The Way Forward on Data Privacy and Data Security

January 28, 2022

Attorney General Phillip J. Weiser

As Colorado's Attorney General, I have focused on the importance of protecting consumers and, in particular, safeguarding their private information. This means that our Department takes our role in implementing and enforcing our data security and data privacy laws seriously. It also means that we worked closely and effectively with the General Assembly on establishing these protections—specifically with Senator Rodriguez and Representative Carver who were here with us today and sponsored the Colorado Privacy Act. Because of our groundbreaking work in this space, Colorado became the third state (after California and Virginia) to establish a comprehensive set of privacy protections. That's a big deal.

Today, we once again gather on Data Privacy Day to celebrate our commitment to this work and engage our community on how we can best protect data privacy and data security. This year, moreover, we are able to discuss our plans for implementing the Colorado Privacy Act as well as to provide guidance on how companies can best comply with our data security requirements. Most of all, however, we are here to learn and build relationships that can help us advance this important work.

The States as Laboratories of Democracy

Not long after I started as Colorado's Attorney General, I made clear that addressing consumer privacy and data security issues would be a priority for me and my Department. In remarks I gave in April 2019, I discussed nation's tradition of protecting data privacy that goes back to the Privacy Act of 1974.[1] That law recognized the importance of protecting personally identifiable information (PII). It set forth a set of Fair Information Practice Principles, or FIPPs. Notably, a linchpin of that law is to "provide notice to the individual regarding its collection, use, dissemination, and maintenance of" PII.[2] Despite the enactment of this law almost 50 years ago, the United States, at least at the federal level, has yet to develop any comprehensive data privacy protection regime, acting merely to protect private information (and PII) for specific sectors, such as health care data.[3]

---

[1] Colorado Attorney General's Office, *Data is King: U.S. Privacy Developments and Implications for Global Markets and Technology Development* (April 10, 2019), available at https://coag.gov/app/uploads/2019/04/Privacy-Speech-Remarks.pdf.

[2]For a discussion of FIPPs, and their origin, see U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum on The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 29, 2008), available at https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[3] See, for example, the Health Insurance Portability and Accountability Act, or HIPAA. Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, § 264, 110 Stat.1936.

Even though the United States developed the concept of FIPPs, the European Union has taken the concept more seriously, developing a regulatory regime based on them.[4] The United States' lag is not due to a lack of trying, however. Over a decade ago, I worked for President Obama when he called on Congress to take action in this area, proposing a "Privacy Bill of Rights" concept.[5] Unfortunately, Congress has yet to act on this call, despite increasing evidence that threats to consumer privacy—including the unknowing sale of consumer data by data brokers and others—is a cause for concern.[6]

In Colorado, we are blessed to have a collaborative culture and an ability to work together to solve problems. The sponsors of the Colorado Privacy Act are tremendous examples of this style of leadership. I've noted throughout my service as Attorney General that there is a stark contrast between how we approach public policy problem solving in Colorado and the ongoing gridlock at the federal level. In contrast with the federal government, we in Colorado work hard on substantive issues, listen to different points of view, work to craft thoughtful solutions, and develop approaches that are legally sound and can be enforced effectively.[7]

The failure of the federal government to act to protect data privacy is also true for the area of data security. At the federal level, President Obama proposed a comprehensive model for protecting data security in 2011.[8] In that proposal, President Obama called on Congress to adopt a national standard for data breaches. Even back then, almost every state had enacted such a law.[9] Unfortunately, Congress has yet to act in this area, leaving companies with a patchwork of standards to follow.

When I reflected on the state of federal inaction on data privacy and security three years ago, I called the state of play a "second best solution."[10] The first best solution, I explained, would

---

[4]comprehensive basis, has acted to develop privacy protections by enforcing commitments in company data privacy policies. For a discussion of the development and enforcement of this model, see Philip J. Weiser, *Entrepreneurial Administration*, 97 B.U. L. Rev. 2011 (2017), available at https://scholar.law.colorado.edu/articles/838.

[5]. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[6] Brooke Auxier, et al., *Americans and Privacy, Pew Research Center* (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[7] For a discussion of this point, see the following letter addressed to the Colorado General Assembly Colorado Attorney General's Office, *Senate Bill 19-078 ("Concerning the Protection of the Open Internet")*, (March 28, 2019), available at https://coag.gov/app/uploads/2020/09/AGO_SB_19_078_net-neutrality-Letter.pdf.

[8] The White House, *The Administration Unveils its Cybersecurity Legislative Proposal*, (May 12, 2011) available at https://obamawhitehouse.archives.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal.

[9] IT Governance USA, *Data Breach Notification Laws by State*, https://www.itgovernanceusa.com/data-breach-notification-laws

[10]As I said in my address:

> I am the first to recognize that the actions by states to address data privacy and security matters is what economists would call "a second best solution." A first best solution would be a comprehensive federal law that protected consumer privacy. Such a law, like the Dodd-Frank law, should authorize State AGs to protect consumers. When Congress starts working on such a law, I will be eager and willing to support

be national leadership by Congress that empowers states to act withing a framework of cooperative federalism. We are not in that world, however, and we must move to adopt second best solutions, meaning that the responsible step to take is to support state leadership to protect consumers. The alternative, unfortunately, is no protection at all.

The Colorado Privacy Act

The Colorado Privacy Act sets forth a set of broad rights for consumers and authorizes our Department to engage in rulemaking and enforcement. We take that responsibility very seriously. Our Chief Deputy Natalie Hanlon Leh leads an Impact Team, which brings together those charged with enforcing this law, along with lawyers who advise our state agency clients on data privacy and data security matters and technologists who protect data that we collect here at the Department of Law. As we proceed to develop rules under this Act, we will do so thoughtfully, carefully, and with the engagement of this team—and external stakeholders. We recently added additional experienced privacy and data security lawyers to our team to help us carryout this important mission.

With respect to our rulemaking process, let me begin by acknowledging just a few big picture issues we will need to work through. For starters, the law makes plain that consumers deserve the right to access and control the use of their data. In short, consumers have a right to know what information companies collect about them and how that information will be used, enabling them to reject the sale and use of their private data by third parties. As discussed during the legislative discussions, the process of consumer notice and approval or rejection of data sharing needs to be conducted fairly, free from what some have called "dark patterns," which can unfairly mislead consumers on this issue. We recognize that California is adopting rules on this topic, and we will need to look at this issue as well. We also recognize that we will need to consider what the process will be for consumers to engage and learn about their data profiles as well as to correct inaccurate data. Finally, the Colorado law's vision of company auditing and data protection assessment procedures is another area where we might well want to provide guidance.

Given the importance and complexity of the rulemaking ahead of us, we have a two-step process in mind. First, we want to hear from you. Before we begin drafting rules, we want to fully understand the concerns and needs of Coloradoan's and Colorado businesses. We envision this process will include a series of high-level conversations at meetings and townhalls. Our goal is to explore what privacy protections in Colorado should look like and what important privacy issues most merit our attention. If you would like to be a part of this process, you will soon be able sign up on the Office of the Attorney General's website to receive notifications about upcoming events.

Over the next few months, we look forward to hearing from Colorado consumers, businesses, and other stakeholders. During this time, we will post a series of topics for informal

---

such an effort. When Congress starts working on such a law, I will be eager and willing to support such an effort. After all, differing laws and reporting requirements designed to protect privacy creates a range of challenges for companies and those working to comply with different—and not necessarily consistent—laws.

Full remarks available at: https://coag.gov/app/uploads/2019/04/Privacy-Speech-Remarks.pdf.

input on our website and solicit responses in writing and at scheduled events. This will help us engage in a more focused dialogue, consider diverse perspectives, and address issues. By this fall, we will post a formal *Notice of Proposed Rulemaking*, which will include a proposed set of model rules. This will kick off a process of collecting verbal and written comments about the proposed rules and how they would operate from a range of stakeholders and other interested persons across Colorado. With the benefit of the time we have under the Act, and Colorado's collaborative culture, we expect to be in a position to adopt final rules around a year from now.[11]

Protecting Data Security

We recognize that effective data privacy also includes attention to data security, and that data protection cannot depend on consumer action alone. Entities should protect consumer privacy by limiting their collection of personal data to only that which is necessary, securing the data that they do collect and ensuring any vendors that access the data also secure it, holding such data only as long as needed, and securely disposing of data that is no longer useful. The Colorado Privacy Act incorporates these key principles by including controller duties of data minimization and care and imposing data security obligations on both data controllers and processors. Colorado's data security statutes and enforcement actions also separately emphasize the importance of data security.

In the absence of federal leadership, all fifty states, Washington D.C., Guam, Puerto Rico, and the Virgin Islands enacted laws that address how companies protect data that they collect and store.[12] In Colorado, we adopted a number of data security statutes that require covered entities that maintain personal and/or personally identifying information to take reasonable steps to protect that information, to dispose of it when it is no longer needed, and to promptly notify Colorado residents when their information is at risk of being misused by unauthorized third parties. Our Department has authority to enforce these laws. Over the last several years, we have taken action various enforcement actions. In the Kozleski case, for example, we executed an Assurance of Discontinuance (Assurance) with the Kozleski CPA firm after it failed to take action to investigate a ransomware attack the potentially involved data breaches and notify victims and our office in a timely fashion.[13] Then, in the Impact Mobile Home Communities (MHC) case, we executed an Assurance that provides critical guidance on what companies should do to follow reasonable data security standards, detect and respond to data incidents, including conducting a prompt, good faith investigation and providing timely notice.[14] With respect to reasonable security standards (including data disposal standards), we expect companies, at a minimum, to have a policy that ensures that sensitive data is not stored for unnecessarily long periods of time and via insecure systems. For that reason, we took action against SEMA Construction, concluding that its

[11] C.R.S. § 6-1-1313(2) (2023) (requiring the Attorney General to pass rules regarding a global opt-out mechanism by July 1, 2023).
[12] National Conference of State Legislatures, *Security Breach Notification Laws*, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[13] Kozleski CPAs Assurance of Discontinuance, https://coag.gov/app/uploads/2022/01/2020.06.08-KozleskiAssuranceAgreement06082020.pdf.
[14] Impact Mobile Home Communities Assurance of Discontinuance, https://coag.gov/app/uploads/2021/06/AOD-Signed-Impact-MHC-and-Colorado-6.11.2021.pdf.

employees had stored personal information, such as Social Security numbers, financial information, and driver's license numbers, in employee email accounts for as long as 20 years—and then failed to notify those affected by a data breach on account of a phishing attack for over two years after the attacks began.[15]

In addition to its requirement to promptly notify Colorado residents when their information is at risk of being misused by unauthorized third parties, Colorado's data security laws require companies to take reasonable steps to protect personally identifiable information and to dispose of it when it is no longer needed.[16] Over the last few years, we have heard from companies and others asking for guidance on what this requirement means. Our answer remains that this standard is a flexible one and calls for case-by-case determinations. A small company of a few employees that serves ice cream, for example, need not follow the same approach as a major provider of health care services that collects and stores sensitive information. Nonetheless, we have provided important guidance in the recent actions noted above that will inform how we make enforcement determinations.

For those looking for a few rules of the road, let me outline some of the important best practices that we will weigh in making decision on whether companies are acting reasonably to safeguard sensitive information. First, we will evaluate whether a company has identified the types of data it collects and has established a system for how storing and managing that data—including ensuring regularly disposing of data it no longer needs. Second, we will consider whether a company has a written information security policy. For companies that have no such policies, or have ones that are outdated or exist only in theory with no attempt to train employees or comply with the policy, we will view more skeptically claims that their conduct is reasonable. To take an obvious example, entities that collect credit card information are expected to protect that information in accordance with the Payment Card Industry's Data Security Standard and any failure to do so will be evidence of a lack of appropriate care. Third, a closely related expectation to keeping a written data security policy is the expectation that companies adopt a written data incident response plan. By developing and implementing such a plan, companies will be better positioned to take remedial action and notify consumers and our Department in a timely way that consumer data was shared inappropriately with third parties. Few valid reasons exist for failure to timely provide notice and we have made this easier for companies by setting up an online data breach reporting tool on coag.gov.[17] Fourth, in recognition of the reality that networks are interconnected, another critical requirement is that entities are more vulnerable to cyberattacks stemming from cybercriminals' unauthorized access to vendor networks. In the famous case of the Target data breach, for example, it was Target's decision to provide an irresponsible vendor with access to its customer data that gave rise to the loss of data involving 70 million customers.[18]

---

[15] SEMA Construction Assurance of Discontinuance, https://coag.gov/app/uploads/2021/11/SEMA-Construction-Fully-Executed-Assurance-of-Discontinuance.pdf.
[16] C.R.S. §§ 6-1-713, 713.5, 716; §§ 24-73-101, 102, 103.
[17] Office of the Attorney General, *Data Protection Laws*, https://coag.gov/resources/data-protection-laws/
[18] Congressional Research Service, The Target and Other Financial Data Breaches (February 4, 2015), https://crsreports.congress.gov/product/pdf/R/R43496/7#:~:text=On%20January%2010%2C%202014%2C%20Targ

Finally, I wanted to acknowledge that the data security threats that companies face are serious and merit constant vigilance. On the ransomware front, as we recognized over the past year, companies are vulnerable and need to take action to protect their employees and customers. Last summer, we issued guidance that can protect against such attacks, referencing prior guidance from the federal government.[19] The federal guidance sets forth a few key steps of sound data security practice:

- Adopt multifactor authentication;
- Use endpoint detection (to look for malicious activity on the network);
- Respond and address any malicious activity detected on the network;
- Encrypt sensitive data (so that data, if stolen, cannot be used); and
- Utilize a skilled, empowered security team (to patch rapidly, and share and incorporate threat information into company defenses).[20]

Following the guidance set out above is not only smart practice to guard against ransomware attacks, but also is relevant to establishing reasonable data security practices. In addition to the above practices, the guidance we issued last summer also calls on companies to:

- Backup your data, system images, and configurations, regularly test them, and keep the backups offline;
- Update and patch systems promptly;
- Test your incident response plan;
- Check your security team's work; and
- Segment your networks.[21]

The above practices are not only sound ways to protect data and avoid ransomware attacks, but also serve as relevant evidence that a company is following reasonable data security practices as required by Colorado law. We recently expanded on this guidance when we released our Data Security Best Practices Guidance this week, providing guidance on how to adopt information security and incident response policies, train your employees to prevent and respond to cybersecurity attacks, notify our department in a timely matter, and other topics.[22]

Conclusion

---

et%20announced%20that%20personal,missed%20opportunities%20to%20prevent%20the%20data%20breach.%20Target.

[19] Office of the Attorney General, A*ttorney General Phil Weiser joins fellow AGs in alerting businesses and government entities to take prompt action to protect operations and personal information*, (July 29, 2021) https://coag.gov/press-releases/7-29-21-2/.

[20] The White House, *What We Urge You To Do To Protect Against The Threat of Ransomware* (June 2, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf.

[21] Colorado Attorney General's Office, *Attorney General Phil Weiser joins fellow AGs in alerting businesses and government entities to take prompt action to protect operations and personal information* (July 29, 2021) https://coag.gov/press-releases/7-29-21-2/.

[22] Available at: https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf

Let me conclude by discussing Colorado's collaborative problem-solving culture. The work to enact the Colorado Privacy Act, the approach we are taking to the upcoming rulemaking, and our implementation of Colorado's data security laws all reflect our commitment to collaboration. Similarly, the conversations at our annual data privacy conference are important not only as a way to disseminate key information—such as that set out in my remarks—but also because they provide our team with an opportunity to learn. To that end, the interdisciplinary structure of our Data Privacy and Security Impact Team, which works to ensure that our enforcement efforts are informed by real world challenges, reflects our commitment to continuous learning and improvement.

The importance of developing new cultural norms in this area will be felt by companies, non-profit entities, governmental organizations, and others.[23] As we all appreciate, managing data is a challenge that all entities need to take seriously. And protecting sensitive information is not something that companies can ignore, allow to be compromised by irresponsible vendors, or put into a policy that can be ignored and not advanced through comprehensive training and an incident response plan. As evidenced by our guidance above, we take seriously our role to help drive this important culture change. Or, as I said at an earlier Data Privacy Day, our goal is to promote Mad Eye Moody as an inspiration for the principle of constant vigilance and to guard against any check the box thinking in this area.[24]

Finally, I appreciate that we are holding this conference in conjunction with our partners at the Wyoming Attorney General's Office. Attorney General Hill and I have worked together on consumer protection efforts as well as on the Attorney General Alliance's Ginsburg-Scalia Initiative.[25] This collaboration is a natural extension of that work as well as an opportunity for Colorado to learn more about the work of Wyoming in the cryptocurrency area. As the states act on the cutting edge of technology policy development, whether as to data privacy, data security, or cryptocurrency, it is important that we do so with a spirit of humility, intellectual curiosity, and collaboration.

---

[23] For a thoughtful discussion of the culture change around the adoption of Chief Privacy Officers by companies, see Bamberger, Kenneth A. and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, Stanford Law Review 63 (2011): 247, http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2011/01/Bamberger-Mulligan-63-Stan-L-Rev-247.pdf.

[24] Colorado Attorney General's Office, *Prepared Remarks: Conference on Data Privacy and Cybersecurity Compliance Toolkit for Small Businesses at the Colorado Department of Law* (Jan. 28, 2020), https://coag.gov/blog-post/prepared-remarks-conference-on-data-privacy-and-cybersecurity-compliance-toolkit-for-small-businesses-at-the-colorado-department-of-law-jan-28-2020/.

[25] https://coag.gov/press-releases/5-11-21; Colorado Attorney General's Office, *The Ginsburg/Scalia Initiative* (August 13, 2021) https://coag.gov/blog-post/the-ginsburg-scalia-initiative-8-13-21/.