NEWS RELEASE

CONTACT: Lawrence Pacheco, Director of Communications
(720) 508-6553 office | (720) 245-4689 cell
Email: Lawrence.pacheco@coag.gov

FOR IMMEDIATE RELEASE

Prepared Remarks of Attorney General Phil Weiser
Closing Keynote Address
Data is King: U.S. Privacy Developments and Implications
for Global Markets and Technology Development
FCBA-IAPP
April 10, 2019

Thank you to the Federal Communications Bar Association (FCBA) and the International Association of Privacy Professionals (IAPP), for hosting us here today at the Cable Center. It is truly an honor to be here. I am excited to talk to you about US privacy developments and the implications for global markets and technology development.

In recent years, the digital economy has transformed our society, powered by internet platforms that collect and analyze massive amounts of data. Facebook, Google, Amazon, Netflix, Microsoft, and Uber are among the most powerful companies in the world because of the data that they collect, process, and control. And they are far from alone: in today's tech economy, personal data is an increasingly valuable commodity for all companies.

Consumer data can be stored, analyzed, and shared in lots of different ways. For companies storing this data, there are risks related to how they may use this data as well as risks related to how others may obtain this data (namely, through hacking). For both state and federal policymakers, the challenge is to protect the privacy of consumers and to allow the responsible and innovative use of personal information to support and provide new or enhanced products and services. In short, we need to develop an adaptive framework that can both facilitate and oversee emerging technologies as well as build confidence on behalf of consumers that they will be protected.

In my talk today, I want to touch on three fronts. First, how did we get to where we are on data privacy? Second, what are the best steps for addressing these challenges? Third, how can state attorneys general play a role in developing and enforcing an appropriate data privacy framework?

"How Did We Get Here"?

As advancements in technology and application development have grown over the past three decades, the collection and processing of personal data has taken off. Simply put, today's digital economy collects amounts of data on all of us that, even three decades ago, would have seemed impossible to imagine. In today's economy, every time we search for a term, hail a ride-sharing ride, or binge watch another series, we are sharing important – and valuable – information about ourselves.

On its face, the data itself is generally innocuous. Who doesn't like *Stranger Things*? But even one data point may reveal more than we might imagine.[1] Moreover, one piece of data might be combined with other data points, analyzed, and used to make predictive judgments. This is not new. Famously, in 2012, we learned —as one headline provocatively put it—"How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did."[2]

Because data is so valuable, a new international industry of organized cybercriminals has emerged, finding ways to steal valuable data. One form of data that is uniquely vulnerable is health care information. As one commenter put it:

> the theft and sale of our health records on the black market [is] a thriving business with "dark web" online stores that don't look much different from an Amazon marketplace. In fact, there were nine times more medical than financial records breached in 2016 — 27 million — representing nearly 10% of the U.S. population.[3]

Unfortunately, even as these technological shifts have altered vast parts of our daily lives, the public policy response remains tentative and tepid, to say the least.

The United States has a rich history in developing privacy regulations, starting with the concept of Fair Information Practice Principles, or FIPPs. These principles date back to the Privacy Act of 1974 and were designed to be technology-agnostic. They provide for a set of requirements as to how personally identifiable information (PII) is treated, starting with the commitment to "provide notice to the individual regarding its collection, use, dissemination, and maintenance of" PII.[4]

Despite developing the generic concept of FIPPs, the United States has largely developed privacy protections only in a sectoral fashion, passing laws that specifically protect certain categories of data. Consider, for example, the Health Insurance Portability and Accountability Act, or HIPAA, which provides privacy protections for health care data. In the face of this gap, the Federal Trade Commission (FTC) has encouraged all entities who collect data to develop privacy policies. Using its authority under the Federal Trade Commission Act to address unfair trade practices, the agency has policed the collection and use of data to ensure that entities honor the commitments made in their privacy policies.[5]

Ironically, the regulatory body that built most on FIPPs and developed a comprehensive regulatory regime governing privacy was the European Union. In 2002, the European Parliament issued its ePrivacy

---

[1] For one discussion of this concept, *see* Paul Ohm & Scott Peppet, *What if Everything Reveals Everything?*, in Big Data is Not a Monolith (Cassidy Sugimoto, Michael Mattioli, and Hamid Ekbia), (2016), *The MIT Press.*

[2] Kashmir Hill. *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, (February 16, 2012), *Forbes*, *available at https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#668709ae6668.*

[3] Robert Lord. *The Real Threat Of Identity Theft Is In Your Medical Records, Not Credit Cards*, (December 15, 2017), *Forbes*, *available at https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/#1bea22061b59.*

[4] For a discussion of FIPPs, and their origin, see *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.

[5] For a discussion of the development and enforcement of this approach, see Philip J. Weiser, *Entrepreneurial Administration*, 97 B.U. L. Rev. 2011 (2017), *available at* https://scholar.law.colorado.edu/articles/838.

Directive ("the Directive"). This Directive addressed concerns related to the processing of personal data and the protection of privacy in the electronic communications sector. It also set out rules on how providers of electronic communication services, such as telecom companies and Internet Service Providers, should manage their subscribers' data.[6] In particular, it set out requirements in seven key areas of protection: confidentiality of communications, security of networks and services, data breach notifications, traffic and location data, spam, public directories, and calling-line identification.[7]

When I worked for President Obama, I worked with a technology policy team that developed a more comprehensive approach towards information privacy. In particular, we undertook to develop a broader base of privacy protections for American consumers in the form of a Consumer Privacy Bill of Rights. In proposing such a model, President Obama stated:

> … it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times.
>
> One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.[8]

In the face of a lack of action on this initiative, the Federal Communications Commission set forth its own principles on privacy for broadband consumers, modelling it on the concept of a Consumer Privacy Bill of Rights.[9] The essence of the FCC's rules was to give consumers greater control over what internet service providers can do with their data. In particular, under these rules, consumers would need to provide an affirmative "opt-in" consent before companies could collect and share sensitive consumer information, including geo-location, financial/health data, and browsing history.

The FCC rules were hotly contested. One significant criticism was that they covered only a segment of the Internet ecosystem, the ISPs. Another criticism was that the rules were overbroad. In 2017, using the Congressional Review Act, Congress repealed the FCC rules before they could ever go into effect.

What Do We Do Now?

To any reasonable observer, it is clear that we have failed to develop a robust and comprehensive regulatory regime around information privacy. It is the lack of such federal regulatory oversight that has left a gap for states like California to adopt the California Consumer Privacy Act, which, among other things, provides consumers with a right to know what data is being collected about them, a right to veto

---

[6] *EU Directive 95/46*: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31, *available at* https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive.

[7] Id.

[8] *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.

[9] *FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency, and Security for their Personal Data*, (October 27, 2016), *available at* https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.

the sale of their personal data, and a right to access their data.[10] This law is set to go into effect next January. Other states, including Colorado, have passed laws governing data privacy and security as well.

The need for federal legislation is becoming more and more self-evident, leading Facebook CEO Mark Zuckerberg to call for comprehensive privacy legislation along the lines envisioned by President Obama and adopted in Europe (and California). In a recent op-ed on this topic, Zuckerberg said:

> [E]ffective privacy and data protection needs a globally harmonized framework. People around the world have called for comprehensive privacy regulation in line with the European Union's General Data Protection Regulation (GDPR), and I agree. I believe it would be good for the Internet if more countries adopted regulation such as GDPR as a common framework.
>
> New privacy regulation in the United States and around the world should build on the protections GDPR provides. It should protect your right to choose how your information is used — while enabling companies to use information for safety purposes and to provide services.
>
> As lawmakers adopt new privacy regulations, I hope they can help answer some of the questions GDPR leaves open. We need clear rules on when information can be used to serve the public interest and how it should apply to new technologies such as artificial intelligence.[11]

While Federal privacy regulation would be the ideal solution, the partisan nature of national politics might make that impossible.

In a range of areas, from privacy to net neutrality, we are seeing States act as laboratories of democracy, developing solutions to challenges not being addressed in Washington, D.C. Just recently, Colorado passed a law on net neutrality in the face of the FCC's radical step to strip away all such protections. My statement on that issue applies in this context, too:

> Until Congress is able to function appropriately, we can take some encouragement from the fact that the States, including their executive and legislative branches, are demonstrating the capacity to advance effective policy solutions. They are working hard on substantive issues, listening to different points of view, crafting thoughtful solutions, and developing approaches that are legally sound and can be enforced effectively. Senate Bill 19-078 is one important example of leadership by the States. By crafting such approaches in Colorado, we can both protect our citizens and provide a model for how our federal government should operate—and hopefully will once again. Until then, I look forward to working on state level public policy to make our government work for people and address important issues—like net neutrality—that protect consumers and enable innovation.[12]

---

[10] *A.B. 375, Title 1.81.5, The California Consumer Privacy Act of 2018, CCPA*, (Cal. 2017), *available at* https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf.

[11] Mark Zuckerberg. *The Internet needs new rules. Let's start in these four areas*, (Mar. 30, 2019), *Washington Post*, *available at* https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.e7b19c54c651.

[12] Philip J. Weiser. *Letter to Colorado General Assembly RE: Senate Bill 19-078* ("*Concerning the Protection of the Open Internet*"), (March 28, 2019), a*vailable at* https://www.coag.gov/sites/default/files/contentuploads/ca/ago_sb_19_078_net_neutrality_letter.pdf.

It is worth noting that, in today's world, both States and other international bodies are taking action in the face of inaction by our federal government. In the case of data privacy, the General Data Protection Regulation (GDPR) referenced by Mark Zuckerberg looms large. This law went into effect last year and provides comprehensive protections, including (1) the right to access your data; (2) the right to correct inaccurate data; (3) the right to erasure (or the right to be forgotten); (4) the right to restrict processing of your data; and (5) the right to data portability.[13] It is fair to say that companies, including international ones that operate in Europe, are still working to comply with the requirements of GDPR.

So What Do We Do Now?

Given the challenges we face, I don't believe that States—and State AGs in particular—can wait until our federal government develops comprehensive privacy protections. As I have explained elsewhere, I believe that states (and federal agencies where able) should lead through entrepreneurial administration.[14] That is indeed what States are now doing.

Take, for example, the issues around data security. At last count, at least 24 states have enacted laws that address data security practices of government entities and private companies. Most of them require businesses that own, license, or maintain PII to implement and maintain "reasonable security procedures and practices," which is consistent with Colorado's own Data Protection Law. In particular, Colorado's HB-1128 requires notification to the Attorney General within 30 days of a data breach and sets out rules for storage and disposal of PII as well as requires companies to have a written disposal policy for both electronic and physical documents that contain PII.[15]

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 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.

In today's second-best world, I believe that States have an obligation to move forward. We should do so with a recognition that we need to collaborate with one another and develop approaches that recognize the challenges around compliance. We can use your help and engagement and we work towards just this end.

---

[13] *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, *available at* https://gdpr-info.eu.

[14] Philip J. Weiser, *Entrepreneurial Administration*, 97 B.U. L. Rev. 2011 (2017), *available at* https://scholar.law.colorado.edu/articles/838.

[15] *Colorado House Bill 18-1128 - Concerning Strengthening Protections for Consumer Data Privacy*, (Colo. 2018), a*vailable at* https://leg.colorado.gov/sites/default/files/2018a_1128_signed.pdf.

Conclusion

Together, we have important work to do to create greater data privacy and security. Public policymakers at both the federal and state level need to be engaged to protect consumers and create rules for our digital economy that allow responsible businesses to thrive. I believe that we in Colorado will play an important part in such efforts and I look forward to working with you.

Thank you for your engagement and I look forward to your thoughts and questions.