing that consumer protection laws required the adoption of Fair Information Practice Principles (FIPPs).[9] Then, as now,

4 NAAG, a professional membership organization, helps organize multistate litigation, develop model statutes and best practices, and write reports articulating a common approach amongst the states. *See* STATE ATTORNEYS GENERAL: POWERS AND RESPONSIBILITIES 246 (Emily Myers & Nat'l Ass'n of Att'ys Gen. eds., 3d ed. 2013) [hereinafter STATE ATTORNEYS GENERAL].

5 *See, e.g.*, Telephone Interview with Matthew Fitzsimmons, Head of Privacy and Data Sec. Div., Office of the Att'y Gen. of Conn. (July 20, 2015) [hereinafter Fitzsimmons Interview]; Telephone Interview with Deborah Hagan, Bureau Chief of Consumer Prot. Div., Office of the Att'y Gen. of Ill., and Matthew Van Hise, Assistant Att'y Gen. and Head of Privacy and Identity Theft Group, Office of the Att'y Gen. of Ill. (July 30, 2015) [hereinafter Hagan & Van Hise Interview]. Connecticut Assistant AG Matthew Fitzsimmons and Illinois Assistant AG Matthew Van Hise co-lead the NAAG Privacy Working Group. *See* Fitzsimmons Interview, *supra*; Hagan & Van Hise Interview, *supra*.

6 Offices taking the lead on privacy and data security enforcement include California, Connecticut, Illinois, Indiana, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Texas, Vermont, and Washington. *See, e.g.*, Divonne Smoyer et al., *Beware the Growth of State AG Enforcement Efforts*, CORP. COUNS. (May 22, 2015), http://www.corpcounsel.com/id=1202727264255/Beware-the-Growth-of-State-AG-Enforcement-Efforts.

7 *See infra* note 52 and accompanying text (explaining that twenty-seven states have participated in one or more multistate investigations in the past five years).

8 Denise Gellene, *Chalk One up for Privacy: American Express Will Inform Cardholders That It Sorts Them for Sales Pitches*, L.A. TIMES (May 14, 1992), http://articles.latimes.com/1992-05-14/business/fi-3033_1_american-express (noting that New York AG Robert Abrams investigated credit card companies for failing to inform consumers that their shopping patterns were being used to categorize them for advertising campaigns in violation of state consumer protection law); Chris Woodyard, *Lungren Joins Suit Accusing TRW of 'Illegal Practices'*, L.A. TIMES (July 9, 1991), http://articles.latimes.com/1991-07-09/business/fi-2151_1_trw-s-credit (explaining that attorneys general sued a major credit-reporting agency for failing to prevent errors in credit reports and selling consumers' data to marketers); Telephone Interview with Susan Henrichsen, Cal. Assistant Att'y Gen. 1990–2005 (July 14, 2015) [hereinafter Henrichsen Interview] (explaining that the privacy enforcement actions in the 1990s involved credit-reporting agencies, telemarketing, spam, browser cookies, and spyware).

9 *See, e.g.*, Chris Oakes, *Michigan Warns Sites on Privacy*, WIRED (June 14, 2000), http://archive.wired.com/politics/law/news/2000/06/36967?currentPage=all (describing lawsuits brought by the Michigan Attorney General's Office against four websites, including a medical site, a financial site, a children's site, and an adult site, alleging that collection of personal data without notice violated state consumer protection law); *see also* Dee-Ann Durbin, *Privacy Rights on Web Sought: State Attorneys General Take Lead on Privacy*, LEDGER (Feb. 10, 2001), https://news.google.com/newspapers?nid=1346&dat=20010210&id=uC

state unfair and deceptive trade acts and practices laws (known as "UDAP laws") were central to privacy-related enforcement activity.

In certain areas, the proactivity of state attorneys general has preceded that of their federal regulatory counterparts. Their offices established baseline protections for privacy policies, data-breach notification, do-not-track browser settings, and certain uses of bank-history databases.[10] Even as attorneys general shaped conceptions of what privacy enforcement should achieve, they extended privacy enforcement to new frontiers, including sexual intimacy and youth.[11]

State attorneys general have been nimble privacy enforcement pioneers, a role that for practical and political reasons would be difficult for federal agencies to replicate. Because attorneys general do not have to wrestle with the politics of agency commissioners or deal with layers of bureaucracy, they can move quickly on privacy and data security initiatives. Career staff have developed specialties and expertise growing out of a familiarity with local conditions and constituent concerns. Because attorneys general are on the front lines, they are often the first to learn about and respond to privacy and security violations. Because constituents express concern about privacy and data security, so in turn do state attorneys general who tend to harbor ambitions for higher office.

This is an auspicious time to study the contributions of state privacy enforcers. Even as Congress has been mired in gridlock, attorneys general have helped fill gaps in privacy law through legislation, education, and enforcement. They have worked with state lawmakers on consumer privacy issues. AG offices have set privacy and security norms in the absence of federal leadership, a trend that may escalate in the coming years.[12] They have

JOAAAAIBAJ&sjid=eP0DAAAAIBAJ&pg=6251,6993124&hl=en (reporting that a multistate group sued banks for selling customers' confidential information without express permission in violation of state unfair and deceptive practice laws, and that browser providers were investigated for failing to give consumers notice and the chance to opt out of the tracking of their online activities).

10 FIPPs' protections enhance individuals' ability to control the extent to which their personal data is collected, used, and shared. *See* BAMBERGER & MULLIGAN, *supra* note 3, at 21. FIPPs include providing notice to data subjects, securing consent for data practices, ensuring data security, and securing opportunities for people to check the accuracy of data held about them. *Id.* at 22.

11 *See infra* subsections II.B.5–6.

12 Given the impending presidential administration of Donald Trump and the Republican Party's control of both Houses of Congress, federal agencies like the FTC and FCC will likely slow down their consumer privacy enforcement efforts. *See* Jedidiah Bracy, *What Will a Trump Administration Mean for Privacy*, IAPP (Nov. 10, 2016), https://iapp.org/news/a/what-will-a-trump-administration-mean-for-privacy/. There are three open commissioner seats (of five) at the FCC and two open seats (of five) at the FTC, as well as the seat of outgoing Chairwoman Edith Ramirez, which will be filled by President-elect Trump. *Id.* The Consumer Financial Protection Bureau (CFPB), an agency created by the Dodd-Frank Wall Street Reform Act, could be dramatically reshaped, as promised by Republican lawmakers, as might its role in enforcing the Fair Credit Reporting Act, the first federal privacy law passed in 1970. *See* James Rufus Koren, *Trump Administration Could Upend Post-*

reinforced and strengthened federal norms on data security among other issues. As California's Attorney General Kamala Harris aptly put it, "We are at an important inflection point, a convergence of AG interest in consumer protection, emerging technologies, and data privacy."[13] The result is the emergence of stronger privacy and data security protections.

This Article has three Parts. Part I provides an overview of the state attorney general's consumer-privacy mission. It identifies AG offices leading consumer privacy efforts and offices supporting their work. Part II describes the regulatory tools available to states to shape privacy practices. Then, it documents key areas where offices of attorneys general have set, shaped, and entrenched privacy and data security norms. Part III evaluates the strengths and weaknesses of AG privacy policymaking and offers suggestions for improvement. It addresses concerns about the potential pile-up of enforcement activity and interest group capture. It explores limits imposed by federal preemption and dormant Commerce Clause doctrine. Part III ends with suggestions about potential new directions for privacy enforcement.

Before turning to my analysis, let me explain my methodology. Because so little had been written about the privacy enforcement of state attorneys general, my research focused on primary sources. I filed open sunshine requests with AG offices around the country. FOIA requests sought materials related to AG offices' education campaigns, legislative efforts, and enforcement activity related to consumer privacy and data security.[14] An overwhelming majority of states responded, providing crucial evidence of AG privacy policymaking.[15]

To put into context the material obtained through FOIA requests, I conducted semi-structured interviews with state attorneys general from four states and former and current career staff from thirteen states.[16] Interviews

---

Crisis Finanical Reforms, Weaken CFPB, L.A. TIMES (Nov. 22, 2016), http://www.latimes.com/business/la-fi-trump-dodd-frank-20161109-story.html.

13 Interview with Kamala Harris, Attorney Gen., Office of the Att'y Gen. of Cal., in L.A., Cal. (Oct. 13, 2015) [hereinafter Harris Interview]; *see also* Paul Pittman, *State Attorneys General Emerge as Enforcers for Consumer Data Privacy*, CYBERSECURITY TODAY (Feb. 7, 2014), http://www.cybersecuritytodayblog.com/2014/02/07/state-attorneys-general-emerge-as-enforcers-for-consumer-data-privacy/.

14 A sample FOIA request letter is included in Appendix I.

15 Appendix II lists the responses to my FOIA requests. Forty-two states and one territory provided responsive materials. *See* Appendix II. In accord with their open sunshine laws, four states—Alabama, Arkansas, Tennessee, and Virginia—denied my request because I am not a state citizen. *Id.* Two states—New Jersey and South Dakota—and five of the six territories never responded to my request. *Id.* Two states conditioned a response on my payment of significant fees ($263.79 for Montana, and $4255.76 for Nebraska) despite my request as an academic for a waiver of the fee. *Id.* It is easy to understand states that denied my request on the basis of state citizenship; those states owe no obligation of transparency to noncitizens. The fees asserted by Montana and Nebraska, however, seemed exorbitant because independent research suggested that neither state had considerable material to disclose.

16 I conducted in-person interviews with California AG Kamala Harris and Connecticut AG George Jepsen and telephone interviews with Indiana AG Greg Zoeller and former

focused on the following questions: In what respect has the AG's office worked on consumer privacy and data security concerns? How do privacy and data security issues come to your office's attention? Has the office worked on proposed state or federal privacy and data security legislation? Does the office devote resources to educating consumers and companies about best practices? Does the office meet with companies to discuss privacy and data security? Are particular investigative techniques and litigation strategies more effective than others? What legal authority does the office rely on when pursuing privacy and data security investigations? Are current laws, notably UDAP laws, sufficient to the task? What has been the office's role in multistate investigations concerning consumer privacy and data security? What are the strengths and weaknesses of informal agreements versus litigation? To what extent has the office worked with federal agencies on privacy and data security issues? Do staff have privacy training or expertise? Does the office have technical experts in house or on retainer? How have the FTC's guidance and white papers influenced enforcement activity? In what areas does the office look to the FTC or other federal agencies for guidance and leadership?

Interviews with career staff varied from interviews with state attorneys general. Discussions with staff tended to focus on the day-to-day experience of working on privacy and data security issues. Staff discussed the enforcement process, including the ins and outs of investigations, pros and cons of enforcement strategies, and practical challenges. They talked about their offices' legislative work and education efforts. Interviews with attorneys general focused on the bigger picture—the office's goals and priorities for privacy enforcement, the practical limits of their work, and the substantive areas in which their activity has had the biggest impact. Public comments of attorneys general and staff, views of privacy professionals, media coverage of AG enforcement, and scholarly perspectives on the work of attorneys general also informed my analysis.

I. The People's Privacy Lawyers

The office of the state attorney general has deep roots in American history. All thirteen colonies had offices of attorneys general whose role was to represent the sovereign in England.[17] After the Revolution, these offices were reestablished as state attorneys general under state constitutions or state

Maryland AG Douglas Gansler. *See* Appendix II. I conducted in-person and telephone interviews with former and current AG staff from Arizona, California, Connecticut, Delaware, Illinois, Iowa, Maine, Maryland, Massachusetts, New York, Ohio, Vermont, and Washington. *Id.* As former FTC Commissioner Julie Brill wisely noted while moderating a discussion of this Article at the 2016 Privacy Law Scholars Conference, there are natural limits to any effort to interview attorneys general and staff. As she said well, one can only get the access that one can get. Comment of Julie Brill, Privacy Law Scholars Conference, Wash., D.C. (June 2, 2016).

17 *See* Johnson v. Commonwealth *ex rel.* Meredith, 165 S.W.2d 820, 826 (Ky. Ct. App. 1942).

statutes.[18] Today, all fifty states and six territories have an office of attorney general or its functional equivalent.[19]

The vast majority of attorneys general are publicly elected.[20] In designing a popularly elected AG's office, states aimed to "weaken the power of a central chief executive and further an intrabranch system of checks and balances."[21] The popular election of attorneys general helped reinforce federalism's commitment to enhance governmental responsiveness to local priorities.[22]

A crucial part of an attorney general's work as the state's chief law enforcer involves protecting the public interest.[23] As this Part explores, in the mid- to late-twentieth century, AG offices took up the mantle of consumer protection, which grew to include privacy and data security concerns. This Part identifies the core group of offices that have taken the lead on privacy enforcement and the significant number of offices that have supported those efforts.

A. Consumer Protection Mission

In the late 1960s and 1970s, state attorneys general embraced their role as consumer watchdog. An important first step was the establishment of consumer protection divisions.[24] Frank Kelley, who served as Michigan Attorney

18 *See* STATE ATTORNEYS GENERAL, *supra* note 4, at 33–37.

19 *See* Cornell W. Clayton, *Law, Politics and the New Federalism: State Attorneys General as National Policymakers*, 56 REV. POL. 525, 527 (1994).

20 *See* Colin Provost, *An Integrated Model of U.S. State Attorney General Behavior in Multi-State Litigation*, 10 STATE POL. & POL'Y Q. 1, 2–3 (2010). Attorneys general are popularly elected in forty-three states, Guam, and the District of Columbia; they are appointed by governors in Alaska, Hawaii, New Hampshire, New Jersey, Wyoming, American Samoa, Northern Mariana Islands, Puerto Rico, and the Virgin Islands. *See* STATE ATTORNEYS GENERAL, *supra* note 4, at 12 n.2. The attorney general of Maine is selected by a secret ballot of the legislature. *Id.* at 12.

21 William P. Marshall, *Break Up the Presidency? Governors, State Attorneys General, and Lessons from the Divided Executive*, 115 YALE L.J. 2446, 2451 (2006). Most attorneys general are independent of the governor's office. *See* Neal Devins & Saikrishna Bangalore Prakash, *Fifty States, Fifty Attorneys General, and Fifty Approaches to the Duty to Defend*, 124 YALE L.J. 2100, 2124 (2015). In six states, attorneys general are members of the governor's cabinet: Alaska, Arizona, Florida, Hawaii, Michigan, and New Jersey. Clayton, *supra* note 19, at 529. The AG's Office of the District of Columbia became an independent agency in 2015 after previously being subordinate to the District's executive branch. *See* Divonne Smoyer & Kimberly Chow, *Q&A: DC Attorney General Karl Racine Talks Consumer Privacy*, IAPP (Apr. 26, 2016), https://iapp.org/news/a/qa-dc-attorney-general-karl-racine-talks-consumer-privacy/.

22 *See* Devins & Prakash, *supra* note 21, at 2125 n.78.

23 *See, e.g.*, State v. Culp, 823 So. 2d 510, 514 (Miss. 2002). *See generally* Trevor W. Morrison, *The State Attorney General and Preemption*, *in* PREEMPTION CHOICE: THE THEORY, LAW, AND REALITY OF FEDERALISM'S CORE QUESTION 81, 85 (William W. Buzbee ed., 2009) [hereinafter PREEMPTION CHOICE].

24 FRANK J. KELLEY & JACK LESSENBERRY, THE PEOPLE'S LAWYER: THE LIFE AND TIMES OF FRANK J. KELLEY, THE NATION'S LONGEST-SERVING ATTORNEY GENERAL 84 (2015).

General from 1961 to 1999, explained that one of his first acts in office was starting a consumer protection division.[25]

Passing supportive legislation was the next step. With the encouragement of the FTC and attorneys general, states adopted UDAP laws.[26] Much like section 5 of the Federal Trade Commission Act,[27] the typical UDAP law bans deceptive commercial acts and practices and unfair trade acts and practices whose costs exceed their benefits.[28] UDAP laws empower attorneys general to seek civil penalties, injunctive relief, and attorneys' fees and costs.[29]

AG offices started focusing on privacy issues in the 1990s. Early enforcement actions targeted intrusive telemarketing, spam, spyware, and the absence of privacy policies.[30] Attorneys general relied on UDAP laws and their common law authority to protect consumers from privacy-invasive business practices.[31] Over the years, AG enforcement power has expanded with the passage of specific privacy and data security laws, many of which were proposed or endorsed by state attorneys general.[32] Although those laws have been helpful, UDAP laws remain crucial to AG privacy enforcement.[33]

---

25 *See id.*; *see also* Dale A. Reinholtsen, *The Role of California's Attorney General and District Attorneys in Protecting the Consumer*, 4 U.C. DAVIS L. REV. 35, 43 (1971) (discussing how the California Consumer Fraud Unit was established in 1959 to protect consumers from unfair, fraudulent, or deceptive business practices).

26 KELLEY & LESSENBERRY, *supra* note 24, at 101–02 (explaining that Frank Kelley helped convince Michigan lawmakers to pass his state's consumer protection act in 1976). Texas AG John Hill's office helped draft the state Deceptive Trade Practices Act, which passed in 1973. *See* JOHN HILL, JR. & ERNIE STROMBERGER, JOHN HILL FOR THE STATE OF TEXAS: MY YEARS AS ATTORNEY GENERAL 17–33 (2008); *see also* Robert Morgan, *The People's Advocate in the Marketplace—The Role of the North Carolina Attorney General in the Field of Consumer Protection*, 6 WAKE FOREST INTRAMURAL L. REV. 1, 4 (1969) (discussing his role, as the AG of North Carolina, in lobbying the state legislature to adopt a broad UDAP law so his office could serve as the "consumers' advocate").

27 15 U.S.C. § 45 (2012).

28 However, some UDAP laws diverge from the wording of section 5, with some states banning unfair trade practices without requiring proof of consumer harm. *See, e.g.*, CONN. GEN. STAT. ANN. § 42-110m (West 2016); MASS. GEN. LAWS ANN. ch. 93A, § 4 (West 2016). Others only ban deceptive trade practices. *See* STATE ATTORNEYS GENERAL, *supra* note 4, at 232.

29 *See, e.g.*, California Unfair Business Act, CAL. BUS. & PROF. CODE § 17206 (West 2016) (imposing $2500 per violation); Illinois Consumer Fraud Act, 815 ILL. COMP. STAT. ANN. 505/7 (West 2016) (allowing civil penalty of $50,000 per unlawful act); *see also* Steven J. Cole, *State Enforcement Efforts Directed Against Unfair or Deceptive Practices*, 56 ANTITRUST L.J. 125, 128 (1987) (explaining that in states like Maryland the "consumer protection authority resides wholly within the Attorney General's Office").

30 Henrichsen Interview, *supra* note 8.

31 *See infra* note 288 and accompanying text.

32 *See, e.g.*, CAL. CONST. art. 1, § 1; Sheehan v. S.F. 49ers, 201 P.3d 472, 479 (Cal. 2009) (holding the right to privacy applies to state actors and private parties).

33 *See, e.g.*, Telephone Interview with Nathan Black, Assistant Att'y Gen., Office of the Att'y Gen. of Iowa (June 21, 2016).

B. The Privacy Enforcers

In the past fifteen years, a core group of states have taken the lead on privacy enforcement: California, Connecticut, Illinois, Indiana, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Texas, Vermont, and Washington.[34] Their offices have spearheaded multistate investigations on privacy and data security matters.[35] They have active individual enforcement dockets. Their offices have worked on privacy and data security legislation; they have educated consumers and businesses about best practices.[36]

Because privacy and data security investigations often involve complicated technical questions, privacy leaders have "brought expertise in-house."[37] Some have hired technologists and have computer labs onsite; others have partnered with computer science departments at local universities.[38] Thanks to funding secured through multistate agreements, AG staff have undergone training with the International Association of Privacy Professionals; many have been certified as privacy professionals.[39]

The FTC—with its extensive technical and policy expertise—has been a crucial source of inspiration for state attorneys general. The FTC's policy reports and research have inspired states to devote resources to investigating certain data practices.[40] FTC policy has been particularly influential in

34 *See infra* notes 43–50, 134, 156, 219, 227, 264–65, 268–70 and accompanying text (discussing the work and activism of state attorneys general).

35 For some privacy leaders, the bulk of enforcement activity related to privacy is spent on multistate investigations. Ohio, for instance, recently led a multistate investigation into the systematic failure of credit-reporting agencies to correct inaccurate credit reports. *See* Press Release, Office of the Att'y Gen. of Ohio, Attorney General DeWine Announces Major National Settlement with Credit Reporting Agencies (May 20, 2015), http://www.ohioattorneygeneral.gov/Media/News-Releases/May-2015/Attorney-General-DeWine-Announces-Major-National-S; FOIA Response Letter from Erin Leahy (June 24, 2016) (Ohio) (on file with author). Pennsylvania has served on the executive committee of several multistate investigations. *See* FOIA Response Letter from Robert A. Muller (Dec. 22, 2015) (Pennsylvania) (on file with author). As explored in Part II, other privacy leaders have devoted significant resources to both individual and multistate investigations.

36 *See infra* notes 375–88 and accompanying text (discussing data security and privacy enforcement actions and resulting AVCs or consent judgments).

37 Harris Interview, *supra* note 13. AG Harris's first technical consultant was Ashkan Soltani, who went on to lead the FTC's Technology Unit. *Id.*

38 *See, e.g.*, Telephone Interview with Ryan Kriger, Assistant Att'y Gen., Office of the Att'y Gen. of Vt. (Sept. 21, 2015) [hereinafter Kriger Interview] (explaining that Vermont AG's Office has partnered with Norwich University's computer science department and has a computer science professor on retainer); Telephone Interview with Paula Selis, Chief of High Tech Unit, Office of the Att'y Gen. of Wash. (June 30, 2015) [hereinafter Selis Interview].

39 *See, e.g.*, Kriger Interview, *supra* note 38. Vermont Assistant AG Ryan Kriger helped coordinate the privacy training of forty-four lawyers from offices around the country with funds from the TJX multistate settlement. *See id.*

40 *See infra* note 222 and accompanying text (discussing how an FTC report inspired the New York Attorney General's Office's investigation of credit-reporting agencies).

states' approach to data security investigations. As former Maryland Assistant Attorney General Steven Ruckman explained, the FTC has served as the "mother ship" on data security issues because it has unique technical know-how that would be hard to reproduce at the state level.[41] AG staff have looked to the FTC's privacy jurisprudence in interpreting their own UDAP laws.[42]

Privacy has been built into the infrastructure of leading privacy offices. California has a privacy enforcement and protection unit in the Consumer Protection Bureau and an e-crime unit in the Criminal Division.[43] Illinois has a privacy and identity theft group in the Consumer Protection Division.[44] New York has an Internet bureau with six attorneys and a data security technologist.[45] Ohio and Indiana have identity theft units in their consumer protection divisions.[46] Connecticut was the first to establish an independent privacy division whose head reports directly to the attorney general.[47] Connecticut AG George Jepsen started a privacy task force in 2011,[48] which was turned into a separate division in 2015.[49] Two full-time attorneys and three part-time staff work in the Office's Privacy and Data Security Division.[50]

41 *See* Interview with Steven Ruckman, former head of Privacy Unit, Office of the Att'y Gen. of Md., in Wash., D.C. (Sept. 11, 2015) [hereinafter Ruckman Interview].

42 *See id.* As Part II documents, AG offices have not simply followed the lead of federal agencies. In important areas, they have set privacy policy in the absence of federal norms; in others, they have pressed the FTC to offer greater privacy protections to consumers than those afforded by federal agencies. In the near future, there may be more aggressive state AG privacy and data security enforcement than enforcement activity at the federal level.

43 *See* Telephone Interview with Joanne McNabb, Chief Privacy Educator, Cal. Att'y Gen. Privacy Unit (Mar. 3, 2015) [hereinafter McNabb Interview Mar. 3]; Press Release, Office of the Att'y Gen. of Cal., Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit (July 19, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

44 *See Office of the Ill. Att'y Gen.: Identity Theft Hotline*, ILL. ATT'Y GEN., http://www.illinoisattorneygeneral.gov/consumers/hotline.html (last visited Oct. 17, 2016).

45 *See* Telephone Interview with Kathleen McGee, Chief of Internet Bureau, Office of the Att'y Gen. of N.Y. (Dec. 8, 2015) [hereinafter McGee Interview].

46 *See* Telephone Interview with Melissa Szozda Smith, Assistant Att'y Gen. and Dir. of Identity Theft Unit, Office of the Att'y Gen. of Ohio (June 30, 2016); Divonne Smoyer & Paul Bond, *Q&A: Indiana AG on Initiatives, Priorities for Privacy Protection*, IAPP (May 27, 2014), https://iapp.org/news/a/q-a-indiana-ag-on-initiatives-priorities-for-privacy-protection/.

47 *See* George Jepsen, *Attorney General: AG's Focus Ranges from Data Breaches to Health Care*, CONN. L. TRIB. (Jan. 11, 2016), http://www.ctlawtribune.com/id=1202746783002/Attorney-General-AGs-Focus-Ranges-From-Data-Breaches-to-Health-Care?mcode=0&curindex=0.

48 *See Christian Nolan, With New Unit, Conn. AG's Office Ratchets up Focus on Data Breaches*, CONN. L. TRIB. (Mar. 13, 2015), http://www.ctlawtribune.com/id=1202720556511/With-New-Unit-Conn-AGs-Office-Ratchets-Up-Focus-on-Data-Breaches?slreturn=20160028122934.

49 *See* Interview with George Jepsen, Att'y Gen., Office of the Att'y Gen. of Conn., in Hartford, Conn. (Jan. 7, 2015) [hereinafter Jepsen Interview].

50 *Id.*

Having a formal privacy unit or division is not necessary for a state attorney general to take a leading role on consumer privacy matters. Massachusetts has aggressively pursued data security investigations without having a dedicated privacy unit or division. Experienced career staff and supportive attorneys general have been crucial to the office's work on security and privacy issues.[51] Nonetheless, the creation of privacy units and the hiring of technical experts have solidified many offices' commitment to privacy and data security enforcement.

In the past five years, twenty-seven states have joined one or more multistate investigations spearheaded by privacy pioneers.[52] They contribute to

51 This is certainly true of Massachusetts Assistant AG Sara Cable, who worked for AG Martha Coakley during her tenure (2007–2015) and now works for AG Maura Healey (2015–present). Of course, outgoing attorneys general cannot control the agendas of their successors. During his tenure, Maryland AG Doug Gansler (2007–2015) established an Internet Privacy Unit with a special focus on youth privacy. *See* Ruckman Interview, *supra* note 41. AG Gansler made data privacy his key initiative when serving as president of NAAG. *See* Telephone Interview with Douglas Gansler, Former Att'y Gen., Office of the Att'y Gen. of Md. (Aug. 31, 2016). When AG Gansler's term ended, his chief of the Internet Privacy Unit went into private practice. *See* Ruckman Interview, *supra* note 41. Privacy continues to be a part of the Office's work, but time will tell if it remains a central mission of the Office.

52 *See, e.g.*, FOIA Response Letter from Craig W. Richards (Dec. 8, 2012) (Alaska) (on file with author) (providing materials showing individual and multistate enforcement activity); FOIA Response Letter from Bethany Diaz (Jan. 12, 2016) (Arizona) (on file with author) (same); FOIA Response Letter from Stefanie Mann (Dec. 3, 2015) (Colorado) (on file with author) (providing materials showing it was a signatory to multistate AVCs but not individual enforcement actions); FOIA Response Letter from Tony Towns (July 26, 2016) (District of Columbia) (on file with author) (same); FOIA Response Email from Mark Hamilton (Aug. 30, 2016) (Florida) (on file with author) (same); FOIA Response Letter from Stella Kam (Dec. 4, 2015) (Hawaii) (on file with author) (same); FOIA Response Email from Cari Sagar (Oct. 22, 2015) (Iowa) (on file with author) (same); FOIA Response Letter from Cheryl Whalen (Sept. 16, 2015) (Kansas) (on file with author) (providing materials showing both individual and multistate enforcement activity); Telephone Interview with Lonnie Styron, Office of the Att'y Gen. of La. (Feb. 3, 2016) (Louisiana) (providing materials showing it was a signatory to multistate AVCs but not individual enforcement actions); FOIA Response Letter from Linda Conti (Nov. 24, 2015) (Maine) (on file with author) (same); FOIA Response Letter from Christy Wendling-Richards (July 19, 2016) (Michigan) (on file with author) (same); FOIA Response Letter from James W. Canaday (Aug. 4, 2016) (Minnesota) (on file with author) (providing materials showing individual and multistate enforcement activity); FOIA Response Letter from Rochelle Reeves (Feb. 25, 2016) (Missouri) (on file with author) (providing materials showing it was a signatory to multistate AVCs but not individual enforcement actions); FOIA Response Letter from Laura Tucker (Sept. 11, 2015) (Nevada) (on file with author) (same); FOIA Response Email from Liz Brocker (Nov. 24, 2015) (North Dakota) (on file with author) (same); FOIA Response Letter from Aaron Cooper (Dec. 16, 2015) (Oklahoma) (on file with author) (same); Telephone Interview with Michael Kron, Office of the Att'y Gen. of Or. (Jan. 11, 2015) (Oregon) [hereinafter Kron Interview]; FOIA Response Letter from Steven A. Travis (Dec. 22, 2015) (West Virginia) (on file with author) (providing materials showing individual and multistate enforcement activity); FOIA Response Letter from Paul Ferguson (Dec. 18, 2015) (Wisconsin) (on file with author) (providing materials showing

multistate investigations by providing assistance on discovery review and other discrete assignments.[53] Their offices also have joined forces with privacy pioneers on education efforts.[54] Thus, in both leading and supporting roles, a sizeable majority of states have been engaged in privacy enforcement.[55]

II. PRIVACY AND DATA SECURITY ENFORCEMENT

This Part shows how important state attorneys general have been to U.S. privacy regulation. It sets the stage by introducing the regulatory tools available to attorneys general and an office's potential to shape privacy practices beyond its borders. Then, it documents areas where attorneys general have helped establish privacy and data security protections and areas where they have harmonized and sharpened existing federal norms. As this Part highlights, attorneys general have been most effective in influencing privacy policy when they have pursued a combination of regulatory tools.

A. Policymaking Tools and Potential Impact

State attorneys general can influence privacy policy through legislation, persuasion, and litigation. Since the 1990s, state AGs have proposed and endorsed state consumer privacy and data security laws.[56] Attorneys general

multistate activity but no individual enforcement actions); FOIA Response Letter from Ryan Schelhaas (Dec. 1, 2015) (Wyoming) (on file with author) (providing materials showing individual and multistate enforcement activity). In the past five years, Alabama, Arkansas, Montana, Nebraska, South Dakota, Tennessee, and Virginia have joined multistate consumer privacy investigations; for different reasons, they never provided a substantive response to my FOIA requests. *See supra* note 15.

53 *See, e.g.*, Telephone Interview with Linda Conti, Assistant Att'y Gen., Office of the Att'y Gen. of Maine (June 22, 2015) [hereinafter Conti Interview] (discussing her contributions to multistate investigations).

54 This is true of Missouri AG Chris Koster who has worked closely with Indiana AG Greg Zoeller to combat illegal robocalling and more generally to protect telephone privacy. *See* Alexandra Kruczek, *AG Zoeller Launches National Do Not Call Summit*, WLFI NEWS (Apr. 8, 2014), http://wlfi.com/2014/04/08/ag-zoeller-launches-national-do-not-call-program/ (reporting that AG Koster and AG Zoeller have run annual summits devoted to educating state and federal law enforcers on how to combat Do Not Call violations).

55 In response to FOIA requests, three states explained that they had no consumer privacy or data security enforcement activity in the past five years. *See* FOIA Response Letter from Daniel Walsh (Nov. 30, 2015) (Georgia) (on file with author); FOIA Response Email from James Boffetti (Nov. 30, 2015) (New Hampshire) (on file with author); FOIA Response Letter from Ché Arguello (Jan. 22, 2016) (Utah) (on file with author). In May 2016, the attorneys general of Utah and Georgia supported efforts to ban transgender individuals from using bathrooms designated for the sex of their chosen (but not birth) identity. I am grateful to Dissent Doe for pointing that out to me.

56 In many states, attorneys general are authorized to propose legislation. *See* Colin Provost, *State Attorneys General, Entrepreneurship, and Consumer Protection in the New Federalism*, 33 PUBLIUS: J. FEDERALISM 37, 39 (2003) (discussing the legislative role of attorneys general); Smoyer et al., *supra* note 6. Delaware, for instance, recently adopted four privacy and data security laws proposed by AG Matt Denn. *See* Press Release, Office of the Att'y

have extended their legislative agenda to Capitol Hill.[57] State AGs, for instance, routinely testify before congressional committees.[58]

Persuasion is another way that attorneys general can shape privacy practices.[59] Attorneys general establish task forces with business leaders, advocacy groups, and experts in the hopes that participants reach consensus on best practices.[60] They reach out to companies with concerns about products and services.[61] Staff provide advice to companies.[62] The California Attorney General's Office, for instance, has offered to review privacy policies.[63] In partnership with a local university's cyber security department, the Vermont Attorney General's Office has offered free penetration tests to businesses to identify basic security vulnerabilities.[64] Connecticut AG George Jepsen

---

Gen. of Del., Internet Privacy and Safety Agenda Becomes Law with Governor's Signature (Aug. 7, 2015), http://news.delaware.gov/2015/08/07/internet-privacy-and-safety-agenda-becomes-law-with-governors-signature/. Violations of state privacy and data security laws are usually considered per se violations of UDAP statutes.

57 *See* Clayton, *supra* note 19, at 535. Attorneys general successfully lobbied to have authority to enforce federal consumer privacy laws. *Id.*

58 *See, e.g.*, Press Release, Office of the Att'y Gen. of Conn., Attorney General Submits Testimony Calling on Congress to Institute Internet Do-Not-Track (Dec. 2, 2010), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=469312.

59 *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 35 (1992); Telephone Interview with Sara Cable, Assistant Att'y Gen., Office of the Att'y Gen. of Mass. (Aug. 13, 2015) [hereinafter Cable Interview]; Fitzsimmons Interview, *supra* note 5; Hagan & Van Hise Interview, *supra* note 5; Kriger Interview, *supra* note 38; Telephone Interview with Joanne McNabb, Chief Privacy Educator, Cal. Att'y Gen.'s Privacy Unit (July 20, 2015) [hereinafter McNabb Interview July 20]; Ruckman Interview, *supra* note 41; Selis Interview, *supra* note 38.

60 *See infra* notes 182–86 and accompanying text (discussing California AG Kamala Harris's reliance on her power to convene to change practices concerning mobile privacy and exploitation of nonconsensual pornography); *see also* Divonne Smoyer & Christine Czuprynski, *Q&A: Connecticut AG Talks Privacy Enforcement, Collaboration with the FTC*, IAPP (Aug. 26, 2014), https://iapp.org/news/a/qa-connecticut-ag-talks-privacy-enforcement-collaboration-with-the-ftc/ (explaining how after meetings with Connecticut AG George Jepsen, Google agreed to review the privacy implications of any app using facial recognition software on Google Glass). As Part III explores, informal agreements lack the force of law, though violations can be the basis of a subsequent lawsuit. Part III assesses the weaknesses of those agreements and prescribes solutions. *See infra* Part III.

61 *See, e.g.*, Letter from George C. Jepsen, Att'y Gen., State of Conn., to Tim Cook, CEO, Apple, Inc. (Sept. 12, 2014), http://www.ct.gov/ag/lib/ag/press_releases/2014/20140912_applewatchletter.pdf (requesting a meeting to discuss Apple Watch's storage of personal and health information and its review of applications' privacy policies to ensure safeguarding of users' health information); Jepsen Interview, *supra* note 49.

62 *See, e.g.*, Cable Interview, *supra* note 59.

63 *See* Vindu Goel, *California Urges Websites to Disclose Online Tracking*, N.Y. TIMES: BITS BLOG (May 21, 2104, 12:00 AM), http://bits.blogs.nytimes.com/2014/05/21/california-urges-websites-to-disclose-online-tracking/?_r=0 (explaining that the California AG's Office "would review companies' privacy policies and work with them to make sure they followed the new law").

64 Press Release, Office of the Att'y Gen. of Vt., Attorney General Sorrell Announces Vermont Cyber Security Project (July 9, 2012) [hereinafter Vermont Cyber Security Project

explained it is more efficient to help companies ensure their privacy and security policies comply with the law than to catch them after they have broken it.[65]

Another important strategy is the issuance of best practice guides.[66] Guidance documents explain an attorney general's understanding of privacy and data security laws.[67] They provide examples of practices that would be considered unfair and deceptive. In preparing guides, staff consult with stakeholders from a broad range of interests.[68] Massachusetts Assistant AG Sara Cable explained, "We want companies to tell us how we can be clear about what we expect and how that clarity can help them satisfy the law and innovate."[69] Stakeholder meetings can involve dozens of participants: the goal is to get as many perspectives as possible.[70] AG offices educate stakeholders about best practices.[71] The California Attorney General's Office held workshops featuring developers talking about how they dealt with privacy concerns in designing mobile apps.[72] Joanne McNabb, the Office's Chief Privacy Educator, explained that "a key part of the education process was having the audience at workshops hear from peers about how they complied with the law."[73]

Publicity is another way to encourage compliance. Attorneys general discuss privacy and data security lapses with the public to change the social meaning of problematic behavior.[74] To retain consumers' trust and contain reputational damage, companies bring their practices into line with the law.[75]

Announcement], http://ago.vermont.gov/focus/news/attorney-general-sorrell-announces-vermont-cyber-security-project.php.

65 *See* Jepsen Interview, *supra* note 49. Not all offices, however, have the inclination or bandwidth to provide retail advice to companies. *See, e.g.*, IDAHO ATT'Y GEN., IDAHO CONSUMER PROTECTION MANUAL 5 (2015) [hereinafter IDAHO ATT'Y GEN.], http://www.ag.idaho.gov/publications/consumer/ConsumerProtectionManual.pdf.

66 *See, e.g.*, McNabb Interview July 20, *supra* note 59 (discussing how California has released best practice guides focused on mobile app developers, healthcare providers, cyber security for small-to-medium businesses, and the development of privacy policies). Consumers are also the audience for the state's best practice guides. *See id.*

67 *See id.*

68 *See, e.g.*, McNabb Interview Mar. 3, *supra* note 43.

69 Cable Interview, *supra* note 59.

70 *See, e.g.*, McNabb Interview July 20, *supra* note 59.

71 *See, e.g.*, Press Release, Office of the Att'y Gen. of Vt., Attorney General Sorrell Announces Data Security For Small Businesses Workshop (Apr. 22, 2013), http://ago.vermont.gov/focus/news/attorney-general-sorrell-announces-data-security-for-small-businesses-workshop.php; Vermont Cyber Security Project Announcement, *supra* note 64 (discussing workshops on cyber security for small businesses held in four counties).

72 *See* McNabb Interview July 20, *supra* note 59.

73 *Id.*

74 *See* CAL. DEP'T OF JUSTICE, CAL. DATA BREACH REPORT 4 (2014) (discussing entities reporting more than one breach in 2013, including American Express, Discover Financial Services, Massachusetts Mutual Life Insurance, and Kaiser Health).

75 *See* AYRES & BRAITHWAITE, *supra* note 59, at 35–38.

When soft-law efforts fail to convince businesses to comply with the law, attorneys general may turn to litigation. Their efforts often begin with a warning letter. Warning letters routinely influence the behavior of regulated entities, eliminating the need for further action.[76] If not, attorneys general may initiate a formal investigation.[77] Indispensable to any investigation is the state AG's authority to obtain discovery before initiating a lawsuit.[78] Under their broad powers of original inquiry, attorneys general can "investigate merely on suspicion that the law is being violated, or even just because [they] want[ ] assurance that it is not."[79] Administrative subpoenas, referred to as civil investigative demands (CIDs), are crucial to investigations.[80] CIDs can be issued to individuals who are not targets of an investigation if "a reasonable basis exists to believe the non-violator possesses information relevant to the investigation."[81]

Attorneys general often join forces to investigate unfair and deceptive commercial practices affecting consumers across the country.[82] Multistate investigations are coordinated through NAAG's Privacy Working Group.[83] An attorney general's office or a group of offices (known as the executive committee) will lead an investigation.[84] In multistate actions, states file separate lawsuits, though offices collaborate on aspects of the proceedings. States issue similar requests for information, share information through common-interest agreements, and engage in joint negotiations.[85]

States—proceeding individually or as a group—often eschew formal adjudication for informal agreements that close investigations.[86] In some states, the attorney general must give an entity the chance to sign an informal agreement, often called an assurance of voluntary compliance (AVC), before pursuing litigation.[87] Under an AVC, an entity or individual typically agrees

76 *See, e.g.*, McNabb Interview Mar. 3, *supra* note 43.

77 *See, e.g.*, Commonwealth v. Pineur, 533 S.W.2d 527, 529 (Ky. 1976) ("Even if one were to regard the request for information in this case as caused by nothing more than official curiosity, nevertheless law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest." (quoting United States v. Morton Salt Co., 338 U.S. 632, 652 (1950))).

78 *See* STATE ATTORNEYS GENERAL, *supra* note 4, at 232.

79 *Morton Salt*, 338 U.S. at 642–43.

80 STATE ATTORNEYS GENERAL, *supra* note 4, at 232–33.

81 Everdry Mktg. & Mgmt., Inc. v. Carter, 885 N.E.2d 6, 10 (Ind. Ct. App. 2008).

82 Attorneys general also undertake investigations with federal agencies. *See infra* subsection III.A.3 (discussing the synergistic relationship between attorneys general and federal agencies).

83 *See* Letter from the Nat'l Ass'n of Att'ys Gen. to Cong. Leaders (July 7, 2015), http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Data%20Breach%20Notification%20Letter.pdf.

84 *See* Ruckman Interview, *supra* note 41.

85 STATE ATTORNEYS GENERAL, *supra* note 4, at 246.

86 *See* Cable Interview, *supra* note 59.

87 *See, e.g.*, IDAHO ATT'Y GEN., *supra* note 65, at 4.

to engage in, or refrain from, certain conduct and to pay a fine and attorneys' fees.[88]

Attorney general enforcement activity naturally influences private behavior within a state's borders, but it also can have an impact beyond the state. Businesses may follow the most restrictive AG-endorsed norms to avoid the costs of piecemeal compliance.[89] This dynamic allows smaller states to "punch above their weight."[90] By adopting the strictest standards, firms can operate in all jurisdictions with some assurance about legal compliance.[91]

Companies have a strong incentive to follow the regulatory standards of powerful states.[92] David Vogel has labeled this phenomenon the "California effect."[93] As Vogel explains, stronger state standards are more likely to be adopted if they emanate from powerful jurisdictions and enjoy wide support from policy groups.[94] In recognition of this phenomenon, Attorney General Harris has said: "If we can strengthen privacy protections here [in California], we can benefit consumers around the world."[95]

Attorneys general also influence each other, both in individual efforts and in multistate investigations on issues of national import. That is the upside of state experimentation as imagined by Justice Louis Brandeis:[96] pol-

88 Under most AVCs, a broken promise constitutes prima facie evidence of a legal violation. *See, e.g.*, WASH. REV. CODE ANN. § 19.16.470 (West 2016) ("[F]ailure to perform the terms of any such assurance shall constitute prima facie proof of a violation of this chapter for the purpose of securing an injunction . . . ."). Attorneys general may sue the violator, pointing to the broken promise as proof of the underlying lawbreaking. Some informal agreements, however, have more teeth: violations, if proven in court, warrant immediate relief. *See, e.g.*, Press Release, Office of the Att'y Gen. of Md., AG Gansler Secures Agreement to Protect Children on Ask.fm (Aug. 14, 2014) [hereinafter Ask.fm Settlement], http://www.marylandattorneygeneral.gov/Pages/NewsReleases/2014/081414.aspx (discussing the assurance of voluntary compliance between Maryland and Ask.fm). Part III explores the weaknesses in the typical AVC and offers solutions. *See infra* Part III.

89 *See* Hogan Lovells, *California Continues to Shape Privacy and Data Security Standards*, PRIVACY TRACKER (Oct. 1, 2013), https://privacyassociation.org/news/a/california-continues-to-shape-privacy-and-data-security-standards.

90 *See* Jepsen Interview, *supra* note 49.

91 *See* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 249–50 (1995).

92 *See id.* at 267–68.

93 *Id.* at 247–70.

94 *See id.* at 268. That bigger states have an advantage over smaller states in this way raises concerns about "horizontal aggrandizement." *See* Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. REV. 698, 751 (2011) (quoting Lynn A. Baker, *Putting the Safeguards Back into the Political Safeguards of Federalism*, 46 VILL. L. REV. 951, 955 (2001)).

95 Jessica Guynn, *Facebook to Require Privacy Policies for All Apps in App Center*, L.A. TIMES (June 22, 2012), http://articles.latimes.com/2012/jun/22/business/la-fi-facebook-ag-20120622 (quoting Attorney General Kamala Harris).

96 *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

icy experiments so successful that they persuade fellow enforcers to follow suit.[97] As former Maine Attorney General James Tierney and former Maine Solicitor General Peter Brann have noted, there is a "remarkable congruence that exists between states and state attorneys general when addressing similar challenges and issues."[98]

Then too, attorney general enforcement activity can spur legislative change. According to Peter Swire who served as President Bill Clinton's Chief Privacy Officer, attorneys general "are why Congress adopted the financial privacy provisions of the Gramm-Leach-Bliley Act of 1999."[99] They forced federal lawmakers' hand by suing banks for sharing consumers' financial data with third parties without notifying consumers or providing a chance to opt out.[100] Congressman Ed Markey applauded attorneys general for making clear that financial privacy required a federal response.[101]

B. Norm Creation

State enforcers have pioneered baseline privacy norms related to privacy policies, data-breach notification, consumer choice, use restrictions, youth privacy, sexual privacy, and telephone privacy. Federal agencies have built upon some of these norms in their enforcement actions.

1. Transparency of Data Practices

A central principle of data privacy law is that individuals should be notified when their data is collected, analyzed, shared, and stored.[102] Attorneys

97 Lemos, *supra* note 94, at 751. As Jessica Bulman-Pozen insightfully explores in her work, state experimentation does not always follow the same playbook, that is, with states engaging in self-contained experiments. Jessica Bulman-Pozen, *Partisan Federalism*, 127 HARV. L. REV. 1077, 1124–25 (2014). State AGs serve as laboratories of democracy in different ways, including by joining together on national issues. Experimentation can involve individual states striking out in unique ways, but it also can involve multistate investigations on national issues. *Id.* Variety is characteristic of AG privacy and data security innovation. Along those lines, multistate privacy and data security AG efforts do not always follow partisan commitments, as is true in other contexts like the environment and healthcare. They often garner the support of both Republicans and Democrats. Although the majority of the thirteen AG privacy pioneers are Democrats (such as California, New York, and Massachusetts), some are Republicans (such as Texas and Indiana).

98 James E. Tierney & Peter Brann, The Role of the State Attorney General (Fall 2015), http://web.law.columbia.edu/sites/default/files/microsites/attorneys-general/cls_syllabus_6.10.15.pdf (course syllabus).

99 Interview with Peter Swire, Professor of Law & Ethics, Ga. Inst. of Tech., in Berkeley, Cal. (June 4, 2015) [hereinafter Swire Interview].

100 *Id.*

101 Congressman Ed Markey offered a privacy amendment to the bill, pointing to Minnesota Attorney General Hatch's lawsuits against banks for sharing customers' data without permission. *See id.* The Markey amendment—which was adopted—required banks to get consumers' opt-in consent before sharing personal data with third parties. *See id.*

102 A prominent FIPPs principle is the right to have notice about how data will be collected, used, and shared. BAMBERGER & MULLIGAN, *supra* note 3, at 21–22.

general have turned the aspiration of notice into a baseline norm by requiring entities to have privacy policies.[103] The idea is that in drafting privacy policies, businesses have to think about, and commit to, certain data practices.[104] Regulators and consumer groups can inspect those policies and hold companies to their promises; consumers can find out what is happening with their personal data.[105]

After failing to persuade technology companies to adopt privacy policies voluntarily in the late 1990s,[106] state attorneys general turned to the courts.[107] In 2001, ten attorneys general sued DoubleClick for using cookies to track users' online activities without providing clear notice to consumers.[108] Although the FTC dropped its investigation because no promises had been broken, the states argued that DoubleClick's failure to make its data practices transparent constituted an unfair commercial practice.[109] DoubleClick ultimately agreed to adopt a privacy policy, allow consumers to opt out of cookies, and undergo annual privacy audits for three years.[110]

State attorneys general paired the pursuit of litigation with legislation. In 2003, California Attorney General William Lockyer proposed the California Online Privacy Protection Act ("CalOPPA"),[111] the first state law to require online services and websites to have privacy policies.[112] Most

103 The FTC has never gone so far as to say that not having a policy is a deceptive or unfair practice. *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2, at 599. Under federal law, only a few sectors of the economy must have a privacy policy, including financial institutions, healthcare providers, and websites collecting information about children under thirteen.

104 *See* Henrichsen Interview, *supra* note 8; McNabb Interview of July 20, *supra* note 59.

105 *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1266–67 (2002). Ryan Calo has done important work exploring the importance of notice and prescribing ways to ensure that it is meaningful. *See* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012).

106 Henrichsen Interview, *supra* note 8 (explaining that in the late 1990s, the attorneys general from California, New York, Washington, Texas, and Illinois convened a series of meetings with Silicon Valley leaders including Sergey Brin and Larry Page).

107 *See, e.g.*, *Granholm Targets Online Privacy*, MICH. DAILY (Feb. 12, 2001), https://www.michigandaily.com/content/granholm-targets-online-privacy (explaining that Michigan Attorney General Jennifer Granholm investigated companies whose privacy policies failed to explain that third-party advertisers collected information about consumers).

108 *See* Stephanie Miles, *DoubleClick Sets Pact with States*, WALL ST. J. (Aug. 27, 2002), http://www.wsj.com/articles/SB1030381164280449795.

109 *See* John Schwartz, *Trade Commission Drops Inquiry of DoubleClick*, N.Y. TIMES (Jan. 23, 2001), http://www.nytimes.com/2001/01/23/technology/23DOUB.html.

110 *See* Press Release, Office of the Att'y Gen. of Cal., Attorney General Lockyer Gains Enhanced Privacy Protections in Consumer Protection Cases (Aug. 28, 2002), https://oag.ca.gov/news/press-releases/attorney-general-lockyer-gains-enhanced-privacy-protections-consumer-protection.

111 *See* CAL. BUS. & PROF. CODE § 22575 (West 2016).

112 Henrichsen Interview, *supra* note 8. Attorneys general have played an important role in updating those laws. *See, e.g.*, Christine Czuprynski & Divonne Smoyer, *Illinois AG Targets ID Theft, Earlier Breach Notification*, IAPP (Apr. 28, 2015), https://privacyassociation.org/news/a/illinois-ag-targets-id-theft-earlier-breach-notification (discussing the efforts of

recently, Delaware Attorney General Matt Denn successfully spearheaded legislation requiring privacy policies.[113] Attorney General Denn modeled the law after CalOPPA.[114]

Recent state enforcement efforts have focused on the mobile ecosystem. In 2011, nearly three-quarters of mobile applications lacked privacy policies.[115] The FTC's 2012 report on mobile apps for children found that in virtually all cases, neither app stores nor app developers informed parents what data was being collected from their children.[116]

California Attorney General Kamala Harris spearheaded an initiative to change this state of affairs. She convened a working group to discuss how developers could be encouraged to post privacy policies. In February 2012, Attorney General Harris obtained, from the six companies whose platforms comprise the majority of the mobile apps market, an agreement to display apps' privacy policies so that consumers could review the policies before installing them.[117] Her office issued a guidance document urging industry to build FIPPs into mobile services, including the posting of privacy poli-

---

Illinois Attorney General Lisa Madigan to update state law to require privacy policies); Alexandra Ross, *Women in Privacy Leadership Roles: Interview with Joanne McNabb*, TRUSTe Privacy Blog (Oct. 24, 2014, 8:00 AM), http://www.truste.com/blog/2014/10/24/women-in-privacy-leadership-roles-interview-with-joanne-mcnabb/ (describing Attorney General Harris's efforts to update CalOPPA to ensure that privacy policies address how they respond to do-not-track signals).

113 *See* Press Release, Office of the Att'y Gen. of Del., Internet Privacy and Safety Agenda Becomes Law with Governor's Signature (Aug. 7, 2015), http://news.delaware.gov/2015/08/07/internet-privacy-and-safety-agenda-becomes-law-with-governors-signature/ (explaining that Delaware Attorney General Matt Denn proposed a law mirroring CalOPPA, which was adopted in 2015).

114 *See id.*; Telephone Interview with Christian Wright, Chief of Consumer Prot. Bureau, Office of the Att'y Gen. of Del. (Oct. 9, 2015) [hereinafter Wright Interview].

115 *See* FPF Staff, *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy*, Future of Privacy F. (May 12, 2011), https://fpf.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/.

116 FTC, Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing 2 (2012), https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

117 *See* Kamala D. Harris, Office of the Att'y Gen. of Cal., Joint Statement of Principles (Feb. 22, 2012), http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf. Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research in Motion were the initial signatories; Facebook signed on in June 2012.

cies.[118] The goal was to align mobile data practices with consumers' reasonable expectations.[119]

Soft-law efforts were followed with coercive ones. Attorney General Harris sent warning letters to 100 companies whose apps lacked privacy policies.[120] The letters demanded compliance with CalOPPA within thirty days or risk penalties of $2500 per download by a California consumer.[121] Attorney General Harris reinforced these warnings on social media. A tweet from Attorney General Harris's verified account said, "Fabulous app, @United Airlines, but where is your app's #privacy policy?"[122] The tweet included a link to CalOPPA.[123] Within a day's time, United Airlines had an easily accessible mobile privacy policy.[124] Attorney General Harris's office sued Delta Airlines after a warning letter failed to elicit a response.[125]

---

118 CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM 9 (2013), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf. Relatedly, attorneys general are working on putting "flesh on the bones" of privacy policies by forging norms concerning their form, timing, and content. California's policy is to have two privacy policies: a succinct privacy policy for consumers and a comprehensive one for watchdogs and regulators. *See* CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY 4 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf; *see also* Final Judgment and Permanent Injunction, People v. Comcast, No. RG15786197 (Cal. Sup. Ct. Sept. 17, 2015), (agreeing to provide simple and easy-to-read disclosures about treatment of unlisted phone numbers and to pay a $25 million penalty after allegedly posting customers' personal data even though they paid for unlisted services).

119 *See* John Kennedy & Annie Bai, *Apps Gone Wild? The FTC and California AG Seek to Rein in Mobile App Privacy Practices*, IAPP (Mar. 1, 2013), https://privacyassociation.org/news/a/2013-03-01-apps-gone-wild-the-ftc-and-california-ag-seek-to-rein-in-mobile.

120 *See* Press Release, Office of the Att'y Gen. of Cal., Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law (Oct. 30, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance.

121 *Id.*

122 Kamala Harris (@KamalaHarris), TWITTER (Oct. 12, 2012, 8:27 AM), https://twitter.com/kamalaharris/status/256778084219502592.

123 *See AG Tweets to United Airlines: Where's Your Privacy Policy?*, IAPP (Oct. 15, 2012), https://iapp.org/news/a/2012-10-15-ag-tweets-to-united-airlines-wheres-your-privacy-policy.

124 Interview with Travis LeBlanc, Chief of the Bureau of Enf't, FCC, in Wash., D.C. (July 10, 2015) [hereinafter LeBlanc Interview].

125 Brandon Bailey, *California Attorney General Sues Delta Air Lines over Smartphone App Privacy Policy*, SAN JOSE MERCURY NEWS (Dec. 6, 2012), http://www.mercurynews.com/business/ci_22141459/california-sues-delta-airlines-over-smartphone-app-privacy. The complaint was dismissed on the grounds that federal law preempts state actions concerning airlines and Attorney General Harris's office appealed the decision. *See* Bernard Nash et al., *State AGs in the News*, STATE AG MONITOR (May 24, 2013), https://web.archive.org/web/20130708101148/http://www.stateagmonitor.com/2013/05/24/state-ags-in-the-news-84. The dismissal was upheld on appeal. *See* Bob Egelko, *Court Says Ca. Privacy Law Doesn't Apply to Airlines' Mobile Apps*, SFGATE (May 25, 2016), http://www.sfgate.com/news/article/Court-says-Ca-privacy-law-doesn-t-apply-to-7946012.php.

Attorney General Harris's efforts transformed the transparency of the mobile app marketplace. According to John Simpson of Consumer Watchdog's Privacy Project, Attorney General Harris "tam[ed] the Wild West in the mobile world."[126] "From September 2011 to June 2012, the number of free Apple Store apps with a privacy policy doubled, from 40 percent to 84 percent."[127]

The FTC has attributed the increase in mobile privacy policies to Attorney General Harris's agreement with platform providers.[128] The change, however, was due to far more than the platforms' design change. Attorney General Harris's guidance documents and workshops, her issuance of warning letters, and ultimately her pursuit of litigation helped reinforce the basic norm that mobile apps must have privacy policies.

In establishing a baseline requirement for privacy policies, state attorneys general have paved a path for federal agencies to build upon. Although the FTC has never taken the position that section 5 requires companies to have privacy policies,[129] it reinforced the norm set by state attorneys general by suing companies for deceptively breaking promises made to consumers in their privacy policies.[130]

2. Data-Breach Notification

In the 1990s, companies had no legal obligation to notify consumers about data breaches. As a result, they had little incentive to improve data security because data breaches cost them nothing.[131] Consumers whose sensitive personal data had been leaked were in the dark: they had no warning that they should check their credit reports for signs of theft.

State attorneys general supported state data-breach notification proposals,[132] which were soon adopted across the nation.[133] Those laws have been

126 Grant Gross, *Mobile Apps Should Limit Data Collection, State AG Says*, COMPUTERWORLD (Jan. 10, 2013), http://www.computerworld.com/article/2493990/mobile-wireless/mobile-apps-should-limit-data-collection—state-ag-says.html (quoting e-mail from John Simpson, Consumer Watchdog Privacy Project).

127 Kennedy & Bai, *supra* note 119.

128 *See* Kristin Cohen & Christina Yeung, *Kids' Apps Disclosures Revisited*, FTC BLOG (Sept. 3, 2015, 11:04 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/09/kids-apps-disclosures-revisited (endorsing Attorney General Harris's mobile privacy proposals).

129 *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2, at 599.

130 *See id.* at 628–30 (discussing FTC enforcement actions based on companies' broken promises).

131 Under federal law, breach notification is only required by certain sectors of the economy, such as covered healthcare providers and financial institutions. *See id.* at 587.

132 *See* Henrichsen Interview, *supra* note 8 (explaining that Attorney General William Lockyer supported California's passage of a data-breach notification law). California was the first state to pass a data-breach notification law, thanks to the hard work of then-Assemblyman Joe Simitian. *See* E-mail from Deirdre Mulligan, Assoc. Professor, Berkeley Sch. of Info., to Danielle Citron, Professor of Law, Univ. of Md. Francis King Carey Sch. of Law (Aug. 12, 2016) (on file with author).

kept up to date thanks to the efforts of attorneys general.[134] Companies suffering breaches have to provide notice to consumers and to attorney general offices.[135] Attorneys general have defended state breach notification laws from federal efforts to preempt them.[136]

State attorneys general have enforced data-breach notification laws, setting norms in the process. Enforcement actions have fleshed out what breach notification statutes mean when they require companies to notify consumers "in the most expedient time possible and without unreasonable delay."[137]

An emerging rule of thumb is that notice should proceed on a rolling basis.[138] California, for instance, sued Kaiser Foundation Health for allegedly waiting four months to notify consumers about a breach, even though

133 Forty-six states, the District of Columbia, and several territories now have data-breach notification laws. *See* Ronald W. Breaux et al., *California AG Cracks Down on Timing of Data Breach Disclosures*, HAYNES BOONE (Feb. 5, 2014), http://www.haynesboone.com/news-and-events/news/alerts/2014/02/05/california-ag-cracks-down-on-timing-of-data-breach-disclosures.

134 *See, e.g.*, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 3 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf (explaining that the California legislature adopted Attorney General Harris's recommendation to update data security law); Erik C. Jones, *Step Aside, States?*, SLATE (Jan. 22, 2015), http://www.slate.com/articles/technology/future_tense/2015/01/obama_data_breach_legislation_federal_laws_shouldn_t_pre_empt_state_laws.html (discussing Illinois Attorney General Lisa Madigan's lobbying to update breach notification statute).

135 *See, e.g.*, OFFICE OF THE ATT'Y GEN. OF CONN., ANNUAL REPORT: FISCAL YEAR 2011–2012, at 5 (2012), http://www.ct.gov/ag/lib/ag/about_us/annualreport2011-12.pdf (discussing Attorney General Jepsen's proposal to amend notification law to secure notice for his office); Selis Interview, *supra* note 38 (explaining that the Washington attorney general lobbied to update breach notification law to ensure that companies gave notice to the office).

136 *See* Letter from the Nat'l Ass'n of Att'ys Gen. to Cong. Leaders (July 7, 2015), http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Data%20Breach%20Notification%20Letter.pdf (signed by forty-seven attorneys general, arguing against preemption of state breach notification laws and emphasizing the important role that attorneys general play in investigating and enforcing data security lapses); *see also* Divonne Smoyer et al., *Beware the Growth of State AG Enforcement Efforts*, CORP. COUNS. (May 22, 2015), http://www.corpcounsel.com/id=1202727264255/Beware-the-Growth-of-State-AG-Enforcement-Efforts.

137 CAL. OFFICE OF PRIVACY PROT., RECOMMENDED PRACTICES ON NOTICE OF SEC. BREACH INVOLVING PERS. INFO. 7 (2007), http://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/PrivacyProtection.pdf.

138 *See* People v. Kaiser Found. Health Plan, Inc., No. RG14711370 (Cal. Sup. Ct. Feb. 10, 2014) (order granting permanent injunction); *see also* Assurance of Voluntary Compliance, *In re* Affinity Health Plan, Inc. (Office of the Att'y Gen. of N.Y., Bureau of Consumer Frauds & Prot. Mar. 18, 2008) [hereinafter Affinity Health Plan AVC] (on file with author) (agreeing, with the state of New York, to provide notice in most expedient time possible and to pay $50,000 where company allegedly notified consumers eleven months after discovering breach).

the company knew the identity of affected consumers two months before.[139] In 2014, Kaiser agreed to provide notice of future breaches as soon as a portion of affected consumers could be identified rather than waiting until the completion of an internal investigation.[140]

Privacy practitioners predict that the *Kaiser* agreement will influence how other state enforcers interpret the timing requirements of their breach notification laws.[141] Time will tell if California's interpretation of its data-breach notification law is adopted elsewhere. California's approach may have spillover effects as companies adopt it to avoid the costs of piecemeal compliance.

In sum, state enforcers—through legislation and litigation—have changed how companies respond to inadequate data security. Notification of breaches has allowed state and federal enforcers to investigate whether inadequate security was responsible for countless data leaks.[142]

3. Respecting Consumer Choice

Do-not-track settings on browsers prevent advertisers from tracking consumers' online activities. What happens if online providers ignore consumers' privacy settings? What if they have promised to respect consumers' settings but fail to keep those promises?

Attorneys general have set precedent that bypassing a consumer's privacy settings is, in itself, an unfair practice. This precedent emerged from an investigation of Google and the advertising firm PointRoll. Google's privacy policy promised that the privacy settings of users' browsers would be honored.[143] Nevertheless, Google and PointRoll placed third-party cookies on Safari users' browsers whose default settings signaled that they should not be tracked.[144] Google deployed a program that invisibly simulated the user changing the default setting by clicking on the "track me" instruction.[145]

---

139 *See* Complaint at 2, People v. Kaiser Found. Health Plan, Inc., No. RG14711370 (Cal. Sup. Ct. Jan. 24, 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/kaiser_complaint.pdf?.

140 *See* People v. Kaiser Found. Health Plan, Inc., No. RG14711370 (Cal. Sup. Ct. Feb. 10, 2014) (order granting permanent injunction).

141 *See, e.g.*, Matthew Staples, *Kaiser Foundation Health Plan Settles California Attorney General Charges over Delayed Data Breach Notification*, EYE ON PRIVACY (Mar. 2014), https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Mar2014/index.html.

142 See *infra* note 235 (discussing data security actions involving failure to provide notice in a timely fashion).

143 *See* Warwick Ashford, *Google Reaches $17M Multi-State Settlement over Safari Snooping*, COMPUTER WEEKLY (Nov. 19, 2013), http://www.computerweekly.com/news/2240209285/Google-reaches-17m-multi-state-settlement-over-Safari-snooping.

144 *See* Wendy Davis, *PulsePoint To Pay $1 Million for Safari Hack*, MEDIA POST (July 26, 2013), http://www.mediapost.com/publications/article/205448/pulsepoint-to-pay-1-million-for-safari-hack.html?edition=.

145 Julia Angwin & Jennifer Valentino-DeVries, *Google's iPhone Tracking*, WALL ST. J. (Feb. 17, 2012), http://www.wsj.com/articles/SB10001424052970204880404577225380456599176. As Chris Hoofnagle explained, "It was as if a Google engineer grabbed the

The incident drew the attention of federal and state authorities. The FTC's case singled out Google, focusing on the company's broken promise to consumers.[146] In a consent decree with the FTC, Google agreed to erase the cookies it had placed on users' computers.[147] The consent decree, however, placed no prohibition on Google's future behavior.[148] In short, the FTC pursued thin protections for consumers based on the agency's long history of using section 5 to ensure that companies live up to their promises in privacy policies.[149]

The FTC invited a group of thirty-nine attorneys general investigating Google to join the consent decree.[150] The multistate group, however, declined the FTC's invitation because it was far more interested in injunctive relief.[151] For the attorneys general, the enforcement action was not about broken promises, though promises had been broken.[152] More important to them was the surreptitious manipulation of consumers' browsers to turn on tracking in contravention of their settings.[153] As the multistate investigation of Google continued, a smaller group of attorneys general pursued an investigation of PointRoll for placing cookies on consumers' Safari browsers despite their settings indicating that cookies should be blocked.[154]

Although the multistate investigations of Google and PointRoll were resolved separately, the substance of the resulting AVCs was the same. Google and PointRoll were prohibited from bypassing consumers' privacy settings unless they received consumers' affirmative, or opt-in, consent.[155]

The message from the states was that evading privacy controls—including default privacy controls—is unfair and perhaps even deceptive, whether

---

user's mouse and clicked on a 'track me' button while the user was not watching." HOOFNAGLE, *supra* note 2, at 350.

146 *See* HOOFNAGLE, *supra* note 2, at 338.

147 Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

148 *See id.*

149 *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2, at 628–30 (discussing FTC's pursuit of thin norms based on enforcement of promises).

150 *See* Ruckman Interview, *supra* note 41. The ten-state executive committee included Connecticut, Florida, Illinois, Maryland, Ohio, New Jersey, New York, Texas, Vermont, and Washington. *Id.*

151 *See id.*

152 *See id.*

153 *See id.*

154 Connecticut, Florida, Illinois, Maryland, New Jersey, and New York participated in the PointRoll investigation. *See, e.g.*, Assurance of Voluntary Compliance, *In re* PointRoll, Inc. (Office of the Att'y Gen. of Conn., Comm'r of Consumer Prot. Dec. 10, 2014) [hereinafter PointRoll AVC] (on file with author).

155 *See* Assurance of Voluntary Compliance, *In re* Google (Office of the Att'y Gen. of Conn., Comm'r of Consumer Prot. Nov. 13, 2013) (on file with author) (an agreement between thirty-nine attorneys general and Google).

or not any promises are broken.[156] Acting New Jersey Attorney General John Hoffman explained: "People have every right to surf the Web without fear that businesses are employing technical tricks to bypass their privacy settings."[157]

The broader impact of the informal agreements with Google and PointRoll is unclear. An open question is whether other companies will internalize the norm to honor consumers' privacy settings—whether or not promises were made—because circumventing consumers' privacy choices would be unfair.

If attorneys general want to ensure that companies respect consumers' privacy settings, they should reinforce that norm with all tools available to them. Attorneys general have not yet proposed or advocated for legislation requiring companies to respect consumers' privacy settings.[158] They would do well to reinforce the standard set in the Google and PointRoll matters with supportive legislation, education efforts, and additional enforcement activity.

4. Use Restrictions

Consumer privacy law is often silent on the question of how companies may use personal data that has been collected legally.[159] This is because norms surrounding use restrictions are hotly contested.[160] Attorneys general

156 *See* Justin Brookman, *State Attorneys General: Evading Privacy Settings Is Illegal*, CDT BLOG (Nov. 20, 2013), https://cdt.org/blog/state-attorneys-general-evading-privacy-settings-is-illegal/. As Illinois Assistant Attorney General Matt Van Hise explained, the attorneys general based their investigation of PointRoll on the premise that it was fundamentally unfair to nullify a consumer's choice not to be tracked. Hagan & Van Hise Interview, *supra* note 5.

157 Press Release, Office of the Att'y Gen. of N.J., N.J. Leads Multi-State Settlement Resolving Allegations That Digital Ad Co. Breached Internet Privacy Settings (Dec. 11, 2014), http://nj.gov/oag/newsreleases14/pr20141211c.html. An important question, taken up in Part III, is whether AVCs, as currently conceived, are the most effective vehicle to shape norms. *See infra* Part III.

158 Attorney General Harris supported an amendment to CalOPPA, which requires companies to notify consumers about their response to do-not-track settings. *See* Lei Shen, *Unpacking the California AG's Guide on CalOPPA*, IAPP (May 27, 2014), https://iapp.org/news/a/unpacking-the-california-ags-guide-on-caloppa/. The amendment, however, said nothing about companies' substantive obligations to honor consumers' choices. Similarly, Illinois Attorney General Lisa Madigan lobbied to amend state privacy law to require privacy policies to notify consumers about entities' response to do-not-track settings. *See* Czuprynski & Smoyer, *supra* note 112.

159 Alex Schneider, *How Could They Know That? Behind the Data That Facilitates Scams Against Vulnerable Americans*, 19 VA. J.L. & TECH. 716, 750–51 (2015); *see* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 16–17 (2014). Discrimination law, of course, speaks to illegal uses of personal data. *Id.* For instance, the federal Equal Credit Opportunity Act forbids discrimination in lending. *Id.*

160 Schneider, *supra* note 159, at 750–51.

have entered the fray by limiting the use of certain personal data to deny financial services to consumers.

New York Attorney General Eric Schneiderman spearheaded an investigation into the major banks' use of a company's database containing information about individuals with less than perfect banking records.[161] The investigation revealed that when individuals were included in the database, they were prevented from opening bank accounts, even if they had immediately paid back money they owed or bounced a single check years before.[162] In that regard, the database was used as a blacklist.[163] Once denied banking services, lower-income applicants often turned to high-cost alternatives like check-cashing outlets.[164]

Three major banks, Santander, Capital One, and Citibank, agreed to refrain from using the database (and others like it) to deny banking services so that no one is rejected for isolated or minor mistakes.[165] The agreement applied to the banks' offices nationwide. Practitioners have warned financial service providers to consider the possibility that they could face an enforcement action for using the company's database.[166] The broader norm-setting work of the informal agreement remains to be seen.

More generally, use restrictions are on the enforcement agenda of state attorneys general.[167] Under consideration is whether there should be restrictions on uses of health data held by sites and services that are not covered by

161 *See* Mitch Lipka, *Consumer Groups Cheer Move to Rein in Banking "Blacklist"*, CBS NEWS: MONEYWATCH (Jan. 29, 2015), http://www.cbsnews.com/news/consumer-groups-cheer-move-to-rein-in-banking-blacklist/.

162 *Santander Agrees to Change ChexSystems Policies, Which Kept Many from Obtaining Bank Accounts*, FOX BUS. NEWS (Feb. 20, 2015), http://www.foxbusiness.com/markets/2015/02/20/santander-agrees-to-change-chexsystems-policies-which-kept-many-from-obtaining/.

163 Danielle Citron, *The Blacklist's Power*, FORBES (June 17, 2014), http://www.forbes.com/sites/daniellecitron/2014/06/17/the-blacklists-power/#2715e4857a0b138390be5c9c.

164 Press Release, Office of the Att'y Gen. of N.Y., A.G. Schneiderman Announces Commitment by Citibank to Eliminate Barriers That Unfairly Keep Low-Income Americans from Opening Checking and Savings Accounts (Jan. 28, 2015), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-commitment-citibank-eliminate-barriers-unfairly-keep-low.

165 *Santander Agrees to Change ChexSystems Policies, Which Kept Many from Obtaining Bank Accounts*, *supra* note 162. Citibank agreed that applications only could be denied if individuals have two or more reported incidents of account abuse, the total loss from those incidents exceeds $500, and the losses remain unpaid. CHI CHI WU & KATIE PLAT, NAT'L CONSUMER LAW CTR. & CITIES FOR FIN. EMPOWERMENT FUND, ACCOUNT SCREENING CONSUMER REPORTING AGENCIES: A BANKING ACCESS PERSPECTIVE 18 (2015), https://www.nclc.org/images/pdf/pr-reports/Account-Screening-CRA-Agencies-BankingAccess101915.pdf.

166 *New York AG, Capital One Agree on Credit Screening Changes*, MANATT, PHELPS & PHILLIPS, LLP (July 18, 2014), https://www.manatt.com/Insights/Newsletters/Financial-Services-Law/Holder-Vows-To-Continue-Operation-Choke-Point;-Hou#Article5.

167 Jepsen Interview, *supra* note 49.

federal health privacy law.[168] Because norms surrounding use restrictions are not well settled, attorneys general are proceeding with caution.

5. Sexual Privacy

Until 2014, if someone's nude image appeared online without permission, little could be done.[169] Websites routinely ignored requests to take down nude images because they enjoyed immunity from liability for user-generated content under federal law; law enforcement turned away victims, urging them to turn off their computers rather than make a big deal about it.[170] All the while, victims had difficulty finding and keeping jobs because their nude images and contact information appeared prominently in online searches of their names.[171] They were terrified that strangers would confront them in person.[172] They moved; some changed their names; all were distraught. The fallout was devastating.[173]

California Attorney General Kamala Harris has fought for the adoption of baseline practices that combat invasions of sexual privacy.[174] Attorney General Harris sponsored bills giving law enforcement the tools to investigate and prosecute invasions of sexual privacy.[175] She convened meetings with major Internet companies, including Microsoft, Facebook, Twitter, Yahoo, and Google, urging them to consider adopting policies permitting the removal of nude images posted without consent.[176] Attorney General Harris

168 *See, e.g.*, Letter from George C. Jepsen, Att'y Gen., State of Conn., to Tim Cook, CEO, Apple, Inc. (Sept. 12, 2014), http://www.ct.gov/ag/lib/ag/press_releases/2014/20140912_applewatchletter.pdf (requesting a meeting to discuss privacy risks of Apple Watch). Illinois Attorney General Lisa Madigan has raised concerns about health websites like WebMD and Weight Watchers. Press Release, Office of the Att'y Gen. of Ill., Madigan: Popular Health Websites Must Ensure Privacy of Users' Health Information (July 12, 2013), http://www.illinoisattorneygeneral.gov/pressroom/2013_07/20130712.html. Paul Ohm has done important work calling for privacy regulation that provides greater protection for sensitive data. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015).

169 Danielle Keats Citron, *Revenge Porn Should Be a Crime*, CNN (Aug. 29, 2013), http://www.cnn.com/2013/08/29/opinion/citron-revenge-porn/.

170 DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 20 (2014).

171 *Id.* at 181.

172 *Id.* at 202.

173 Danielle Citron, *Attorney General Kamala Harris to Help Law Enforcement in Investigations of Criminal Invasions of Sexual Privacy*, LAW ENF'T CYBER CTR. (Oct. 20, 2015), http://www.iacpcybercenter.org/the-groundbreaking-work-of-attorney-general-kamala-harris-to-help-law-enforcement-in-investigations-of-criminal-invasions-of-sexual-privacy/.

174 *Id.* I have served as an adviser to Attorney General Harris and her executive team on revenge porn, harassment, and privacy since the fall of 2014.

175 *Cyber Exploitation*, OFFICE OF THE ATT'Y GEN. OF CAL., https://oag.ca.gov/cyberexploitation (last visited Sept. 27 2016).

176 Press Release, Office of the Att'y Gen. of Cal., Attorney General Kamala D. Harris, Tech Leaders, and Advocates Launch Offensive in Fight Against Cyber Exploitation (Oct. 14, 2015), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-tech-leaders-and-advocates-launch-offensive. In February 2015, Attorney General Harris convened a Task Force meeting with technology companies, law enforcement liaisons, advo-

organized a Cyber Exploitation Task Force made up of victim advocates, fifty major technology companies, law enforcement representatives, and experts.[177] The Task Force worked on strategies for educating law enforcement and best practices for online platforms.[178]

Attorney General Harris's efforts influenced the practices of online intermediaries, including search engines and social networks. After sustained public conversation about nonconsensual pornography and participation in the Task Force, Google and Microsoft agreed to remove nude images from searches of victims' names upon their request.[179] Twitter banned the nonconsensual posting of someone's nude images.[180] Facebook clarified its nudity ban with a detailed explanation of the difference between nudity addressing social issues like photos of mastectomies, which are permitted, and images of buttocks and genitals posted without the subject's permission, which are banned.[181] Attorney General Harris created an online hub providing resources for law enforcement, victims, and companies interested in addressing invasions of sexual privacy, harassment, and stalking.[182]

Important precedent has also been set concerning the operation of sites that extort money from victims of nonconsensual pornography.[183] In her

---

cacy groups, and experts in her San Francisco office. As an adviser to Attorney General Harris, I spoke at the meeting, describing cyber exploitation, its various forms and impact, and ways to combat it.

177 Joe Mullin, *California AG Goes All-Out to Fight "Revenge Porn"*, ARS TECHNICA (Oct. 14, 2015), http://arstechnica.com/tech-policy/2015/10/california-ag-goes-all-out-to-fight-revenge-porn/. In October 2015, Attorney General Harris held a press conference in Los Angeles announcing the rollout of the cyber exploitation hub, at which I spoke. *Cal AG Harris Launches Cyber Exploitation Initiative*, ILC CYBER REPORT (Oct. 14, 2015), https://ilccyberreport.wordpress.com/2015/10/14/cal-ag-harris-launches-cyber-exploitation-initiative/.

178 Press Release, Office of the Att'y Gen. of Cal., Technology Industry Leaders and Lawmakers Express Support for Attorney General Kamala D. Harris's New Initiative to Combat Crime of Cyber Exploitation (Oct. 14, 2015), https://oag.ca.gov/news/press-releases/technology-industry-leaders-and-lawmakers-express-support-attorney-general.

179 Jessica Guynn, *Google to Remove 'Revenge Porn' from Search Results*, USA TODAY (June 19, 2015), http://www.usatoday.com/story/tech/2015/06/19/google-revenge-porn-search-results/28983363/; Patrick Howell O'Neill, *Microsoft Joins Google in Censoring Revenge Porn*, DAILY DOT (July 22, 2015), http://www.dailydot.com/politics/microsoft-ban-revenge-porn-bing-xbox-live-onedrive/.

180 Ema O'Connor, *California Launches New Way for "Revenge Porn" Victims to Strike Back*, BUZZFEED NEWS (Oct. 15, 2015), http://www.buzzfeed.com/emaoconnor/california-helps-revenge-porn-victims-strike-back#.uqB6rAzoV; Hayley Tsukayama, *Twitter Updates Its Rules to Specifically Ban 'Revenge Porn'*, WASH. POST (Mar. 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/11/twitter-updates-its-rules-to-specifically-ban-revenge-porn/.

181 Evan Selinger, *How to Defeat Internet Bullies*, CHRISTIAN SCI. MONITOR (Mar. 27, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0327/How-to-defeat-Internet-bullies.

182 *Cyber Exploitation*, *supra* note 175.

183 *See* Press Release, Office of the Att'y Gen. of Cal., Attorney General Kamala D. Harris Announces Arrest of Revenge Porn Website Operator (Dec. 10, 2013), http://oag.ca

capacity as California's "top cop,"[184] Attorney General Harris successfully prosecuted operators of sites that encouraged users to post nude photos and charged for their removal.[185] For instance, the operator of UGotPosted, Kevin Bollaert, faced charges of extortion, conspiracy, and identity theft for allegedly urging users to post their ex-lovers' nude photos and then charging individuals up to $350 for the removal of a photo.[186] Bollaert's conviction signaled that extorting money from individuals whose confidential nude images were posted without permission is an illegal enterprise.[187]

The FTC followed Attorney General Harris's lead by bringing an enforcement action against revenge porn site operator Craig Brittain.[188] The FTC's charges focused on the site's solicitation of individuals' nude photos and contact information and the disclosure of that information to the public.[189] The FTC argued that it was unfair for Brittain to exploit nude images shared in confidence for commercial gain.[190] In the consent decree, Brittain pledged not to disclose anyone's nude images online without first getting express written consent.[191] Here again, it was state attorney general enforcement setting precedent protecting sexual privacy, which the FTC emulated under its section 5 authority.

6. Youth Privacy

Teenagers—youth between thirteen and eighteen years old—are vulnerable to exploitation when their personal data is collected, analyzed, and shared. Nonetheless, federal privacy law provides little protection to children

.gov/news/press-releases/attorney-general-kamala-d-harris-announces-arrest-revenge-porn-website-operator. Christopher Bollaert was tried before a jury in late 2014 and convicted in February 2015. Andie Adams & Candice Nguyen, *San Diego Man Convicted of Extortion, ID Theft in 'Revenge Porn' Case*, NBC SAN DIEGO (Feb. 2, 2015), http://www.nbcsandiego.com/news/local/Kevin-Bollaert-Convicted-in-Revenge-Porn-Case-Website-290593621.html.

184 Not all attorneys general have authority over criminal investigations and prosecutions. *See* STATE ATTORNEYS GENERAL, *supra* note 4, at 307–10. The California Attorney General's Office has that power. *See id.* at 312.

185 Press Release, Office of the Att'y Gen. of Cal., Attorney General Kamala D. Harris Announces Three-Year Sentence for Cyber Exploitation Website Operator (June 8, 2015), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-three-year-sentence-cyber.

186 Danielle Citron, *Can Revenge Porn Operators Go to Prison?*, FORBES (Jan. 17, 2015), http://www.forbes.com/sites/daniellecitron/2015/01/17/can-revenge-porn-operators-go-to-jail/#2953b3ca53ca; *see also* Adams & Nguyen, *supra* note 183.

187 Danielle Citron & Woodrow Hartzog, *The Decision That Could Finally Kill the Revenge-Porn Business*, ATLANTIC (Feb. 3, 2015), http://www.theatlantic.com/technology/archive/2015/02/the-decision-that-could-finally-kill-the-revenge-porn-business/385113/.

188 Press Release, FTC, Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos (Jan. 29, 2015) https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges.

189 *Id.*

190 *Id.*

191 *Id.*

who are thirteen and older.[192] Attorneys general have endeavored to protect the privacy of teenagers. Recent attorney general efforts have focused on the adoption of laws limiting the commercial use of student data collected by education technology companies.[193]

Teenagers' social media interactions have attracted the attention of attorneys general, particularly as to child predators and cyber bullying. In 2006, forty-nine attorneys general formed a task force to investigate predators' use of social networks to contact teenagers.[194] At the time, MySpace was a main site of teen interaction. MySpace agreed to improve its privacy features.[195] Pursuant to the AVC, the default setting for profiles of users under eighteen would be "private," so only established friends could visit their pages. Friend requests from users over eighteen could be sent to users under sixteen only if requesters knew the users' last names or email addresses. Even if users under sixteen overrode the privacy settings, their profiles would still only be viewable by other uses under eighteen.[196] The company agreed to undergo biannual audits of their consumer complaint

192 The federal Children's Online Privacy Protection Act places certain conditions on the collection of data from children who are twelve and under when they are online. Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247, 13,248 (Mar. 15, 2006) (codified at 16 C.F.R. § 312). During the FTC's rulemaking process to update the law, child privacy advocates urged the FTC to expand COPPA's definition of "child" to include adolescents. THE PUB. HEALTH ADVOCACY INST., PRIVACY: STATE LAW APPROACHES TO ADDRESS DIGITAL FOOD MARKETING TO YOUTH 40 (2013), http://www.phaionline.org/wp-content/uploads/2013/12/DigitalMktgFullReportPDF.pdf. The FTC declined to do so. *Id.*

193 The Delaware Attorney General's Office is currently working on a rulemaking related to its new student privacy law. Wright Interview, *supra* note 114. *See* KAMALA D. HARRIS, CAL. DEPT. OF JUSTICE, READY FOR SCHOOL: RECOMMENDATIONS FOR THE ED TECH INDUSTRY TO PROTECT THE PRIVACY OF STUDENT DATA (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ready-for-school-1116.pdf? (laying out best practices for education technology companies collecting, using, and storing sensitive student data, including medical histories, social and emotional assessments, child welfare or juvenile justice system involvement, progress reports, location data, and test results, in light of the adoption of new California student data privacy laws). In 2005, forty-two attorneys general alleged that it was a deceptive trade practice to ask high school students to fill out surveys implying they were meant for colleges and universities when in fact they were given to advertisers. Press Release, Office of the Att'y Gen. of N.Y., States Settle with Student Data Collection Company (Jan. 13, 2005), http://www.ag.ny.gov/press-release/states-settle-student-data-collection-company. The company settled with the states, agreeing to give parents and students the opportunity to opt out of participation in the survey. *Id.*

194 Adam Thierer, *The MySpace-AG Agreement: A Model Code of Conduct for Social Networking?*, (Progress & Freedom Found., Paper No. 15.1, 2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1092206; *see also* Divonne Smoyer, *State Attorneys General as U.S. Privacy Regulators: Q&A with Maryland AG Doug Gansler*, IAPP (Jan. 28, 2014), https://iapp.org/news/a/state-attorneys-general-as-u-s-privacy-regulators-q-a-with-maryland-attorn/.

195 Thierer, *supra* note 194.

196 MySpace & Attorneys General, Joint Statement on Key Principles of Social Networking Sites Safety, NAT'L ASS'N ATT'YS GEN. (Jan. 14, 2008), http://www.naag.org/assets/files/pdf/20080115.Joint%20Statement%20on%20Key_Principles_of_Social_Networking_Sites_Safety.pdf.

handling and response procedures.[197] More recently, in agreements with Maryland and New York, the anonymous social network Ask.fm has pledged to adopt a comprehensive risk management plan and program, including the hiring of a trust and safety officer.[198]

7. Telephone Privacy

Attorneys general were central to the establishment of state Do Not Call registries. Even before a federal Do Not Call list was established,[199] states created their own registries.[200] After the adoption of a federal Do Not Call registry, states supplemented federal law with stronger protections for consumers. State Do Not Call laws have been extended to cellphones.[201]

A number of states have aggressively enforced federal and state Do Not Call laws. Since 2002, the Indiana Attorney General's Office has obtained 314 settlements with, or judgments against, telemarketers, resulting in awards totaling more than $22 million, which has reduced the number of telemarketing calls made to state citizens.[202] Indiana Attorney General Greg

197 *Id.*

198 *See* Press Release, Office of the Att'y Gen. of Md., AG Gansler Secures Agreement to Protect Children on Ask.fm (Aug. 12, 2014), http://www.marylandattorneygeneral.gov/Pages/NewsReleases/2014/081414.aspx; *see also* Michael Bodley, *Ask.fm, Attorney General Reach Agreement to Keep Children Safer Online*, BALT. SUN (Aug. 14, 2014), http://articles.baltimoresun.com/2014-08-14/business/bs-bz-ask-fm-20140814_1_ask-fm-gansler-maryland-attorney-general.

199 The Telephone Consumer Protection Act of 1991 (TCPA) placed restrictions telemarketing and robocallers. 47 U.S.C. § 227 (2012). Under the TCPA, the Federal Communications Commission (FCC) was directed to create a national Do Not Call database for persons wishing to opt out of telemarketing calls. *Id.* The FCC, however, determined, incorrectly, that the TCPA does not apply to calls from government contractors. *Telemarketing and the Telephone Consumer Protection Act (TCPA)*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/telemarketing/ (last visited Nov. 29, 2016). In 2003, the federal Do-Not-Call Implementation Act (DNCA) established the FTC's Do Not Call Registry to facilitate compliance with the TCPA. 15 U.S.C. § 6151 (2012). That statute did not preempt state Do Not Call laws with stronger restrictions. 47 U.S.C. § 227.

200 Indiana Attorney General Greg Zoeller explained that Missouri was the first state to pass a Do Not Call law. Telephone Interview with Ind. Att'y Gen. Greg Zoeller (July 8, 2016) [hereinafter Zoeller Interview]. While working on a Do Not Call bill as the Deputy Attorney General to then-Indiana Attorney General Nixon, Greg Zoeller talked to the Missouri Attorney General's Office about the strengths and weaknesses of its bill. *Id.* Crucial to Zoeller was that there be no exemptions included in Indiana's Do Not Call bill, such as the preexisting relationship exemption in the Missouri law that permitted a significant number of unwanted marketing calls to consumers. *Id.* Indiana's legislature passed the strongest state Do Not Call law, thanks to lobbying by Attorneys General Nixon and Zoeller. *Id.*

201 *See, e.g.*, Andrew B. Lustigman, *Indiana Do Not Call List Extends to Include Mobile Numbers*, ADVERT. LAW BLOG (May 27, 2011), http://www.olshanlaw.com/blogs-Advertising-Law-Blog,Indiana-Do-Not-Call-Mobile.

202 ECTV Indiana, *AG Zoeller Files Lawsuit Against California Telemarketer Accused of Robocalling Violating Do Not Call List*, FACEBOOK (Oct. 22, 2014), https://www.facebook.com/ECTVNEWS/posts/374351109381928.

Zoeller and Missouri Attorney General Chris Koster have also led an annual Do Not Call training for states and federal agencies.

Recent attorney general efforts have focused on reversing a change to the federal Telephone Consumer Privacy Act (TCPA), which exempts federal debt collectors from Do Not Call obligations.[203] In May 2016, Attorney General Zoeller testified that the recent TCPA amendments undermined his state's tough Do Not Call law by legitimizing robocalls from debt collectors.[204] Along with twenty-four state attorneys general, Attorney General Zoeller called upon Congress to defend the telephone privacy rights of citizens by passing the HANGUP Act, which would reinstate the application of Do Not Call laws to debt collectors.[205] In 2015, Attorney General Zoeller succeeded in convincing the Federal Communications Commission (FCC) to permit phone companies to implement call blocking technology; his office, on behalf of forty-five other attorneys general, urged the major phone companies to adopt such call-blocking technology.

Through legislation, education, and enforcement, state attorneys general have set norms protecting consumers' telephone privacy. Over the years, their policymaking has made a significant difference in combating intrusive and unwanted phone calls.

C. Norm Reinforcement

Along with norm-setting work, state attorneys general have entrenched and, at times, augmented established data security and privacy norms set at the federal level. This Section explores how.

1. Federal Privacy Statutes

Federal privacy regulations related to healthcare, children's online activities, and credit reporting agencies are enforceable by state and federal authorities.[206] Attorneys general have taken up the mantle of enforcement with vigor. Precedent set by federal agencies has guided their investigations of alleged violations of the Health Insurance Portability and Accountability

203 The TCPA amendment allows debt collection robocalls to people's cell phones if the debt is owned or guaranteed by the United States. 47 U.S.C. § 227. Crucially, it preempts stronger state laws prohibiting unsolicited cellphone calls by federal debt collectors.

204 *Testimony of Indiana Attorney General Greg Zoeller: TCPA and HANGUP Act, Before the S. Comm. on Com., Sci., and Transp.*, 114th Cong. 1 (2016) (statement of Greg Zoeller, Ind. Att'y Gen.), https://www.commerce.senate.gov/public/_cache/files/a8cddd55-39e8-4085-9043-3dd67ffa7b54/88D45DDDB5D28C4D241FC363E11B96B7.zoeller-testimony.pdf.

205 *Id.*

206 NAAG played an important role in lobbying for concurrent enforcement power for federal privacy statutes. Provost, *supra* note 56, at 39.

Act (HIPAA),[207] the Fair Credit Reporting Act (FCRA),[208] and the Children's Online Privacy Protection Act (COPPA).[209]

Connecticut was the first state to sue a healthcare provider for failing to secure health data as required by HIPAA.[210] When the Department of Health and Human Service's Office of Civil Rights does HIPAA training for staff at offices of attorneys general, it uses Connecticut's litigation of the case as the exemplar of how to bring a HIPAA action.[211] New York, Maryland, Massachusetts, Texas and Vermont have brought HIPAA cases as well.[212]

Attorneys general have fought for credit-reporting agencies to comply with the basic requirements of FCRA. The three major credit-reporting agencies recently agreed to improve the accuracy of credit reports, to enhance the fairness of procedures for resolving consumer disputes about errors, and to protect consumers from unfair harm to their credit histories in connection with medical debt.[213] New York initiated its investigation of the credit-reporting agencies after the FTC released a study finding that twenty-

207 In 2009, the Health Information Technology for Economic and Clinical Health Act (HI-TECH Act) authorized state attorneys general to enforce HIPAA. Health Information Technology for Economic and Clinical Health Act, Pub. Law No. 111-5, §§ 13001–424, 123 Stat. 226 (2009) (codified as amended at 42 U.S.C. §§ 300jj–300jj-51, 17901–53).

208 15 U.S.C. § 1681 (2012).

209 Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247 (Mar. 15, 2006) (codified at 16 C.F.R. § 312 (2012)).

210 Press Release, Office of the Att'y Gen. of Conn., Attorney General Sues Health Net for Massive Security Breach Involving Private Medical Records and Financial Information on 446,000 Enrollees (Jan. 13, 2010), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=453918.

211 Fitzsimmons Interview, *supra* note 5; Jepsen Interview, *supra* note 49. In its settlement with Connecticut, HealthNet agreed to provide consumers with two years of credit monitoring, $1 million of identity theft insurance, and reimbursement for the costs of security freezes. Press Release, Office of the Att'y Gen. of Conn., Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info (July 6, 2010), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

212 *See, e.g.*, Commonwealth v. Beth Israel Deaconess Med. Ctr., Civ. No. 14-3627 (Mass. Sup. Ct. Nov. 20, 2014); State v. Innova Hosp., No. 2010CI-13714 (Tex. Cty. Ct. Oct. 11, 2010); State v. HealthNet, Civ. No. 2:11-CV-16 (Vt. Dist. Ct. Jan. 14, 2011); Press Release, Office of the Att'y Gen. of Md., Eye Care Retailer Settles in Data Security Lapse (Aug. 19, 2015), https://mdoag-public.sharepoint.com/press/2015/081915.pdf; Press Release, Office of the Att'y Gen. of N.Y., A.G. Schneiderman Announces Settlement with University of Rochester to Prevent Future Patient Privacy Breaches (Dec. 2, 2015), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-university-rochester-prevent-future-patient.

213 *See* Press Release, Office of the Att'y Gen. of N.Y., AG Schneiderman Announces Groundbreaking Consumer Protection Settlement with the Three National Credit Reporting Agencies (Mar. 9, 2015), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-groundbreaking-consumer-protection-settlement-three-national; *see also* AnnaMaria Andriotis, *Credit-Reporting Giants Agree to Overhaul*, WALL ST. J. (Mar. 9, 2015), http://www.wsj.com/articles/credit-reporting-giants-agree-to-overhaul-1425873884.

six percent of consumers had errors in their credit reports.[214] Subsequently, thirty-one attorneys general, led by Ohio, entered into a separate agreement with the three credit-reporting agencies under similar terms.[215]

Attorneys general have strengthened the privacy protections accorded children under COPPA, which requires website operators to obtain verified parental consent before collecting, using, or disclosing personal information collected from children under thirteen.[216] COPPA does not limit the type of data that can be collected from children.[217] Texas has sharpened COPPA's protections in cases against app providers that collected location data from children without telling their parents. Agreements included injunctive relief forbidding app providers from collecting location data from children under thirteen, whether or not parents provided consent.[218]

2. Data Security

Attorneys general have been active "first responders" to data breaches involving entities that are not regulated by federal privacy laws.[219] State

214 Consumer Fin. Servs. Grp., *NY Attorney General Enters into Far-Reaching Settlement with Largest Credit-Reporting Agencies*, BALLARD SPAHR (Mar. 19, 2015), http://www.ballardspahr.com/alertspublications/legalalerts/2015-03-19-ny-attorney-general-enters-into-far-reaching-settlement-with-largest-credit-reporting.aspx.

215 Press Release, Office of the Att'y Gen. of Ohio, Attorney General DeWine Announces Major National Settlement with Credit Reporting Agencies (May 20, 2015), http://www.ohioattorneygeneral.gov/Media/News-Releases/May-2015/Attorney-General-DeWine-Announces-Major-National-S; *see also* Jim McCabe, Angela E. Kleine & Sarah Nicole Davis, *Déjà Vu: State AG Consumer Reporting Settlement Follows Landmark New York Agreement*, MORRISON FOERSTER (May 26, 2015), http://www.mofo.com/~/media/Files/ClientAlert/2015/05/150526StateAGConsumerSettlement.pdf.

216 Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247 (Mar. 15, 2006) (codified at 16 C.F.R. § 312 (2012)).

217 *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Questions (explaining that operators under COPPA must provide notice to parents before collecting personal information from children, give parents the choice of consenting to collection and internal use of a child's information, and give parents the opportunity to prevent further use or online collection of a child's personal information); *see also* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2, at 603.

218 State v. Sun Ground, No. D-1-GV-14-000021 (Tex. Dist. Ct. Jan. 9, 2014) (order approving assurance of voluntary compliance); State v. Ploosh LLC, No. D-1-GV-13-001273 (Tex. Dist. Ct. Nov. 14, 2013) (order approving assurance of voluntary compliance); *Children's Apps Collected Personal Information*, FOX SAN ANTONIO NEWS (Nov. 4, 2015), http://foxsanantonio.com/news/tech/childrens-apps-collected-personal-information-11-06-2015 (discussing the Texas Attorney General's cases against children's app developers and agreements not to collect location data).

219 Christopher R. Nolen, *State Attorneys General Offer Perspectives on Data Breaches*, LEXOLOGY (Dec. 15, 2015), http://www.lexology.com/library/detail.aspx?g=54a5a467-747b-4d85-ad1d-3fafade085b79 ("[T]he state attorney general is the 'front-line' regulator dealing with companies that have suffered data privacy breach incidents.").

enforcement activity has been pursued under state data security,[220] data disposal,[221] encryption,[222] breach notification,[223] and UDAP laws.[224]

The FTC has embraced a process-based approach to data security, which entails assessing steps taken by entities to achieve "reasonable security."[225] Multistate AVCs and settlement agreements have emulated the FTC's approach.[226] An added benefit of state enforcement is that attorneys general can seek civil penalties for data security violations under UDAP and other state statutes.[227]

---

220 *See, e.g.*, CAL. CIV. CODE § 1798.81.5(b) (West 2016); Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00 (2010).

221 *See, e.g.*, CAL. CIV. CODE § 1798.81.5(b); CONN. GEN. STAT. § 42-471 (2015); 815 ILL. COMP. STAT. ANN. 530/40 (West 2012); MASS GEN. LAWS ch. 931, § 2.

222 *See, e.g.*, CAL. CIV. CODE § 1798.85(a)(3) (requiring encryption for Social Security numbers); CONN. GEN. STAT. § 42-470.

223 *See, e.g.*, CAL. CIV. CODE § 1798.82.

224 *See, e.g.*, CONN. GEN. STAT. §§ 42-110a–110q.

225 Thomas J. Smedinghoff, *An Overview of Data Security Legal Requirements for All Business Sectors* (Oct. 8, 2015), http://ssrn.com/abstract=2671323. That approach assesses whether entities have a security program, engage in periodic risk assessments, provide adequate training to employees, have plans to deal with potential breaches, ensure that outside data vendors secure data, and employ technical, physical, and administrative safeguards. *Id.* The process-based approach was adopted by Massachusetts in its data security regulations. *See generally* 201 MASS. CODE REGS. 17.00 (2010).

226 *See, e.g.*, People v. Comcast Cable Commc'ns Mgmt. LLC, No. RG15786197 (Cal. Super. Ct. Sept. 17, 2015) (order granting permanent injunction) (noting parties' agreement that defendant would strengthen restrictions on vendors); People v. Payday Loan Store of Ill., Inc., No. 10CH44962 (Ill. Cir. Ct. Oct. 3, 2012) (notice of dismissal by agreement) (including parties' agreement that defendant would provide employee training and adopt policy on destruction of data); State v. Villarreal, No. 2010-CI-13625 (Tex. Dist. Ct. Aug. 26, 2010) (order granting permanent injunction) (noting parties' agreement that defendant would adopt comprehensive security program); Assurance of Voluntary Compliance, *In re* Health Net, No. 10-040 (Office of the Att'y Gen. of N.Y. Aug. 2, 2010) [hereinafter Health Net AVC] (on file with author) (agreeing to train staff about mandatory encryption, adopt a comprehensive security program, and engage in a security audit by a third party); Assurance of Voluntary Compliance, *In re* TJX Cos., Inc., No. 09-083 (Office of the Att'y Gen. of N.Y. May 28, 2009) [hereinafter TJX Cos. AVC], http://www.infolawgroup.com/2009/07/articles/breach-notice/tjx-settles-with-state-attorneys-general-for-9-75-million/ (settling with forty-one attorneys general to adopt a program that matches the information security program required by the FTC's consent decree); Press Release, Office of the Att'y Gen. of Mass., TD Bank to Pay $625,000 to Address Data Breach Involving Thousands of Massachusetts Residents (Dec. 8, 2014), http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-12-08-td-bank.html (agreeing to implement written security program, conduct annual security audit, encrypt data, and take reasonable steps to ensure security procedures of data vendors).

227 Civil penalties have ranged from $70,000 to more than $9 million. *See, e.g.*, *Villareal*, No. 2010-CI-13625 ($70,000); TJX Cos. AVC, *supra* note 226 ($9.75 million). Under section 5, the FTC cannot seek civil penalties for unfair or deceptive data security practices. Hartzog & Solove, *Scope and Potential*, *supra* note 2.

Attorneys general have strengthened security protections for sensitive data.[228] Consider the recent investigation of Uber's internal location tracking system. Uber executives allegedly used the tracking system—called "God View"—to access the location of journalists' locations.[229] On January 6, 2016, Uber agreed to adopt security measures that would protect the real-time locations of riders.[230] The agreement required Uber to encrypt rider location data, adopt multi-factor authentication before employees could access "especially sensitive rider personal information," and limit access to location data.[231]

Another aspect of data security strengthened by state attorneys general relates to the assistance provided data-breach victims. Attorneys general routinely ask companies to provide victims with a year of free credit monitoring and identity-theft insurance.[232] Connecticut Attorney General George Jepsen has argued that consumers should receive two years of identity-theft insurance and credit monitoring in data breaches involving "highly sensitive information" even though state law only requires one year of credit monitoring.[233]

3. Bankruptcy

The FTC and state attorneys general have set important standards for the sale of consumer data in bankruptcy proceedings. Fifteen years ago, in *FTC v. Toysmart.com, LLC*,[234] the FTC and forty-four state attorneys general

228 In 2011, Massachusetts broke new ground in litigation against a restaurant chain that allegedly failed to protect credit card data even though it knew about a security breach. The settlement established that failing to adhere to the strict Payment Card Industry Data Security Standards amounted to a deceptive trade practice. Commonwealth v. Briar Grp., LLC, Civ. No. 11-1185 (Mass. Dist. Ct. Mar. 28, 2011) (order of final judgment by consent). Practitioners warned clients that the case would have "broad implications and telegraph the posture of the Massachusetts Attorney General in future data breach cases" and stands as a "harbinger of similar actions pursued in other jurisdictions on like grounds." *Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?*, EDWARDS ANGELL PALMER & DODGE (Apr. 2011), http://media.lockelord.com/files/upload/2011-CA-MA-AG-DataSecurity.pdf.

229 Kim Bellware, *Uber Settles Investigation into Creepy 'God View' Tracking Program*, HUFFINGTON POST (Jan. 6, 2016, 8:42 PM), http://www.huffingtonpost.com/entry/uber-settlement-god-view_568da2a6e4b0c8beacf5a46a.

230 Press Release, Office of the Att'y Gen. of N.Y., A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy (Jan. 6, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy.

231 *Id.*

232 OFFICE OF THE N.Y. STATE ATT'Y GEN., INFORMATION EXPOSED: HISTORICAL EXAMINATION OF DATA BREACHES IN NEW YORK STATE 14 (2014), http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf.

233 Jenna N. Felz, *Connecticut May Become First State to Require Identity Theft Protection*, BAKER HOSTETLER DATA PRIVACY MONITOR (June 15, 2015), http://www.dataprivacymonitor.com/data-breaches/connecticut-may-become-first-state-to-require-identity-theft-protection/ (internal quotation marks omitted) (quoting Attorney General Jepsen).

234 FTC v. Toysmart.com, LLC, Civ. No. 00-11341 (D. Mass. July 21, 2000).

asked a bankruptcy court to stop a toy retailer from selling customers' data because the company had promised not to share the data with third parties in its privacy policy. Their argument was that the sale would amount to a deceptive practice.[235]

Although the FTC offered to settle the case by allowing the sale to a qualified buyer, the attorneys general continued to object on the grounds that any sale would be unlawful without consumer consent.[236] The settlement was never approved, and consumers' data was destroyed.[237] Attorneys general next lobbied Congress to require the appointment of a consumer privacy ombudsman in bankruptcy proceedings.[238] The amendment was adopted in 2005.[239]

Since *Toysmart*, state attorneys general have challenged the sale of customer data in other bankruptcies, securing stronger protections than sought by the FTC.[240] In the bankruptcy proceedings for RadioShack, the FTC argued that the buyer should agree to be bound by RadioShack's privacy policy, which said that consumers' data would not be sold, or, alternatively, that RadioShack would obtain consumers' affirmative consent before transferring their personal data.[241] Thirty-eight attorneys general, however, insisted upon stronger protections. RadioShack settled with the states, agreeing to destroy most of the data, including Social Security numbers, telephone numbers, and dates of birth, and to reduce the number of data points per customer available for sale from 170 to 7.[242]

Attorneys general have secured protections for consumers' data beyond promises made in privacy policies. With their enforcement leadership, sales of highly sensitive personal data, such as sexual and dating preferences, have been prevented.[243] In cases where privacy policies were silent as to what would happen to data in the event of bankruptcy, attorneys general have convinced bankruptcy ombudsmen to ban the sale of sensitive data and to give consumers a chance to opt out of the sale of the remaining data.[244]

---

235 *States Active in Recent Mega Bankruptcies*, NAAG GAZETTE (June 30, 2009), http://www.naag.org/publications/naagazette/volume-3-number-5/states-active-in-recent-mega-bankruptcies.php.

236 *Id.*

237 *Id.*

238 *Id.*

239 *Id.*

240 *Id.*

241 *State AGs Demand Changes to Bankrupt RadioShack's Use of Customer Data*, HOGAN LOVELLS CHRON. DATA PROT. (July 22, 2015), http://www.hldataprotection.com/2015/07/articles/consumer-privacy/state-ags-demand-changes-to-bankrupt-radio-shacks-use-of-customer-data/.

242 *Id.*

243 *See, e.g.*, James R. Hood, *True.com Sale Is Off; Failed Buyer Trashes Texas Attorney General*, CONSUMER AFF. (Oct. 25, 2013), https://www.consumeraffairs.com/news/truecom-sale-is-off-failed-buyer-trashes-texas-attorney-general-102513.html.

244 *See, e.g.*, *States Active in Recent Mega Bankruptcies*, *supra* note 235 (reporting that attorneys general secured protections for consumer data in Circuit City bankruptcy, including banning sale of data that would trigger data-breach notification laws).

4. Privacy Governance

In the past fifteen years, major businesses have hired chief privacy officers to address privacy and data security concerns.[245] Emulating the approach of the FTC, state attorneys general have turned privacy's presence in the C-Suite from a voluntary practice into a legal requirement.[246] In multistate and individual actions, state attorneys general have required companies to integrate privacy professionals into corporate boardrooms.

Consider the multistate investigation of Google for collecting data from unsecured wireless networks nationwide through its Street View vehicles. An eight-state executive committee, led by Connecticut, investigated Google for its collection of network identification information and "payload data" transmitted over unsecured business and personal wireless networks between 2008 and March 2010.[247] Google acknowledged the possibility that the collected data included partial or complete email communications.

Thirty-eight states and the District of Columbia signed an AVC with Google resolving consumer protection and privacy claims.[248] As part of the AVC, Google agreed to adopt a privacy program requiring notification of senior management about the terms of the agreement, designation of an employee to coordinate the privacy program, employee training about the importance of user privacy, and development of policies and procedures for responding to events involving the unauthorized collection, use, or disclosure of user data. Google agreed to provide privacy awareness training to

245 BAMBERGER & MULLIGAN, *supra* note 3, at 251.

246 FTC consent decrees in consumer privacy cases typically require companies to establish comprehensive privacy programs that include the designation of an employee to coordinate and be responsible for the privacy program. *See, e.g.*, Decision and Order, *In re* Google Inc, No. C-4336 (Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf.

247 Press Release, Office of the Att'y Gen. of Conn., Attorney General Announces $7 Million Settlement with Google over Street View Collection of WiFi Data (Mar. 12, 2013), http://www.ct.gov/ag/cwp/view.asp?Q=520518. In addition to Connecticut, the executive committee included Arizona, Florida, Illinois, Kentucky, Massachusetts, Missouri, and Texas. *Id.* NAAG's chief counsel for cyber law, Hedda Litwin, advised the multistate group. *Id.* Other states joining the multistate agreement included Alaska, Arkansas, California, Colorado, Delaware, Hawaii, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Vermont, Virginia, and Washington. *Id.* Privacy advocacy group Electronic Privacy Information Center urged the Federal Communications Commission and the Department of Justice to investigate Google as well. Letter from Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr., to Julius Genachowski, Chairman, FCC (May 18, 2010), https://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf. The FCC fined Google for failing to comply with its investigation. *In re* Google, Inc., 27 FCC Rcd. 4012 (Apr. 13, 2012).

248 Press Release, Office of the Att'y Gen. of Conn., Assurance of Voluntary Compliance (Mar. 11, 2013), http://www.ct.gov/ag/lib/ag/press_releases/2013/20130312_google_avc.pdf.

counsel advising product teams. The company paid a seven-million-dollar fine to the states.

California has embraced this approach in recent cases. In 2015, California sued Houzz, an online home remodeling retailer, for recording telephone calls with consumers without informing them that they were being recorded in violation of California's wiretap and UDAP laws.[249] In a stipulated judgment, the company agreed to appoint an individual to serve as a chief privacy officer to oversee compliance with privacy laws and report concerns to company executives.[250] Houzz agreed to conduct a privacy risk assessment addressing its compliance with relevant privacy laws and that of its business partners with whom it shares consumers' personal data.[251] Wells Fargo similarly agreed to adopt a privacy program in its 2016 settlement with the California Attorney General's Office.[252]

As Kenneth Bamberger and Deidre Mulligan document in their important work, the presence of privacy professionals in corporate boardrooms is on the rise.[253] Following the lead of the FTC, attorneys general have reinforced such self-regulation with law, for the good of consumers.

* * *

State attorneys general have shaped privacy and data security policy in several ways. They have established privacy norms in the absence of federal leadership. They have pressed for thicker consumer privacy protections than those sought by federal agencies. They have reinforced federal norms in areas where federal agencies have had superior technical and policy expertise. The next Part assesses that work and makes suggestions for moving forward.

III. Moving Forward

As responses to FOIA requests and qualitative interviews demonstrate, attorneys general have been privacy pioneers. This Part turns from the past and looks towards the future. It highlights key features of AG offices that have been crucial to privacy policymaking in the hopes that those features can be replicated and improved.[254] It assesses criticism of state privacy

249 People v. Houzz Inc., No. 115-cv-286406 (Cal. Super. Ct. Oct. 2, 2015) (order granting permanent injunction), https://oag.ca.gov/system/files/attachments/press_releases/2015%2010-02%20-%20Final%20Judgment%20and%20Permanent%20Injunction.pdf. The FTC declined to investigate Google in the Street View matter.

250 *Id.*

251 *Id.*

252 People v. Wells Fargo Bank, No. BC611105 (Cal. Super. Ct. Mar. 28, 2016), https://oag.ca.gov/system/files/attachments/press_releases/Court%20approved%20Wells%20Fargo%20Stip%20Judgment%203_28_16_0.pdf?. Wells Fargo agreed to designate officers to oversee the company's compliance with its agreement not to record phone calls with consumers without notifying them that they are being recorded. *Id.*

253 *See* Bamberger & Mulligan, *supra* note 3.

254 Several states have expressed interest in learning from the privacy-related work of other offices. *See, e.g.*, Wright Interview, *supra* note 114 (discussing his desire, as Chief of

enforcement, including concerns that multiple enforcers risk over-deterrence and interest group capture. It evaluates calls for federal preemption of both AG enforcement power and state laws. It explores the implications of the dormant Commerce Clause doctrine. This Part identifies weaknesses in state enforcement activity and offers suggestions to enhance its efficiency, efficacy, and transparency. It ends with a turn to substance by urging state enforcers to address troubling practices that deserve regulatory oversight.

A. Strengths

States' chief law enforcers have responded quickly to consumer privacy concerns. This is partially because staff can pursue initiatives with little bureaucratic wrangling. After all, the buck stops with a single boss—the state attorney general. As Kathleen McGee, the Chief of New York's Internet Bureau, explains, "we do not have the politics of five commissioners so it is easier for us to move forward on cases."[255]

Also, unlike federal agencies, state attorneys general are directly accountable to voters, many of whom voice concerns about privacy and data security. Idaho AG Lawrence Wasden echoed others in noting that because privacy and data security are at the top of his constituents' list, they are at the top of his.[256] This Section explores the deeper structural reasons for such swift and nimble privacy policymaking.

1. Specialization

Offices of attorneys general—particularly career staff—have developed specialties that grow out of a familiarity with local conditions. They "are the first to see and understand the cons and conmen working their way through the system, receiving and fielding consumer complaints about everything . . . . [They] often see problems consumers are facing before [the FTC does] in Washington."[257] In turn, staff focus on the privacy and data security problems in their states.

Consider the specialization of the privacy leaders' offices. Since the birth of Silicon Valley, California's attorneys general have been finely attuned

---

the Consumer Protection Bureau, to expand the Delaware AG Office's privacy-related work); Kron Interview, *supra* note 52 (same). Joanne McNabb, California's privacy educator, has spoken to other AG offices for this reason. McNabb Interview Mar. 3, *supra* note 43.

255 McGee Interview, *supra* note 45.

256 Divonne Smoyer & Frederick Lah, *Idaho AG Talks Breach Notification, His Role as Privacy Enforcer*, IAPP (Oct. 28, 2014), https://iapp.org/news/a/idaho-ag-talks-about-breach-notification-his-role-as-privacy-enforcer/; *see also, e.g.*, Lemos, *supra* note 94, at 722–23 (explaining that attorneys general have incentive to respond to interests of constituents, which is amplified by their ambitions for higher office).

257 Comm'r Julie Brill, Keynote Address to the Nat'l Ass'n of Att'ys Gen.: Federal and State Law Enforcement Cooperation: A Lesson from Baseball (Mar. 6, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/federal-and-state-law-enforcement-cooperation-lesson-baseball/120305naagspeech.pdf.

to privacy and data security issues in the technology sector.[258] Health privacy and data security are focal points for Massachusetts[259] and Connecticut,[260] an outgrowth of the high concentration of hospitals and insurance compa-

258 This theme was clear from responses to FOIA requests, research, and interviews of AG Kamala Harris, *see* Harris Interview, *supra* note 13, and current and former staff, *see, e.g.*, Henrichsen Interview, *supra* note 8; LeBlanc Interview, *supra* note 124; McNabb Interview Mar. 3, *supra* note 43.

259 The Massachusetts Attorney General's Office has pursued enforcement actions against health providers for failing to maintain basic security practices and unreasonably delaying data-breach notification. *See, e.g.*, Press Release, Office of the Att'y Gen. of Mass., Boston Children's Hospital Settles Data Breach Allegations (Dec. 19, 2014), http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-12-19-boston-childrens.html; Press Release, Office of the Att'y Gen. of Mass., Beth Israel Deaconess Medical Center to Pay $100,000 Over Data Breach Allegations (Nov. 21, 2014), http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-11-21-beth-israel-data-breach.html; Press Release, Office of the Att'y Gen. of Mass., Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients (July 23, 2014), http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html; Press Release, Office of the Att'y Gen. of Mass., Former Owners of Medical Billing Practice, Pathology Groups Agree to Pay $140,000 to Settle Claims That Patients' Health Information Was Disposed of at Georgetown Dump (Jan. 7, 2013), http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-at-dump.html; Press Release, Office of the Att'y Gen. of Mass., South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations (May 24, 2012), http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html. The Massachusetts AG's Office has also provided training in data privacy protection to physicians. Press Release, Office of the Att'y Gen. of Mass., Physicians Receive Training and Education in Data Privacy Protection (Oct. 25, 2012), http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-10-25-physicians-training.html.

260 *See, e.g.*, Assurance of Voluntary Compliance, *In re* Hartford Hosp. (State of Conn., Dept. of Consumer Prot. Nov. 3, 2015), http://www.ct.gov/ag/lib/ag/press_releases/2015/20151105_hartford_hospital_privacyavc.pdf; Assurance of Voluntary Compliance, *In re* Yale Univ. (State of Conn., Dept. of Consumer Prot. May 11, 2015) (on file with author); Assurance of Voluntary Compliance, *In re* Metro. Life Ins. Co. (State of Conn., Dept. of Consumer Prot. Jan. 23, 2012), http://www.ct.gov/ag/lib/ag/press_releases/2012/1-24-12_metropolitan_life_insurance_co.pdf; Assurance of Voluntary Compliance, *In re* Griffin Hosp. (State of Conn., Dept. of Consumer Prot. Mar. 15, 2011) (on file with author); Assurance of Voluntary Compliance, *In re* Express Scripts, Inc. (State of Conn., Dept. of Consumer Prot. Oct. 11, 2010) (on file with author). The AG's Office has advised local hospitals on HIPAA and HITECH compliance. *See* 2011–2012 CONN. ATT'Y GEN. ANN. REP., http://www.ct.gov/ag/lib/ag/about_us/annualreport2011-12.pdf.

nies within their borders.[261] The New York attorney general's office has long focused on privacy issues involving the financial sector.[262]

Concerns of citizens heavily influence an attorney general's agenda.[263] As former Illinois Assistant AG Erik Jones explained, "[A]ttorneys general hear directly from the residents they serve on a daily basis."[264] For that reason, identity theft and data security have been a priority for Illinois AG Lisa Madigan.[265] Her office has heard from thousands of residents whose identities were stolen in the wake of data breaches.[266] Her constituents' struggles were behind her recent efforts to update the state's data-breach notification law.[267] For the same reason, combating illegal telemarketing is a priority for Indiana[268] and North Carolina.[269]

---

261 Also influential is the fact that Massachusetts has the most comprehensive state data security regulations in the country. *See* Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts, 201 MASS. CODE REGS. 17 (2010); *see also* Letter from Maura Healey, Mass. Att'y Gen., to Reps. Michael C. Burgess & Jan Schakowsky (Mar. 17, 2015), http://www.mass.gov/ago/docs/press/2015/ago-ltr-redsbna-of-2015.pdf.

262 *See* Lipka, *supra* note 161 and accompanying text (discussing New York's settlement with banks to restrict the use of bank-history database); Press Release, Office of the Att'y Gen. of N.Y., AG Schneiderman Announces Groundbreaking Consumer Protection Settlement, *supra* note 213; *see also*, Press Release, Office of the Att'y Gen. of N.Y., Spitzer Secures Privacy Agreement with National Bank (Jan. 25, 2000), http://www.ag.ny.gov/press-release/spitzer-secures-privacy-agreement-national-bank.

263 Lemos, *supra* note 94, at 747.

264 Jones, *supra* note 134. Jones is now a partner at Venable with a practice focusing on data privacy and state attorney general activity. *Erik Jones*, VENABLE LLP, https://www.venable.com/erik-jones/ (last visited Sept. 22, 2016). As Jones noted in our session on state AG privacy policymaking at the 2016 Privacy and Security Forum, inadequate data security was a crucial issue for AG Madigan because countless constituents struggled with the economic and emotional fallout of data breaches.

265 *See* Jones, *supra* note 134.

266 *Id.*

267 *Id.*

268 The most common complaint made to the Indiana AG's Office is unwanted telephone calls. *See AG Zoeller, Missouri AG's Office Host 3rd Annual No Call Summit Focused on New Efforts to Stop Unwanted Calls*, CITY COUNTY OBSERVER (Apr. 23, 2016), http://citycountyobserver.com/ag-zoeller-missouri-ags-office-host-3rd-annual-no-call-summit-focused-on-new-efforts-to-stop-unwanted-calls/. In 2015, the Office received 14,000 complaints about unwanted calls, the majority of which were about robocalls. *See AG Zoeller Urges Congress to Pass HANGUP Act, Ban All Robocalls to Cell Phones*, IN.GOV (Feb. 10, 2016), http://www.in.gov/activecalendar/EventList.aspx?view=EventDetails&eventidn=242410&information_id=237505&type=&syndicate=syndicate. AG Greg Zoeller helped strengthen the state's telephone privacy laws, banning nearly all types of robocalls. *See supra* note 200. Indiana has joined forces with Missouri to hold annual Do Not Call conferences to educate AG offices about consumers' rights and potential penalties. *See Do Not Call: The History of Do Not Call and How Telemarketing Has Evolved*, 1 NAGTRI J. 4 (2016), http://www.naag.org/publications/nagtri-journal/volume-1-number-4/do-not-call-the-history-of-do-not-call-and-how-telemarketing-has-evolved.php.

269 *See, e.g.*, Complaint, FTC v. Caribbean Cruise Line, Inc., Civ. No. 15-CV-60423 (S.D. Fla. Mar. 3, 2015); State v. ISI Alarms NC, Inc., 13 CV 014147 (N.C. Sup. Ct. Apr. 30, 2015)

Staff expertise extends beyond local concerns. The Texas Attorney General's Office has been at the forefront of privacy protections in bankruptcy sales since 2000.[270] Through changing administrations, career staff have secured protections for consumer data in various bankruptcy proceedings, including Living.com,[271] DrKoop.com,[272] True.com,[273] and RadioShack.[274]

The Vermont Attorney General's Office has shown an avid interest in data security.[275] Like other states, the Vermont data-breach notification law requires businesses to notify the office within fourteen days of discovering a

(order granting permanent injunction) (noting parties' agreement that defendant would abide by Do Not Call Registry and other telemarketing legal requirements and to pay the state $1 million); State v. Auto. Prot., LLC (N.C. Sup. Ct. Jan. 24, 2011) (order granting permanent injunction) (ordering the defendant to stop violating North Carolina's Telephone Solicitations Act and UDAP law); State v. Darain Atkinson et al., 10 Civ. 007470 (N.C. Sup. Ct. Nov. 8, 2010) (order granting permanent injunction) (describing defendant's settling of claims with North Carolina and ten other states related to violations of Do Not Call laws); Assurance of Voluntary Compliance, *In re* Rosetta Stone Comm. (Office of the Att'y Gen. of N.C. Apr. 14, 2011) (on file with author) (agreeing to comply with state and federal telemarketing laws related to autodialed and pre-recorded calls, to implement written procedures for employees to ensure compliance with the law, and to pay $10,000 in civil penalties to state); Assurance of Voluntary Compliance, *In re* Pub. Policy Polling, LLC (Office of the Att'y Gen. of N.C. Sept. 3, 2010) (on file with author); Assurance of Voluntary Compliance, *In re* Blue Cross Blue Shield of N.C. (Office of the Att'y Gen. of N.C. Jan. 27, 2010) (on file with author) (agreeing not to contact North Carolina residents with pre-recorded messages in violation of North Carolina law and to pay $95,000 in civil penalties to the state).

270 Todd R. Weiss, *Texas Attorney General Sues to Stop Living.com Data Sale*, COMPUTERWORLD (Oct. 2, 2000), http://www.computerworld.com/article/2588972/data-privacy/texas-attorney-general-sues-to-stop-living-com-data-sale.html (explaining that after Texas sued the online retailer to prevent the sale of customer data in bankruptcy proceedings, the company agreed to destroy consumers' financial data and to sell customer list only if consumers had a chance to remove their names).

271 *Id.*

272 *Texas AG Reaches Privacy Settlement with Dr. Koop*, AUSTIN BUS. J. (Mar. 20, 2002), http://www.bizjournals.com/austin/stories/2002/03/18/daily24.html (noting that the Texas AG reached an agreement with the trustee administering the bankruptcy liquidation of the company providing access to medical databases and publications).

273 Bryan Cohen, *Texas AG Settles with Bankrupt Online Dating Service*, LEGAL NEWSLINE (Dec. 12, 2013), http://legalnewsline.com/stories/510516699-texas-ag-settles-with-bankrupt-online-dating-service.

274 Texas was the first of thirty-eight state attorneys general to object to RadioShack's proposed sale. Melanie Cohen, *The Daily Docket: Texas AG Cites Privacy Concerns in RadioShack Customer Data Sale*, WALL ST. J. BLOG (Apr. 17, 2015, 10:14 AM), http://blogs.wsj.com/bankruptcy/2015/04/17/the-daily-docket-texas-ag-cites-privacy-concerns-in-radioshack-customer-data-sale/; *see also* Press Release, Office of the Att'y Gen. of Tex., Attorney General Paxton Objects to Sale of Texans' Personal Data in RadioShack Bankruptcy Case (Mar. 25, 2015), https://www.texasattorneygeneral.gov/oagnews/release.php?id=5000.

275 Kriger Interview, *supra* note 38.

breach.[276] This has allowed the office to intervene on behalf of Vermont citizens—with the chance of improving data security beyond its borders.[277]

2. Multistate Cooperation

Another strength is the ability of state enforcers to collaborate with each other.[278] Members of the NAAG Privacy Working Group hold monthly telephone calls to discuss best practices and emerging risks.[279] They coordinate responses to data breaches impacting citizens across the country.[280]

Interviews with attorneys general and career staff have highlighted the importance of multistate efforts to share expertise and conserve resources.[281] The Texas Attorney General's Office, for instance, often takes the lead in bankruptcy proceedings,[282] while Connecticut and Illinois frequently spearhead data security cases.[283] Members of the NAAG Privacy Working Group also take turns leading multistate investigations.[284] Small states join multistate efforts in cases where they would have lacked the resources and expertise to proceed alone.[285] Crucially, multistate investigations grow in strength as more states participate. The Chief of the Illinois Consumer Protection Bureau, Deborah Hagan, explained that attorneys general enjoy more lever-

276 VT. STAT. ANN. tit. 9, § 2435 (West 2016).

277 Kriger Interview, *supra* note 38. Vermont Assistant AG Ryan Kriger explained that a small state like Vermont can impact data security practices across the country when it investigates data breaches impacting citizens nationwide. *Id.* To take just one month—July 2014—the Vermont AG's Office communicated with thirty-one companies, mostly with national operations, to press for remedial actions in the wake of data breaches. FOIA Response Letter (Vermont) (on file with author).

278 *See, e.g.*, Brief for Attorneys General as Amici Curiae Supporting General Hood's Motion to Dismiss, Google, Inc. v. Jim Hood, No. 3:14-CV-981, 2015 WL 1029600 (S.D. Miss. Feb. 15, 2015) (supporting Mississippi's request for discovery in its investigation of Google).

279 Cable Interview, *supra* note 59.

280 *Id.*

281 Fitzsimmons Interview, *supra* note 5; Hagan & Van Hise Interview, *supra* note 5; Jepsen Interview, *supra* note 49; McNabb Interview July 20, *supra* note 59.

282 *See supra* notes 270–74 (discussing bankruptcy cases led by Texas).

283 Connecticut and Illinois are leading investigations into data breaches of eBay (with Florida's assistance), *see* Ryan Mac, *California Joins Other States in Investigation of eBay Hack*, FORBES (May 23, 2014), http://www.forbes.com/sites/ryanmac/2014/05/23/as-ebay-notifies-users-of-hack-states-launch-investigation/#3af21dd4bd6a, Neiman Marcus, *see* Chris Dolmetsch & Andrew Harris, *Connecticut Attorney General Probing Neiman Marcus Breach*, BLOOMBERG NEWS (Jan. 14, 2014), http://www.bloomberg.com/news/articles/2014-01-13/connecticut-attorney-general-probing-neiman-marcus-breach, and Home Depot (with California's assistance), *see, e.g.*, Jonathan Randles, *States Investigate Home Depot Breach*, LAW360 (Sept. 9, 2014), http://www.law360.com/articles/575613/states-investigate-home-depot-data-breach.

284 *See id.*

285 Conti Interview, *supra* note 53 (discussing Maine's involvement in various multistate investigations).

age proceeding together than if they pursue cases individually.[286] Particularly in data-breach matters, multistate efforts garner considerable support, likely because constituents express considerable concern about identity theft.

To be sure, in any given multistate investigation, there are usually a handful of states that decline to participate. Why would states remain on the sidelines? One possibility is that their offices are preoccupied with other issues; another is the potential influence of lobbyists. Nonetheless, what can be said is that cooperation has been the overwhelming trend when it comes to consumer privacy and data security matters.

Of course, productive relationships among state attorneys general are not inevitable. AG offices could interfere with multistate cooperation. For instance, an attorney general could offer a weak settlement to a company, undermining the negotiating position of a multistate group interested in establishing thicker protections for consumers.[287] Staff could break away from a multistate effort to earn political points for the boss.[288] These scenarios are possible, but the experience of the NAAG Privacy Working Group shows that cooperation happens more frequently than not. Productive relationships amongst career staff and limited state budgets weigh in favor of collaboration.[289]

Then too, multistate agreements can harmonize norms across jurisdictions, especially as more and more states participate. They set privacy policy for a company's activities in the signature states.[290] Crucially, multistate settlements have stabilized and entrenched norms set by the FTC,[291] especially in the area of data security.[292]

3. Federal Agencies: Synergies and Dialogue

Attorneys general have enjoyed a synergistic relationship with federal agencies working on privacy and data security issues. This has been true since the earliest days of AG engagement with consumer protection issues. In the 1970s, the FTC was crucial to the passage of state UDAP laws, which gave enforcement power to attorneys general.[293]

---

286 Hagan & Van Hise Interview, *supra* note 5.

287 Former Maryland Assistant AG Steven Ruckman helped me think through these possible scenarios.

288 Some limelight-seeking is inevitable and potentially productive. *See* Lemos, *supra* note 94, at 742 (explaining that because attorneys general are elected, they have "incentive to make a name for themselves"). An attorney general might break away from others' efforts to press for greater protections for constituents.

289 Cable Interview, *supra* note 59.

290 *See supra* note 247 (discussing how precedent set in Google matters went further than the FTC consent decree in protecting consumers' privacy choices).

291 *See supra* notes 226–27 (discussing multistate AVC in the TJX data-breach case).

292 *See, e.g.*, TJX Cos. AVC, *supra* note 226; Assurance of Voluntary Compliance, *In re* Choicepoint (Or. Dep't of Justice May 30, 2007) (on file with author).

293 *See* Cole, *supra* note 29, at 126. The FTC promoted state UDAP laws because state attorneys general lacked authority to enforce section 5 and the FTC needed help protecting consumers from unfair and deceptive trade practices. *Id.*

The FTC has remained a strong supporter of state privacy enforcers. Then-FTC Commissioner Julie Brill, who stepped down from her post near the end of her term, has emphasized the crucial role played by attorneys general in privacy regulation.[294] At a NAAG meeting, she noted that the FTC has "relied on our partners in the states to help us carry out our mission to protect consumers as they navigate the marketplace . . . in today's fast-paced, technologically advanced world, we depend on you more than ever."[295]

Federal agencies and state attorneys general have joined forces in efforts to nudge compliance.[296] For instance, New York AG Eric Schneiderman and the FCC criticized PayPal's proposal to condition service on consumers' receipt of robocalls.[297] As AG Schneiderman and the FCC noted in public statements, PayPal's proposed policy would violate the Telephone Consumer Protection Act.[298] In social media, consumers expressed their disapproval of PayPal's plan.[299] PayPal soon reversed course, agreeing to make robocalls only to consumers who explicitly opted in to receiving them.[300] FCC's Chief of Enforcement Travis LeBlanc explained that PayPal—like other companies faced with bad publicity—went further than what the law required to contain the damage to its reputation.[301]

294 Divonne Smoyer & Christine Nielsen Czuprynski, *FTC Commissioner Brill Urges State AGs to Up the Ante*, REEDSMITH TECH. L. DISPATCH (July 25, 2014), http://www.technology-lawdispatch.com/2014/07/privacy-data-protection/ftc-commissioner-brill-urges-state-ags-to-up-the-ante/. Before serving as FTC commissioner, Brill served as an assistant AG in two state attorney general offices, Vermont and North Carolina. *Id.*

295 Brill, *supra* note 257.

296 The relationship between attorneys general and federal agencies reflects a "polyphonic federalism" that Robert Schapiro envisions in his work. *See, e.g.*, ROBERT A. SCHAPIRO, POLYPHONIC FEDERALISM: TOWARD THE PROTECTION OF FUNDAMENTAL RIGHTS (2009) (exploring state and federal relations as promoting plurality, diversity, and productive dialogue in a dynamic, bottom-up way).

297 Dani Kass, *FCC, NY AG Question PayPal, EBay Autodialing Policies*, LAW360 (June 11, 2015), http://www.law360.com/articles/666650/fcc-ny-ag-question-paypal-ebay-autodialing-policies.

298 Jennifer Abel, *New York Attorney General Questions PayPal and eBay Robocall Mandates*, CONSUMER AFF. (June 11, 2015), http://www.consumeraffairs.com/news/new-york-attorney-general-questions-paypal-and-ebay-robocall-mandates-061115.html.

299 *See* Zach Miners, *PayPal Users May Get Break on Unsolicited Robocalls, Texts*, COMPUTERWORLD (Jun. 8, 2015), http://www.computerworld.com/article/2932320/data-privacy/paypal-users-may-get-break-on-unsolicited-robocalls-texts.html; *see also* Twitter, https://twitter.com/search?q=%23paypal%20%23robocalls&src=typd (Oct. 18, 2016) (a search of tweets containing #paypal and #robocalls).

300 Press Release, Office of the Att'y Gen. of N.Y., Statement by AG Schneiderman on Paypal's Robocalling Commitments (June 29, 2015), http://www.ag.ny.gov/press-release/statement-ag-schneiderman-paypal%E2%80%99s-robocalling-commitments.

301 LeBlanc Interview, *supra* note 124. Before taking over as Chief of Enforcement for the FCC, LeBlanc served as the top deputy and senior adviser to AG Harris and ran California's first high-tech crime and data privacy unit. Press Release, FCC, FCC Chairman Wheeler Announces Appointment of Acting Chief, Enf't Bureau (Mar. 4, 2014), https://www.fcc.gov/document/chairman-wheeler-appointment-acting-chief-enforcement-bureau.

An important illustration of the synergistic relationship between the FTC and attorneys general involves Google. In 2011, the FTC entered into a consent order with Google requiring it to obtain outside audits of its privacy practices for the next twenty years.[302] Attorneys general reinforced the FTC's efforts.[303] In a letter sent by NAAG in 2012, thirty-nine attorneys general criticized Google's unified privacy policy, which allowed the company to share consumers' personal data across its services.[304] As the group of state attorneys general argued, consumers did not have a real choice to "exit the Google products ecosystem."[305] The group pressed Google to give consumers the ability to review and delete data collected about them from different Google services.[306] The attorneys general urged the company to be more transparent about the types of personal data collected by each service.

In 2013, Google agreed to changes related to the transparency of its data practices. Consumers were notified of ways that they could keep information associated with one service separate from information associated with another; consumers were given the ability to see how some data was collected and shared across services. FTC Commissioner Brill noted: "That 39 AGs recently called on Google to explain its new privacy policies shows we are not only on the same team—we are on the same page of a winning playbook."[307]

The relationship between federal agencies has also generated productive dissent, the sort of "uncooperative federalism" explored by constitutional law scholars Jessica Bulman-Pozen and Heather Gerken.[308] The case involving Google's failure to respect consumers' do-not-track settings exemplifies the point.[309] There, state attorneys general pressed for thicker consumer privacy protections, forsaking the thinner protections in the FTC's consent decree.[310]

The precedent set in multistate agreements—such as the Google and PointRoll matters—could prod a change in the FTC's privacy jurisprudence,

302 Decision and Order, *In re* Google, Inc., No. C-4336, (Oct. 13, 2011); Press Release, FTC, FTC Gives Final Approval to Settlement with Google over Buzz Rollout (Oct. 24, 2011), http://www.ftc.gov/opa/2011/10/buzz.shtm.

303 Brill, *supra* note 257.

304 Letter from Nat'l Ass'n of Att'ys Gen. to Larry Page, CEO of Google (Feb. 22, 2012), https://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf.

305 *Id.*

306 Letter from Twenty-three Att'ys Gen. to Larry Page, Chief Exec. Officer, Google, Inc., (July 3, 2013), https://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf.

307 Brill, *supra* note 257.

308 Jessica Bulman-Pozen & Heather K. Gerken, *Uncooperative Federalism*, 118 YALE L.J. 1256, 1271 (2009).

309 *See supra* notes 143–45 and accompanying text.

310 *See supra* notes 148–54. The Google Street View investigation fits in the same mold. Although privacy advocacy group EPIC urged the Department of Justice and the FCC to investigate Google's collection of consumers' unencrypted Wi-Fi payload data in 2010, only the states, with the leadership of Connecticut, pursued the matter vigorously, ending with an AVC with thirty-eight states. *See supra* note 154; *see also* Comments of Marc Rotenberg, Bright Ideas Discussion at EPIC, July 15, 2016 (on file with author).

much in the way that Daniel Solove and Woodrow Hartzog have called on the FTC to press for thicker norms.[311] The FTC is more likely to embrace evolving norms if they reflect existing best practices. The precedent set by state attorneys general could help nudge best practices towards greater consumer protections that the FTC might endorse in its privacy jurisprudence. Because attorneys general serve as "connected critics" to the FTC, they may have a powerful bid for the FTC's attention.[312] In short, attorneys general serve as crucial partners, dissenters, and enforcement gap fillers vis-à-vis federal agencies.

4. EU Harmonization

Might industry look favorably on AG enforcement activity because, in certain respects, it comports with EU requirements, especially if companies collect data from European citizens? In 2016, the Department of Commerce and European regulators struck a deal that will allow U.S. companies to handle European citizens' personal data if they agree to follow certain data protection principles.[313] Depending on the circumstances, U.S. companies may be expected to comply with the EU General Data Protection Regulation

311 Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2.

312 *See* Bulman-Pozen & Gerken, *supra* note 308, at 1288 (discussing the role of the connected critic in the uncooperative federalism model).

313 Under the European Commission's Directive on Data Protection of 1998, EU Member States cannot transfer personal data to countries that lack an "'adequa[te]' standard for privacy protection." *U.S.-EU Safe Harbor Overview*, EXPORT.GOV (Dec. 18, 2013), https://build.export.gov/main/safeharbor/eu/eg_main_018476. Under the EU-U.S. Safe Harbor agreement, U.S. companies could handle the personal data of the citizens of EU Member States if they agreed to follow seven data-practice principles. *Id.* In 2015, a European Court of Justice decision, Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 362/14, invalidated the EU Safe Harbor agreement based on the U.S. surveillance practices exposed by Edward Snowden. On February 2, 2016, European authorities and U.S. officials struck an agreement that renegotiated the Safe Harbor deal, allowing businesses to continue moving people's digital information across the Atlantic. *See* Mark Scott, *U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await*, N.Y. TIMES (Feb. 2, 2016), http://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html?_r=0. The deal was officially approved by the EU's Member States. *See* Hogan Lovells, *Privacy Shield Receives Final Approval from European Commission—Some Initial Practical Advice*, CHRON. DATA PROT. (July 12, 2016), http://www.hldataprotection.com/2016/07/articles/international-eu-privacy/privacy-shield-receives-final-approval-from-european-commission-some-initial-practical-advice-for-clients/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ChronicleOfDataProtection+%28HL+Chronicle+of+Data+Protection%29; *see also* Press Release, Eur. Comm'n, Statement by Vice-President Ansip and Commissioner Jourová on the Occasion of the Adoption by Member States of the EU-U.S. Privacy Shield (July 8, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm. As Omer Tene, Vice President of Research and Education at the International Association of Privacy Professionals, explains, there are lingering concerns that the Privacy Shield may not satisfy the additional requirements and burdens of the GDPR. Bradley Barth, *Survey: 34% of Privacy Pros Expect Their Companies to Certify Under Privacy Shield*, SC MAG. (Sept. 1, 2016), http://www.scmagazine.com/survey-34-of-privacy-pros-expect-their-companies-to-certify-under-privacy-shield/article/519777/.

(GDPR).[314] Paul Schwartz has discussed efforts to harmonize EU-U.S. privacy policymaking in the shadow of a looming collision with EU data regulations.[315]

Adhering to AG privacy policymaking would enable compliance with the European approach in certain respects.[316] Data-breach notification norms are similar to the GDPR's requirement that data controllers notify individuals about data breaches without "undue delay" in certain circumstances.[317] State AG enforcement has provided special protection for sensitive information, which resonates with provisions of the GDPR.[318] California urges companies to explain their privacy policies in a clear and understandable manner, much as in the EU.[319] Compliance with AG privacy norms cannot avoid all of the collisions that Paul Schwartz insightfully explores, but to the extent that they do, there is an upside to following them. Adhering to the norms set by AG enforcement actions can facilitate compliance with certain EU regulations.[320]

314 EU Member States accord omnibus protections to the handling of all personal data. *See* Schwartz, *The Value of Privacy Federalism*, *supra* note 1. Each EU Member State has its own data protection commission. *Id.* By contrast, privacy regulation in the United States does not come from a single source or regulator but rather from a combination of federal and state legislation, federal agencies, and state attorneys general. *Id.*

315 *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

316 Thanks to Tanya Forsheit, Jules Polonetsky, Peter Swire, and Chris Wolf, who emphasized this point with me. As Tanya Forsheit noted, with the passage of California's Electronic Communications Privacy Law and the work of AG Harris, California could be understood as compliant with EU data protection laws, if such a possibility could exist. Telephone Interview with Tanya Forsheit, Partner, Frankfurt, Kurnit, Klein & Selz (Dec. 9, 2015).

317 The data-breach notification provisions of the GDPR were inspired by federal and state data-breach notification laws. In a plenary session, the European Parliament approved the GDPR. *See Data Protection Reform—Parliament Approves New Rules Fit for the Digital Era*, EUR. PARLIAMENT NEWS (Apr. 14, 2016), http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era.

318 *See supra* notes 185–87, 218, 230 (discussing, respectively, California's approach to the nonconsensual posting of nude images, Texas's various informal agreements banning the collection of children's location data due to its sensitive nature, and New York's informal agreement to protect highly sensitive location data).

319 *Say What You Do and Do What You Say: Guidance for Privacy Policies, and for Life*, INFORMATIONLAWGROUP (May 26, 2014), http://www.infolawgroup.com/2014/05/articles/privacy-law/guidelines-for-your-privacy-policies-and-your-life-say-what-you-do-and-do-what-you-say/. California's best practices urge companies to inform consumers about what types of data are collected, with whom data is shared, how long data is retained, and how data can be corrected in a clear and easily understandable way, akin to the approach of the GDPR. *Id.*

320 I am grateful to Margot Kaminski for urging me to frame the issue in this way.

B. Objections and Proposals

AG privacy enforcement has been subject to criticism. Some object to having more than fifty state enforcers on the beat and to the diverse array of state laws applied by them. This Section addresses concerns about the potential pile-up of enforcement activity and calls for federal preemption. It discusses the possibility of interest group capture and the implications of dormant Commerce Clause doctrine. It turns to weaknesses in the tactics and strategies employed by state attorneys general, and it offers solutions. This Part ends by exploring new directions for AG privacy policymaking.

1. Threshold Concerns

A common objection to AG privacy enforcement is that "having fifty-plus attorneys general and federal agencies on the beat leads to over-enforcement and overwhelms companies."[321] Federal administrative law has something to teach us in this respect. In *FTC v. Standard Oil Co. of California*, the Supreme Court held that the cost of an investigation by one agency is "part of the social burden of living under government."[322] But does that presumption change if a company faces investigations by fifty or more regulators? Is there something legally significant about the potential pile-up effect? Should Congress preempt state enforcement? Should it preempt state data security and privacy laws in favor of a uniform federal standard? Instead of over-deterrence, is the risk one of too little enforcement due to capture by corporate interests?

a. Pile-Up Effect

The specter of fifty state attorneys general pursuing a company for privacy or data security violations is more theoretical than real. As Massachusetts Assistant AG Sara Cable remarked, "The idea that all 50 attorneys general will jump on a company separately is an illusion."[323] Of course, state attorneys general could bring separate actions against companies, but they hardly ever do so in practice. Entities do not face fifty or more separate investigations and enforcement actions, let alone more than one.

That trend will likely continue. Because states have limited resources, AG offices look for partners to share the burdens of litigation.[324] Similarly,

321 Kriger Interview, *supra* note 38.

322 449 U.S. 232, 244 (1980) (quoting Petroleum Expl., Inc. v. Pub. Serv. Comm'n, 304 U.S. 209, 222 (1938)).

323 Cable Interview, *supra* note 59.

324 States have lined up on different sides in amicus briefs to courts. This was true in the *Spokeo v. Robins* case, 136 S. Ct. 1540 (2016), which addressed whether plaintiffs had Article III standing to sue a people-search website under the federal Fair Credit Reporting Act for failing to maintain procedures to ensure the accuracy of personal data collected and shared with employers. In an amicus brief submitted to the Supreme Court on behalf of twelve other states and the District of Columbia, Massachusetts argued that false information in a data profile can be expected to cause negative consequences for consumers,

businesses favor multistate litigation because it is cheaper and easier to negotiate with an office (or group of offices) representing several states. States and companies have strong incentive to prefer multistate proceedings rather than separate actions.

Overlapping state investigations—though rare—have been productive. Recall that three major credit-reporting agencies faced an investigation by New York and a separate multistate investigation, which resulted in agreements with similar terms. Although there were duplicate costs, the pile-up was productive. As Chris Hoofnagle explained, the major credit-reporting agencies had brazenly ignored the mandates of FCRA for years and federal agencies did nothing about it.[325] Under-enforcement was the norm for decades. The concurrent investigations put important pressure on credit-reporting agencies to clean up their acts.[326]

What about duplicative state and federal actions? Again, though rare, when entities have faced separate federal and state investigations, productive dialogue has been the result. Recall that the FTC and the multistate group investigated Google for deploying code that changed consumers' no-track settings.[327] There, overlapping federal-state jurisdiction and separate enforcement actions led to valuable dissent, rather than the same result for double the price.

Of course, if the pile-up effect becomes a reality, entities could urge state legislators to cut the budget of attorneys general or to limit the scope of their authority.[328] As Margaret Lemos explains, business interests are capable of being heard by state legislatures and shutting down state AG enforcement.[329] Industry could lobby Congress to limit the role of state attorneys general in privacy and data security enforcement.

Now to the normative question of whether Congress should shut attorneys general out of the enforcement calculus.

---

including lost jobs. Press Release, Office of the Att'y Gen. of Mass., AG Healey Files Supreme Court Brief Promoting Integrity and Fair Use of Personal Data (Sept. 9, 2015), http://www.mass.gov/ago/news-and-updates/press-releases/2015/2015-09-09-spokeo-amicus.html. On behalf of seven other states, Alabama argued against standing on the grounds that class actions threaten the viability of businesses and that narrow, technical violations of FCRA should not satisfy the injury-in-fact requirement. Brief for Alabama et al. as Amici Curiae Supporting Petitioner, Spokeo v. Robins, 136 S. Ct. 1540 (2016) (No. 13-339). The disagreement in *Spokeo* grew out of concerns about class action litigation rather than the merits of consumer privacy policy.

325 Memorandum from Chris Hoofnagle, Adjunct Professor of Law, Berkeley Sch. of Law (Jan. 15, 2015) (on file with author).

326 *Id.* There have been pile-ups of state attorneys general, notably in the tobacco litigation. *See* MARTHA A. DERTHICK, UP IN SMOKE: FROM LEGISLATION TO LITIGATION IN TOBACCO POLITICS (3d ed. 2012).

327 *See supra* note 144.

328 Colin Provost, *The Politics of Consumer Protection: Explaining State Attorney General Participation in Multi-State Lawsuits*, 59 POL. RES. Q. 609, 613 (2006).

329 Lemos, *supra* note 94, at 748.

b. Preempting State Enforcers

Should Congress curtail or eliminate the enforcement role of state attorneys general in privacy and data security matters on the grounds that their participation risks undue complexity, high costs, and over-deterrence? Federal laws could limit or remove AG offices' ability to enforce privacy and security consumer protections.

In considering such proposals, Congress should proceed carefully.[330] State enforcers are essential to the efficient deterrence of privacy and data security violations given the increasing marginalization of private law and the practical constraints on federal agencies. Typically, public enforcement and private law claims operate together to discipline the market.[331] But this is not so for data harms, by which I mean setbacks to consumers' legally protected interests due to inadequate data security or other privacy violations.[332] Why not?

Although the most logical place for plaintiffs to begin is with the privacy torts, they provide little relief for contemporary privacy and security problems. Overly narrow interpretations of the privacy torts—intrusion on seclusion, public disclosure of private fact, false light, and misappropriation of image—have prevented their ability to redress data harms.[333] Similarly, negligence, contract, and private UDAP claims are routinely dismissed due to a lack of an "injury in fact" sufficient to support a finding of standing or cognizable harms, or due to the economic loss rule.[334] For most courts, privacy and data security harms are too speculative and hypothetical, too based

330 Proposed federal data-breach notification laws have pressed the point. Some would eliminate state enforcement; others would curtail the role of attorneys general in the enforcement of a federal data-breach notification law. *See, e.g.*, Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015). Under the Data Security and Breach Notification Act of 2015, state attorneys general could bring enforcement actions for data security failures only if the FTC has declined to do so. *Id.* Massachusetts AG Maura Healey opposes the bill because it "inject[s] unnecessary delay and costs, and unnecessarily complicat[es] their efforts to enforce their respective consumer protection laws." Letter from Maura Healey, Mass. Att'y Gen., to Michael C. Burgess, Chairman of H. Subcomm. on Com., Mfg. & Trade, & Jan Schakowsky, Ranking Member of H. Subcomm. on Com., Mfg. & Trade (Mar. 17, 2015), http://www.mass.gov/ago/docs/press/2015/ago-ltr-re-dsbna-of-2015.pdf.

331 David C. Vladeck, *Preemption and Regulatory Failure Risks*, *in* PREEMPTION CHOICE, *supra* note 23, at 54, 56 (explaining that tort law helps fill regulatory gaps by forcing the disclosure of information, deterring excessive risk taking, and securing redress for injuries).

332 *See* Catharine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. (forthcoming 2017); Daniel J. Solove & Danielle Keats Citron, Data Harms: Rethinking Privacy and Data Security Injuries (unpublished manuscript) (on file with author).

333 Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1826–28 (2010) [hereinafter Citron, *Mainstreaming*].

334 *See, e.g.*, *In re* Sci. Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014). A minority of courts have upheld class actions in data-breach cases, including the Seventh Circuit. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819

on subjective fears and anxieties, and not concrete and significant enough to warrant recognition.[335]

Given that private litigation is not an avenue for efficient deterrence, the more salient risk of curtailing or, more drastically, eliminating state AG enforcement is under-deterrence.[336] Federal authorities cannot attend to most privacy and security problems because their resources are limited and their duties ever expanding.[337] Simply put, federal agencies have too few resources and too many responsibilities.

If enforcement were solely in the hands of federal agencies, local matters would surely be overlooked. This is especially true for data security matters. Vermont's Assistant AG Ryan Kriger explained, "Attorneys general fill an important niche by serving as the local cop on the beat. They investigate local actors whose poor data practices impact citizens of our state."[338] The FTC has brought a little over fifty data security cases in the past ten years due to limited resources.[339] State enforcers have been filling enforcement gaps. Attorneys general were given the authority to pursue HIPAA violations precisely because Congress recognized that the Department of Health and Human Services' Office of Civil Rights could not do it all. State attorneys general complement the efforts of federal agencies, and, as we have seen, they strengthen existing protections.[340]

The FTC has been applauded for its norm-setting and norm-guiding efforts, and rightly so.[341] Since 1997, the FTC has held workshops, issued guidance documents, and met with stakeholders.[342] The FTC's settlements have established a jurisprudence of privacy.[343] But what will happen in the

F.3d 963 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

335 *See, e.g.*, *In re* Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013); Hammer v. Sam's E., Inc., No. 12-cv-2618, 2013 WL 3756573 (D. Kan. July 16, 2013).

336 Municipalities may have power to enforce UDAP laws, and some do engage in privacy policymaking. The costs of coordination, however, would be significant, and no network like NAAG exists to facilitate those efforts.

337 *See* David A. Hyman & William E. Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 GEO. WASH. L. REV. 1446 (2014).

338 Kriger Interview, *supra* note 38. Since the 1980s, the FTC has explicitly focused on national trade practices. HOOFNAGLE, *supra* note 2.

339 *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (discussing "10 practical lessons businesses can learn from the FTC's 50+ data security settlements").

340 *Id.* at 2256. In 1969, an ABA commission urged the FTC to coordinate with local enforcement agencies to have them handle local consumer abuses. REPORT OF THE ABA COMM'N TO STUDY THE FED. TRADE COMM'N (1969), *reprinted in* 1 J. REPRINTS FOR ANTITRUST L. & ECON. 883, 948 (1969) [hereinafter REPORT OF THE ABA COMM'N].

341 Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2, at 600.

342 *Id.* at 625.

343 *Id.* at 619.

coming years is unclear.[344] President-elect Donald Trump has two commissioner seats to fill and will appoint a new chairperson to lead the agency.[345] Career staff's consumer privacy and data security efforts may be stymied by politics.[346]

Added to that concern are federal lawmakers' efforts to slash the FTC's budget.[347] Attorneys general would serve as a crucial fail-safe in the event that the FTC was forced to slow down its privacy and security work. Chris Hoofnagle has written about the role that state attorneys general played after an angry Congress shut down the FTC not once but twice in the 1980s after the agency crusaded too vigorously against used car salesmen, the funeral industry, and children's advertising.[348] Reagan-era leadership brought the FTC nearly to a halt, and during this time, class action lawyers and state attorneys general took up the slack.[349] More recently, state attorneys general stepped in to address predatory lending, discriminatory lending, and foreclosure abuse when federal enforcers failed to address fraudulent practices related to the mortgage crisis of the late 2000s.[350] This possibility cautions against efforts to preempt the privacy enforcement power of state attorneys general.

Given the important role that attorneys general have played in addressing privacy and data security issues, their enforcement power should not be curtailed or eliminated without careful consideration. Attorneys general have pioneered, shaped, and stabilized privacy norms while ensuring that

344 The FTC is led by five commissioners appointed by the president and confirmed by the Senate for seven-year terms. *Id.* at 608. "No more than three commissioners can be members of the same political party." *Id.* The president chooses one commissioner to act as chairperson. *Id.* There are currently two empty FTC commissioner seats; President-elect Donald Trump can appoint members of the Republican Party to fill those seats.

345 Current FTC Chairwoman Edith Ramirez's seven-year term ends in 2017. Ramirez began her service on the Commission in 2010. She was selected by President Obama to replace Jon Leibowitz as FTC Chairperson when Leibowitz stepped down in 2013. *See* Edward Wyatt, *White House Elevates a Commissioner to Chairwoman of the F.T.C.*, N.Y. TIMES (Feb. 28, 2013), http://www.nytimes.com/2013/03/01/business/obama-set-to-appoint-edith-ramirez-to-fill-top-ftc-post.html.

346 *See* Michael Kan, *Worries and Uncertainty Cloud Outlook for Digital Privacy Under President Trump*, CIO (Nov. 9, 2016), http://www.cio.com/article/3140182/security/worries-and-uncertainty-cloud-outlook-for-digital-privacy-under-president-trump.html (discussing concerns that Donald Trump's pro-business positions will strip away data security and data privacy regulations designed to protect consumers).

347 Divonne Smoyer & Aaron Lancaster, *Think the FTC Is the De Facto U.S. Data Protection Authority? State AGs May Have Something to Say*, PRIVACY PERSPS. (Dec. 12, 2013), https://iapp.org/news/a/think-the-ftc-is-the-de-facto-u-s-data-protection-authority-state-ags-may/.

348 HOOFNAGLE, *supra* note 2, at 66.

349 *Id.* at 73. In the 1960s, sharp disagreement among the five commissioners rendered its consumer protection mission ineffective. REPORT OF THE ABA COMM'N, *supra* note 340, at 891. During that period, the FTC endorsed the adoption of state UDAP laws. That history underscores the importance of attorneys general in the protection of consumer privacy.

350 *See* Mark Totten, *The Enforcers & the Great Recession*, 36 CARDOZO L. REV. 1611 (2015).

companies internalize some of the costs of data harms that would otherwise be borne by consumers alone.[351] State enforcers have engaged in a productive dialogue with federal enforcers, resulting in more comprehensive protection for consumers. They have been able to pursue privacy initiatives quickly because career staff do not have to worry about whether a majority of federal commissioners endorse their actions. Attorneys general should remain equal enforcement partners to federal agencies given their unique ability to leverage local knowledge and expertise quickly and efficiently.[352]

c. Preempting State Law

Should Congress adopt data protection legislation that supplants state laws? Whether preemptive federal laws should be adopted depends upon the specific protections afforded consumers and the concomitant gains in efficiency.[353] If a federal law would offer a strong level of protection or set a statutory floor that could be strengthened by state law, then the question is worth serious consideration.[354] Once a federal bill with a real chance of passage is proposed, its costs and benefits can be meaningfully explored.

The issue of federal preemption is often raised in the context of data-breach notification proposals.[355] The FTC has taken the position that "a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected."[356] The National Conference of State Legislatures[357] and forty-nine attorneys general support federal legislative proposals that would set a floor for breach notification but allow state lawmakers to layer on more restrictive rules.[358] Along these lines,

351 *See* Solove & Citron, *supra* note 332. If courts change their view of plaintiffs' privacy and data security cases or if the resources provided federal agencies become unlimited, a reassessment of this view would be in order.

352 *See* 115 CONG. REC. 1539 (1969) (remarks of Sen. Nelson) (criticizing the FTC for delaying investigations to protect industry).

353 *See* Schwartz, *Preemption and Privacy*, *supra* note 1 (providing a careful and thoughtful approach to efforts to preempt state privacy and security legislation).

354 *See, e.g.*, VOGEL, *supra* note 91, at 255 (noting that in the environmental arena, federal regulatory statutes set minimum standards that permit states to enact tougher standards).

355 *See, e.g.*, Data, Privacy & Sec. Practice Grp., *Federal Bills Pursue Comprehensive Data Breach Notification*, KING & SPALDING (Oct. 14, 2014), http://www.kslaw.com/imageserver/KSPublic/library/publication/ca101414.pdf; *see also* Jedidiah Bracey, *Are Multiple Mobile Privacy Guidelines Helping or Hurting the Mobile Ecosystem?*, IAPP (June 27, 2013), https://iapp.org/news/a/are-multiple-mobile-privacy-guidelines-helping-or-hurting-the-mobile-ecosys/.

356 Data, Privacy & Sec. Practice Grp., *supra* note 355.

357 *Id.*

358 Letter from State Att'ys Gen. to Cong. Leaders (July 7, 2015), http://www.ct.gov/ag/lib/ag/press_releases/2015/20150707_naag_data_breach_notification_letter.pdf.

Congress adopted health privacy and financial privacy laws that set a floor for breach notification, thus allowing states to adopt stricter requirements.[359]

In the absence of a preemptive federal data-breach notification law (or other such laws), state attorneys general should work to harmonize the patchwork of state laws, as California recently suggested.[360] Idaho AG Lawrence Wasden has urged state attorneys general to work together to identify the "best aspects" of data-breach laws and work to amend them so "that they are more homogenous."[361] The NAAG Privacy Working Group provides an effective forum for organizing such activity.[362] Attorneys general have proposed state privacy legislation modeled after another state's law.[363] Harmonization around security and privacy best practices is something career staff and attorneys general have emphasized as a goal, and it should be.

More broadly, calls for federal preemption are animated by concerns that AG enforcement will result in a one-way ratchet to stronger regulation. Upward regulatory creep could serve as a barrier to entry.[364] Companies like Microsoft, Facebook, Twitter, and Google have ample resources to pay for legal compliance, but smaller companies or startups may not. Consider a startup mobile app developer. As soon as the developer's app is offered in the iTunes store, consumers in all fifty states can download it. Will the developer be able to shoulder the expense of compliance with the privacy and data security rules in all of those states? Will the cost of compliance squeeze out upstarts like the developer? Not always. New businesses can outsource compliance to lawyers who specialize in helping startups with regulatory hurdles.[365] Alternatively, they might accept the risks associated with being mostly compliant or ignore the rules since law enforcers tend to focus on larger companies than smaller ones.[366]

Then too, it is important to recognize that the costs of stronger regulation are offset by its benefits. Improvements in data security mean less fraud and identity theft, which would reduce the negative externalities borne by

359 Relatedly, preemption attacks on state UDAP laws have been unsuccessful. Section 5 of the Federal Trade Commission Act does not preempt them. Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 989 n.41 (D.C. Cir. 1985).

360 *See* KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 2012–2015 (Feb. 2016), https://oag.ca.gov/breachreport2016. Other attorneys general emphatically agree with this point. *See, e.g.*, Zoeller Interview, *supra* note 200. Federal lawmakers have tried to pass a federal data-breach notification law since 2005 but with no success. *See* CITRON, *supra* note 170; *see also* Data, Privacy & Security Practice Grp., *supra* note 355, at 4 n.9. Gridlock has prevented federal legislation across the board.

361 Smoyer & Lah, *supra* note 256.

362 Cable Interview, *supra* note 59.

363 California legislation served as a model for Delaware Attorney General Matt Denn when he drafted the recently enacted student privacy bill and a law requiring privacy policies. Wright Interview, *supra* note 114.

364 Thanks to David Law for raising this concern with me.

365 Andrew Keane Woods, *Silicon Valley's Regulatory Lament*, LAWFARE BLOG (June 3, 2016, 2:55 PM), https://www.lawfareblog.com/silicon-valleys-regulatory-lament.

366 *Id.*

consumers, banks, payment processors, and merchants. Stronger privacy and data security protections would enhance consumers' trust in companies' products and services.[367] They would emulate certain aspects of the EU's data protection regime, thus encouraging cross-Atlantic commerce. Ultimately, however, if state privacy regulation becomes so complex and onerous and its costs far exceed its benefits, federal lawmakers should take seriously the question of a preemptive national data protection regime.

d. Capture Concerns

What about the opposite concern—that state attorneys general are vulnerable to influence designed to discourage privacy enforcement? Attorneys general are increasingly subject to aggressive lobbying.[368] In a prize-winning series of articles for *The New York Times*, Eric Lipton exposed troubling practices by lawyers and former attorneys general, including the "use [of] campaign contributions" and "personal appeals at lavish corporate-sponsored conferences," to push attorneys general "to drop investigations, change policies, negotiate favorable settlements or pressure federal regulators."[369]

Lobbying might explain why some attorneys general tread lightly when it comes to privacy or data security violations.[370] But even if some states fall

367 For an important work on trust and privacy, see Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. (forthcoming 2016).

368 Eric Lipton, *Lobbyists, Bearing Gifts, Pursue Attorneys General*, N.Y. TIMES (Oct. 28, 2014), http://www.nytimes.com/2014/10/29/us/lobbyists-bearing-gifts-pursue-attorneys-general.html?_r=0.

369 *Id.* Indeed, the point is particularly salient in the 2016 presidential election. *See* Steve Eder & Megan Twohey, *Donald Trump's Donation Is His Latest Brush with Campaign Fund Rules*, N.Y. TIMES (Sept. 6, 2016), http://www.nytimes.com/2016/09/07/us/politics/donald-trump-pam-bondi.html?_r=0. In 2013, Florida AG Pam Bondi's office was investigating Trump University for violating the state's UDAP law. While the investigation was ongoing, AG Bondi solicited Donald Trump for a campaign contribution, which his foundation arranged. After the donation was received, the Florida AG's Office dropped its investigation of Trump University. The donation (and a subsequent fundraiser held by Trump in AG Bondi's honor) has been subject to complaints about the corrupting influence of money in politics. *See* Sara Gonzales, *The Trump University Corruption Story Just Got Worse for Pam Bondi (and Donald Trump)*, REDSTATE (Sept. 7, 2016), http://www.redstate.com/saragonzales/2016/09/07/trump-university-corruption-story-just-got-worse-pam-bondi-trump/.

370 Attorneys general have complained about the politicization of the office and the emergence of the Democratic Attorneys General Association (DAGA) and the Republican Attorneys General Association (RAGA). *See Former Arkansas Attorney General and Former United States Senator Mark Pryor Visits Columbia Law School, Discuss the Politicization of the Office of State Attorney General*, COLUM. L. SCH.: NAT'L STATE ATT'YS GEN. PROGRAM (Apr. 29, 2015), https://web.law.columbia.edu/sites/default/files/microsites/attorneys-general/mark_pryor_-april_2015.mp3. DAGA was founded in 2002. *Democratic Attorneys General Association*, BALLOTPEDIA: ENCYCLOPEDIA AM. POL., https://ballotpedia.org/Democratic_Attorneys_General_Association (last visited Sept. 18, 2016). RAGA was founded in 1999. *See About RAGA*, RAGA, http://www.republicanags.com/about (last visited Sept. 18, 2016). Despite such politicization, attorneys general and staff have repeatedly emphasized that politics has

prey to influence peddling, other states will not. As Mark Totten has insightfully argued, while no individual state attorney general is resistant to capture, it is unlikely that all fifty attorneys general will succumb to the demands of lobbyists.[371]

Further militating against interest group capture is politics.[372] State attorneys general are an ambitious lot; many go on to higher office.[373] Many of the privacy leaders of the 1990s are now U.S. senators and governors.[374] Elected attorneys general further their careers with high-visibility investigations.[375] They win favor with constituents by pursuing consumer protection matters.[376]

As this study shows, influence peddling has not eliminated AG interest in privacy and data security issues. Attorneys general have investigated privacy violations of industry players from all sectors of the economy, including major credit-reporting agencies, retailers, technology companies, banks, hospitals, and insurance companies. When attorneys general have intervened, their enforcement activity has had important spillover effects.

The increasing level of lobbying of attorneys general is troubling, to be sure. It does "create[ ], at the minimum, the appearance of undue influence."[377] The problem could be partially addressed with more robust disclosure laws. But concerns about capture do not justify the removal of state attorneys general from the privacy enforcement calculus.

e. Dormant Commerce Clause

What about federalism concerns implicated by the dormant Commerce Clause? Does the array of state privacy and data security laws interfere with the integration of the nation into a single market and national polity? The dormant Commerce Clause is an implied restraint on state activity stemming from the Supreme Court's construction of the Commerce Clause.[378] Under the Court's jurisprudence, states may regulate interstate commerce unless a

played little role in the enforcement of data privacy and security matters. *See* Christopher R. Nolen, *State Attorneys General Offer Perspectives on Data Breaches*, LEXOLOGY (Dec. 15, 2015), http://www.lexology.com/library/detail.aspx?g=54a5a467-747b-4d85-ad1d-3fafade085b7 (stating that privacy and data security are on the agenda "whether it is the Republican Attorneys General Association, the Democratic Attorneys General Association or the National Attorneys General Association").

371 Totten, *supra* note 350, at 1658.

372 Lemos, *supra* note 94, at 721–22.

373 Provost, *supra* note 56, at 37.

374 Former New York AG Eliot Spitzer (1999–2007) went on to become governor in 2007; Connecticut AG Richard Blumenthal (1991–2011) was elected to the U.S. Senate in 2011; Michigan AG Jennifer Granholm (1999–2003) was elected to the U.S. Senate in 2003.

375 Devins & Prakash, *supra* note 21, at 2143, 2145.

376 *Id.* at 2145; *see also* Clayton, *supra* note 19; Provost, *supra* note 328, at 612.

377 Lipton, *supra* note 368.

378 Jason Lynch, Note, *Federalism, Separation of Powers, and the Role of State Attorneys General in Multistate Litigation*, 101 COLUM. L. REV. 1998, 2023 (2001).

state regulation "clearly discriminate[s] against interstate commerce" and is not "demonstrably justified by a valid factor unrelated to economic protectionism"[379] or "the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."[380]

Do state laws invoked by attorneys general in multistate and individual enforcement actions, notably state data-breach notification laws, violate those principles? To date, no court has struck down a state data-breach notification law on the basis of the dormant Commerce Clause analysis.[381]

As a start, breach notification laws would not violate the anti-discrimination principle.[382] The burden imposed on interstate commerce by data-breach notification laws arguably is not "clearly excessive" in relation to the benefits of those laws. Companies can readily identify the state citizens covered by the statutes and thus can provide notice according to each state's law.[383] The cost of compliance is not excessive in light of the benefits to consumers. The state interest in ensuring notification of data breaches is strong. Without notice, consumers would not know to monitor their credit for fraud; companies might be inclined to skimp on data security since breaches would cost them nothing if hidden from the public and regulators.[384] State data-breach notification laws fill an important gap. Federal

379 New Energy Co. of Ind. v. Limbach, 486 U.S. 269, 274 (1988).

380 Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

381 *See* Anthony Glosson, *California Lawmakers vs. the Dormant Commerce Clause*, ANTHONY GLOSSON BLOG (Feb. 13, 2014, 4:46 AM), http://anthonyglosson.com/california-lawmakers-vs-the-dormant-commerce-clause/.

382 Bilyana Petkova, who has written insightfully about privacy federalism, writes that the anti-discrimination approach is wise given that "[t]here is no way of knowing whether a state experiment is going to be successful without giving it time to unfold." Bilyana Petkova, *The Long-Term Promise of Privacy Federalism, Part I*, TECH. & MKTG. L. BLOG (Sept. 1, 2015), http://blog.ericgoldman.org/archives/2015/09/the-long-term-promise-of-privacy-federalism-part-1-guest-blog-post.htm.

383 The recently amended California data-breach notification law requires companies to disclose breaches involving login information. Anthony Glosson argues that "[b]ecause log-in information, by itself, provides no indication of a user's state of residence, the law forces websites either to post embarrassing breach notifications prominently to their own pages, or to collect *more* information in order to distinguish between California or non-California users." Glosson, *supra* note 381. That dormant Commerce Clause argument is worth close study given the potential burdens on companies and the possibility that consumers may be worse off if companies have to engage in re-identification to accomplish the statute's goals. Such study must acknowledge the important reason behind the amendment. Because consumers often use the same login information for different accounts, notice of a breach would nudge consumers to change their login information across the board, preventing fraud at other sites.

384 Donald G. Gifford presents a thoughtful separation of powers argument about multistate tobacco litigation in his book, SUING THE TOBACCO AND LEAD PIGMENT INDUSTRIES: GOVERNMENT LITIGATION AS PUBLIC HEALTH PRESCRIPTION (2010). As Gifford explains, the separation of powers inquiry does not apply to the state in its relationship with Congress. *See id.* Gifford argues that attorneys general become legislators when they invoke ill-defined common law doctrines to create a national regulatory regime in multistate settlements. *See id.* By contrast, in multistate privacy and security cases, attorneys general are

health and financial privacy laws require notice of breaches, but they only apply to certain data holders and certain types of health and financial data.

2. Tactics and Strategies

Attorneys general have successfully employed various tactics, including legislative efforts and persuasion campaigns. Other tactics, however, are worth close inspection.

a. Reimagining Informal Agreements

The norm-shaping efforts of attorneys general may not be as effective as they could be due to their overreliance on informal agreements known as AVCs. Under the typical AVC, violations amount to prima facie evidence of lawbreaking.[385] Violators incur no obligations, fines, or penalties unless the attorney general files a lawsuit on the substantive violation and wins. In other words, noncompliance can only be punished if offices file a formal complaint.

Companies favor AVCs with such terms because violations do not result in automatic penalties.[386] Many companies that agree to change their practices will do so, but some may not. AVCs drafted in this way will fail to generate the same fear and interest sparked by lawsuits and consent decrees because companies risk little when they ignore them. That violators have little to worry about if they break their promises undermines the privacy-norm entrepreneurship of attorneys general. Informal agreements can influence privacy and data security practices *if* they are taken seriously. If, however, AVCs are viewed as paper tigers, then they are virtually worthless. AVCs would be more influential if attorneys general brought suit in the wake of a violation.

All AVCs should employ strong terms. Attorneys general should insist that violations of agreements amount to lawbreaking. In Maryland and Iowa, violations of informal agreements warrant immediate penalty.[387] Multistate AVCs similarly provide that states have automatic authority to enforce or seek sanctions for violations of their terms.[388] That should be true of all AVCs. As Iowa Assistant Attorney General Nathan Blake explains, when informal agreements make clear that violations put the party into contempt and those agreements are widely available to the public, they can be as influential as consent decrees.[389]

---

applying state UDAP laws, other state statutes, or federal sectoral laws. There is no legislative usurpation where attorneys general are enforcing state and sometimes federal laws.

385 *See, e.g.*, Affinity Health Plan AVC, *supra* note 138 (stating that evidence of violation amounts to "*prima facie* proof of a violation of the applicable statutes").

386 Telephone Interview with Divonne Smoyer, Partner, Reed & Smith (July 6, 2015).

387 *See* Telephone Interview with Nathan Blake, Iowa Assistant Attorney Gen. (June 21, 2016) [hereinafter Blake Interview]; *see also* Ask.fm Settlement, *supra* note 88.

388 *See, e.g.*, PointRoll AVC, *supra* note 154.

389 Blake Interview, supra note 387.

Stronger terms should be coupled with careful compliance checks. Those checks should involve independent audits by third parties that report results directly to states.[390] States should impose strong sanctions if audits reveal non-compliance.[391] Stronger terms coupled with aggressive compliance would enhance the norm-setting potential of AVCs.[392]

Another aspect of informal agreements should be assessed: their transparency. AVCs can change practices and policy only if the public finds out about them. If AVCs are covered by non-disclosure agreements, they cannot educate the public. To be sure, there may be costs to proceeding publicly: trust between regulators and entities could be lost.[393] Career staff explained that some non-disclosure agreements engendered proactive compliance.[394] Concerns about trust should be considered, but with a thumb on the scale in favor of transparency.

Attorneys general should follow the lead of the FTC in not only publicizing agreements, but also frequently weaving them together to show the lessons of those agreements. After a number of consent decrees, the FTC often circles back in blog posts to discuss the significance of recent cases.[395] This can help educate the public, established businesses, and startup companies alike. This approach would reinforce the norm-setting work of state attorneys general.

b. Formal Adjudication

A broader critique relates to state enforcers' preference for informal agreements over formal adjudication. To be sure, there are states with active

390 Informal agreements sometimes secure opportunities for state oversight. Multistate AVCs often require that states be allowed to inspect privacy programs. *See, e.g.*, PointRoll AVC, *supra* note 154; *see also In re* Maloney Props., Inc., Civ. No. 12-112 (Mass. Sup. Ct. Mar. 21, 2012) (order granting assurance of discontinuance/assurance of voluntary compliance). Others require third-party audits but say nothing about reporting them to states. *See, e.g.*, Health Net AVC, *supra* note 226 (requiring a third-party audit by security professionals after the loss an of unencrypted hard drive with consumer data).

391 In the 1960s, the FTC was strongly criticized for its overreliance on informal agreements that had little bite and no oversight. REPORT OF THE ABA COMM'N, *supra* note 340. An ABA commission made recommendations along the lines I suggested above, and the FTC's current approach focuses on seeking cease and desist orders and filing formal actions. *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2.

392 State attorneys general should press for stronger civil penalties to make deterrence meaningful. In a case against a notorious spammer filed by the New York Attorney General's Office, the Office eventually settled for only $50,000 after promising to seek damages of over $20 million. The defendant laughingly admitted that the modest settlement wouldn't "change his business practices at all." Stacy Cowley, *N.Y. AG Settles with Self-Described 'Spam King'*, COMPUTERWORLD (July 23, 2004), http://www.computerworld.com/article/2566184/technology-law-regulation/n-y—ag-settles-with-self-described—spam-king-.html.

393 *See* Richards & Hartzog, *supra* note 367.

394 Ruckman Interview, *supra* note 41.

395 Lesley Fair, *Speaking of* Spokeo*: Part 3*, FTC BUS. BLOG (June 15, 2012, 11:02 AM), https://www.ftc.gov/news-events/blogs/business-blog/2012/06/speaking-spokeo-part-3.

privacy litigation dockets.[396] Some states display a preference for litigation over informal agreements.[397] But, as responses to FOIA requests show, the better part of state investigations end in informal agreements.

The preference for informal agreements has everything to do with the fact that states have limited resources. Within those constraints, state enforcers should consider the important role that formal adjudication plays. Pleadings and other litigation documents educate the public.[398] Complaints articulate a state's theory of why an entity's actions constitute an unfair or deceptive act or practice.

To the extent that states have resources, they ought to think about the expressive and coercive advantages of formal proceedings. The FTC's primary tool of enforcement is litigation, which usually ends in consent decrees. As Daniel Solove and Woodrow Hartzog have shown, those consent decrees are greeted with public fanfare and close inspection by regulated entities.[399]

To be sure, the FTC has been subject to criticism for its reliance on consent decrees. Critics have attacked the substance of those agreements, contending that they pay insufficient attention to cost-benefit analysis.[400] During his tenure, FTC Commissioner Joshua Wright argued that the agency needed to engage in more rigorous economic analysis in its section 5 cases.[401] In co-authored scholarship, then-Professor Wright argued that adjudications of private claims under state UDAP laws showed that those acts were not truly "Little-FTC Acts" because they failed to engage in rigorous cost-benefit analysis.[402]

---

396 Texas is the most actively engaged in individual enforcement activities. The FOIA response from the Texas Attorney General's Office produced eleven AVCs, seven settlement agreements, three judgments, and one ongoing case over the past five years. Two of the Office's cases proceeded through the stages of litigation. Texas has taken the lead in several multistate actions.

397 Some states eschew informal agreements (or AVCs) in favor of litigation. This is true of California's privacy cases. Based on the response to a FOIA request, in the past five years, the Attorney General's Office filed five lawsuits, all ending in settlement agreements; no AVCs were filed. Similarly, the FOIA response from Massachusetts indicated that the Attorney General's Office entered into two AVCs and seven consent judgments in the past five years. California and Massachusetts are actively involved in multistate investigations.

398 *See* CITRON, *supra* note 170 (exploring the powerful expressive role of law).

399 *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 2, at 607.

400 Berin Szoka, *Josh Wright's Unfinished Legacy: Reforming FTC Consumer Protection Enforcement*, TRUTH ON THE MKT. (Aug. 26, 2015), http://truthonthemarket.com/2015/08/26/josh-wrights-unfinished-legacy/.

401 *Id.* Commissioner Wright dissented from the agency's policy reports on Data Brokers and the Internet of Things on the grounds that they lacked economic analysis of the privacy issues. *Id.*

402 Henry N. Butler & Joshua D. Wright, *Are State Consumer Protection Acts Really Little-FTC Acts?*, 63 FLA. L. REV. 163 (2011) (finding that successful private suits under state UDAP laws would not have been successful under section 5, which does not allow private rights of action). Private claims assessed by Butler and Wright did not focus on privacy or data security issues. If they had, courts would have likely dismissed them on the grounds that plaintiffs failed to show cognizable harm. *See* Solove & Citron, *supra* note 332.

Yet, as Ryan Calo thoughtfully shows, privacy protections embedded in the FTC's privacy jurisprudence support market mechanisms.[403] The FTC's section 5 cases addressing inadequate data security and privacy violations stem from its attention to the market benefits of privacy and its engagement in cost-benefit analysis.[404] This accords with interviews with career staff and state attorneys general: cost-benefit analysis is crucial to state enforcers when considering whether to begin an investigation.[405] Both the market benefits of innovation and privacy should be considered, as it seems they are for federal and state enforcers.

c. Closing Letters

The FTC has issued closing letters, which explain why it has dropped an investigation. Closing letters explain why the agency thought a company's practices met the law's requirements. Attorneys general do not issue closing letters or advisory opinions on privacy and data security issues, but should they? Might a closing letter or advisory opinion signal and solidify norms by identifying activity that falls within the bounds of the law?

Career staff have expressed skepticism about the idea. Of advisory opinions, Massachusetts Assistant AG Sara Cable remarked:

> It could put the AG in a tight spot if [it] put out an advisory opinion and it goes stale. The office could put out an opinion and then come to realize it did not have a full grasp on things. The landscape shifts so quickly. Also, there may be a disincentive to do an advisory opinion because it could weaken the office's enforcement posture.[406]

State attorneys general and career staff might understand their legislative advocacy as akin to closing letters or rulemakings. Recent legislation, from bans on employer access to employees' social media to limits on the use of student data for marketing, addresses practices that are unfair and deceptive. Typically, violations of those laws constitute per se violations of UDAP laws. If understood in that light, state attorneys general might reconsider the usefulness of closing letters or advisory opinions.

d. Thicker Norms and Blind Spots

State attorneys general should continue to press for thicker privacy norms to address emerging challenges. As pressures mount to ensure that U.S. data practices are adequate in the eyes of European authorities, state

403 *See* Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649 (2015).

404 *See id.*

405 *See, e.g.*, Cable Interview, *supra* note 59; Fitzsimmons Interview, *supra* note 5; Kriger Interview, *supra* note 38. To be sure, when UDAP laws do not have an explicit harm requirement, offices have more flexibility to think about cases where the privacy harm is more intangible but no less real. Cable Interview, *supra* note 59; Kriger Interview, *supra* note 38.

406 Cable Interview, *supra* note 59.

enforcers should continue to work on areas of convergence to enhance trust and facilitate trade.

State enforcers should continue to address new frontiers for privacy protection. There are shadowy data practices in need of oversight. Certain uses of Big Data should be on the agendas of state attorneys general. For instance, behavioral-scoring algorithms rate consumers' likelihood to engage in risk-taking activities, to underperform on the job, or to develop mental illnesses.[407] Some of those uses of Big Data may fall outside the domain of FCRA or anti-discrimination laws.[408] Attorneys general should investigate unfair and deceptive uses of scoring algorithms given their potential to further marginalize vulnerable populations. Because use restrictions are hotly contested, the FTC's privacy jurisprudence has not addressed them. Attorneys general should continue their role as pioneers to curtail certain uses of scoring products.[409]

The data brokerage industry similarly deserves the scrutiny of state enforcers. Data brokers "amass digital dossiers on individuals that include incomplete and misleading data, selling them to potential employers," insurers, and landlords.[410] In most instances, consumers have no idea that such dossiers have cost them crucial opportunities. Individuals have no leverage to force data brokers to disclose or correct those dossiers. Former FTC Commissioner Julie Brill pressed attorneys general to investigate data brokers under FCRA and state UDAP laws.[411] Attorneys general can go further than the procedural protections of FCRA. Relying on state UDAP laws, state attorneys general should seek stronger restrictions on the data brokerage industry.

Last, there are stalking cellphone apps whose entire enterprise is arguably illegal.[412] Once installed on someone's phone, stalking apps secretly track everything someone does with a cellphone and upload the activity to a

407 Citron & Pasquale, *supra* note 159, at 2–6; *see* Sam Pfeifle, *How Big Data Discriminates*, IAPP (June 24, 2014), https://iapp.org/news/a/how-big-data-discriminates/ (discussing concerns created by systems using data and algorithms to include and exclude people from opportunities, and discussing Citron and Pasquale's *The Scored Society*, *supra* note 159). For troubling uses of scoring products in the criminal justice system, see Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks.*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

408 *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

409 There are offices interested in investigating such practices though their work has yet to be publicly revealed.

410 Citron, *Mainstreaming*, *supra* note 333, at 1816; *see* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 240, 266 n.131 (2007).

411 Paul Bond & Christine Nielsen Czuprynski, *Commissioner Brill to States: Data Brokers Aren't Going to Regulate Themselves*, REEDSMITH: TECH. L. DISPATCH (Apr. 18, 2013), http://www.technologylawdispatch.com/2013/04/privacy-data-protection/commissioner-brill-to-states-data-brokers-arent-going-to-regulate-themselves/.

412 Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243, 1246–48 (2015).

site that stalkers can watch in real time.[413] In previous work, I have called upon state attorneys general to seek civil penalties and injunctive relief against spyware and stalking app providers under state UDAP and wiretap laws.[414] Attorneys general should devote efforts to updating state wiretap laws to ensure the illegality of the sale of apps designed to secretly intercept communications.[415]

These are but a few examples of blind spots: privacy-invasive practices that have largely been ignored by enforcers. As this study shows, state attorneys general have been pioneers. They have a variety of tools to forge thicker privacy norms and to address blind spots. As a group, they have more resources than federal agencies.[416] They should harness their collective power to tackle these problems and to press for thicker protections.

Conclusion

State attorneys general have played a critical role in U.S. privacy law, which until now has received scant appreciation and study. Much as Justice Louis Brandeis imagined states as laboratories of the law, offices of state attorneys general have been laboratories of privacy enforcement. Attorneys general have used their broad legal authority and unique local knowledge to address gaps in the law. They have established baseline privacy protections and paved new frontiers for privacy practices. In areas where federal agencies have valuable technical and policy expertise but less manpower, AG offices have been crucial enforcement partners, harmonizing federal norms. AG privacy policymaking will be even more important if federal agencies slow down consumer privacy and data security efforts.

Looking forward, state attorneys general should harness their collective power to press for thicker data protections. They should act more boldly in the face of uses of Big Data and scoring algorithms that disadvantage the vulnerable. This Article hopefully marks the beginning of a more sustained conversation about the privacy policymaking of state attorneys general and the future directions that it can take.

---

413 *Id.*

414 *See id.*

415 *Id.* at 1274–77 (arguing that state wiretapping laws should be updated to cover the sale and manufacturer of stalking apps and suggesting legislative language to update the law).

416 Indeed, the entire budget of the FTC is less than the California AG's Office. For instance, in 2015, the FTC requested $293 million for its entire budget. Fed. Trade Comm'n, Fiscal Year 2015 Congressional Budget Justification 35 (2014), https://www.ftc.gov/system/files/documents/reports/fy-2015-congressional-budget-justification/2015-cbj.pdf. The budget for the California Department of Justice, led by AG Harris, was more than $741 million in 2012. *Attorney General of California*, Ballotpedia, https://ballotpedia.org/Attorney_General_of_California (last visited Feb. 1, 2016).

APPENDIX I: SAMPLE FOIA REQUEST LETTER

Dear FOIA Coordinator:

Under [specific state open records law], I am requesting an opportunity to inspect or obtain information regarding the Attorney General's efforts related to the collection, use, storage, and/or disclosure of consumers' personal data.

For the purpose of this request, the phrase "collection, use, storage, and/or disclosure of consumers' personal data" encompasses various issues, including but not limited to data breaches; data security; data-breach notification; spyware; spam; robocalls or unwanted telephone calls; facial recognition software; privacy policies; sale of consumer data; collection or use of consumers' personal data without notice and/or consent; and the like.

(1) Please provide copies of all pre-investigatory letters your office sent to an entity or person regarding the collection, use, storage, and/or disclosure of consumers' personal data covering the period of 2010 to the present.

(2) Please provide copies of all assurances of voluntary compliance (or assurances of voluntary discontinuance) your office entered into with an entity or person regarding the collection, use, storage, and/or disclosure of consumers' personal data covering the period of 2010 to the present.

(3) Please provide copies of all litigation-related documents (including but not limited to pleadings and settlements) your office filed or entered into with an entity or person regarding the collection, use, storage, and/or disclosure of consumers' personal data covering the period of 2010 to the present.

(4) Please provide copies of all assurances of voluntary compliance (or assurances of voluntary discontinuance) or consent decrees/settlements related to multistate investigations regarding the collection, use, storage, and/or disclosure of consumers' personal data covering the period of 2010 to the present.

(5) Please provide copies of all documents, including best practice guides, issued by your office in which the office gives advice to companies or consumers regarding the collection, use, storage, and/or disclosure of consumers' personal data covering the period of 2010 to the present.

(6) Please provide copies of all documents related to your office's efforts to propose, lobby for, or support state or federal legislation related to the collection, use, storage, and/or disclosure of consumers' personal data covering the period of 2010 to the present.

If there are any fees for searching or compiling this information, please inform me in advance. However, I would like to request a waiver of all fees because the disclosure of the requested information is in the public interest, is made in connection with a scholarly project, and will contribute significantly to the public's understanding of your state's interest in consumer protection. My scholarship focuses on information privacy law. This request is made in connection with research focusing on the privacy policymaking of state attorneys general. This information is not being sought for commercial purposes.

Thank you for considering and responding to this request. I look forward to hearing from you. Your open records law requires a response within [ ] business days. If my request will take longer, please contact me with information about when I might expect copies or the ability to inspect the records.

If you deny any or all of these records, please cite each specific exemption you feel justifies the refusal to release the information requested and notify me of your appeal procedures under the law. I can be reached at [e-mail address] or [cell phone number].

APPENDIX II: FOIA REQUEST AND INTERVIEW DATA

State	FOIA Request	Interview
AL	Denied (Noncitizen)	
AK	Yes	
AZ	Yes	Yes (Staff)
AR	Denied (Noncitizen)	
CA	Yes	Yes (AG/Staff)
COL	Yes	
CT	Yes	Yes (AG/Staff)
DE	Yes	Yes (Staff)
FL	Yes	
GA	Yes	
GU	Yes	
HI	Yes	
ID	Yes	
IL	Yes	Yes (Staff)
IN	Yes	Yes (AG)
IA	Yes	Yes (Staff)
KS	Yes	
KY	Yes	
LA	Yes	
MA	Yes	Yes (Staff)
ME	Yes	Yes (Staff)
MD	Yes	Yes (AG/Staff)
MI	Yes	
MN	Yes	
MS	Yes	
MO	Yes	
MT	$263.79 fee	
NE	$4255.76 fee	
NV	Yes	
NH	Yes	
NJ	No	
NM	Yes	
NY	Yes	Yes (Staff)
NC	Yes	
ND	Yes	
MP	No	
OH	Yes	Yes (Staff)

APPENDIX II (CONT'D)

OK	Yes	
OR	Yes	
PA	Yes	
PR	No	
RI	Yes	
SC	Yes	
SD	No	
TN	Denied (Noncitizen)	
TX	Yes	
UT	Yes	
VT	Yes	Yes (Staff)
VI	No	
VA	Denied (Noncitizen)	
WA	Yes	Yes (Staff)
WV	Yes	
WI	Yes	
WY	Yes	
DC	Yes	