#DataPrivacySummit

OUTCOMES REPORT

DATA PRIVACY SUMMIT

MARCH 27, 2019 , WASHINGTON, D.C.

BROUGHT TO YOU BY accessnow

accessnow

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For more information about the summit or this report, please contact: Eric Null (eric@accessnow.org), Jennifer Brody (jennifer@accessnow.org), and Isedua Oribhabor (isedua@accessnow.org)

Access Now thanks the following sponsors for their support of the Data Privacy Summit: Apple, Microsoft, Mapbox, Google, Internet Society, AT&T, and Dropbox.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

DATA PRIVACY SUMMIT

The Data Privacy Summit was a full-day event organized by Access Now at the Eaton Hotel (1201 K Street NW) in Washington, D.C. to examine online data practices and the need for new, strong data protection policy in the United States. This event brought together privacy experts across different fields for an interactive dialogue to map the current data protection and privacy debate, identify where consensus exists, and narrow existing questions where more clarity is needed, all toward the ultimate goal of achieving a comprehensive, rights-respecting data protection framework in the United States.

Below are takeaways from the conference and next steps for 2020:

1. **Past is prologue: notice-and-consent has failed, and we should not repeat this failure.**
2. **Privacy protections implicate a variety of interests, and Congress should seek to understand all those interests, with particular regard for marginalized communities.**
3. **The U.S. must move beyond notice-and-consent to enact privacy protections that place the primary onus for safeguarding privacy on companies, not individuals.**
4. **There is some agreement on the substance of privacy legislation, but significant disagreements continue to exist.**
5. **Workable solutions will require a deeper understanding of data protection standards and policy.**
6. **Passing a poorly crafted bill in haste would do more harm than good.**

THE NEED FOR DATA PROTECTION IN THE UNITED STATES

Across the United States, the topic of privacy and data protection is more prominent than ever. Following from the scandals around Facebook and Cambridge Analytica to the passage and implementation of the California Consumer Privacy Act to Maine's Act to Protect the Privacy of Online Consumer Information,[1] there have been increasingly sophisticated discussions of the benefits and challenges of the virtually unfettered collection and use of data in the U.S. But we don't yet know how U.S. lawmakers will respond at the national level.

The U.S. does not have a federal privacy law. Instead, regulators have embraced a sectoral approach to privacy, meaning there is a patchwork of laws that give Americans limited protections for certain types of data, like health or student data. But there is no blanket, or comprehensive, protection against unchecked data collection, misuse, manipulation, or abuse. Unfortunately, the lack of a comprehensive law has led to repeated privacy violations, catastrophic data breaches, and little or no recourse for users.

In fact, the only federal limitation on what many companies can do with personal data is the Federal Trade Commission (FTC) Act's prohibition on "unfair and deceptive trade practices," as enforced by the agency. Most privacy enforcements stem from the "deceptive" prong of the FTC Act, which essentially prohibits companies from lying about their privacy practices. The "unfair" prong is seldom used as a privacy enforcement mechanism.

Not only is the FTC's authority inadequate, so are its resources. The FTC conducts investigations and enters into consent decrees with entities believed to have violated this prohibition, but they are not very effective. Facebook was subject to a consent decree dating back to 2011,[2] and it did little if anything to prevent the Cambridge Analytica misuse of data.[3] The FTC's July 2019 consent decree and $5 billion fine against Facebook was based largely on that 2011 consent decree, which was the only reason the FTC could seek monetary damages.

The Cambridge Analytica scandal highlights many of the problems with the U.S. approach. We generally have very little understanding regarding the amount of data that companies like Facebook collect about us, let alone understanding the profiles they create or inferences they make from that data. Further, these companies are under little obligation to provide meaningful information about whether and how our profiles are purchased, analyzed, or transmitted. Terms of service/use are often long, complicated, and at the same time, provide little useful detail. Many companies have a lengthy, impenetrable "privacy" policy with provisions that let them share undefined personal information with undisclosed "third parties," including "vendors" and/or "business partners." With little enforcement or repercussions for harmful corporate practices, bad actors like Cambridge Analytica can easily exploit the loopholes. The current regime has led to an environment in which companies routinely take advantage of individuals. In short, the status quo in the U.S. does not protect people, and, as such, it is not sustainable.

In this ecosystem, members of Congress have been introducing or reviving data protection proposals. Some of these proposals are regressive and may only serve to further entrench the prevailing business model that rewards unchecked data collection and exploitation in the dark. Others are a solid starting point for a conversation about what is necessary to provide the data protection people in the U.S. and around the world desperately need.

1. Gilbert, F. (2019, June 10). Maine Follows California Lead: Prohibits ISP Use, Sale, Disclosure of Online Consumer Information Without Prior Affirmative Consent. Retrieved from https://www.natlawreview.com/article/maine-follows-california-lead-prohibits-isp-use-sale-disclosure-online-consumer
2. Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises. (2019, February 28). Retrieved from https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
3. Access Now Policy Team. (2018, March 21). It's not a bug, it's a feature: How Cambridge Analytica demonstrates the desperate need for data protection. Retrieved from https://www.accessnow.org/its-not-a-bug-its-a-feature-how-cambridge-analytica-demonstrates-the-desperate-need-for-data-protection/

THE DATA PRIVACY SUMMIT

Organized by Access Now, the Data Privacy Summit provided a forum to consider the current debates around a U.S. federal data privacy law, with the goal of surfacing areas of agreement and identifying where more research will be necessary. The conference brought together experts in the space with a variety of thoughts and opinions about what a federal law should look like. However, across the board, speakers appeared to agree it was time for Congress to take action and pass such a law. The event featured four panels, four lightning talks, and three keynotes presentations, summarized below.

THE HISTORY AND FOUNDATIONS OF DATA PRIVACY

Moderator: Meg Leta Jones (Assistant Professor, Georgetown University)

Speakers: Susan Lyon Hintze (Founder and Managing Partner, Hintze Law), Jasmine McNealy (Assistant Professor, College of Journalism and Communications at the University of Florida), Harriet Pearson (Partner, Hogan Lovells), Jules Polonetsky (CEO, Future of Privacy Forum)

Stories from the past several decades of privacy conversations helped set the stage for the day's conversations. Speakers described the transition of data privacy from a "tech story" to a "front page story" and noted that the growing number of professionals working on privacy issues signals a maturation of the field and demonstrates that it is an issue that people increasingly understand and care about.

Participants credited the implementation of data privacy laws in the European Union — both the Data Protection Directive (DPD) and its successor, the General Data Protection Regulation (GDPR) — as a spur and guiding force for conversations in the U.S. With its comparatively large penalties for violations of the law, they observed, the GDPR is a more powerful tool for enforcement than the tools under the current U.S. regime, and has likely helped push the U.S. discussion forward.

The trajectory of the "notice-and-consent" framework was also a major topic. Speakers observed that this framework no longer functions to give individuals a "yes or no" option; instead it forces them to "take it or leave it."

Speakers also examined the impact of privacy decisions on traditionally marginalized communities, discussing the impact and privacy harms for these communities and the political power that some groups lack to ensure their interests adequately represented. The panel concluded by noting considerations to keep in mind moving forward, including the need for more resources at the FTC and space for additional watchdogs and investigations.

MAPPING THE ONLINE DATA ECOSYSTEM

Moderator: Andrea Peterson (Investigator, Project on Government Oversight)

Speakers: Afua Bruce (Director of Technology, New America's Public Interest Technology program), Lea Kissner (Chief Privacy Officer, Humu), Stephanie Nguyen (Designer + Researcher, Fellow, Center for Public Leadership at Harvard Kennedy School), Maurice Turner (Senior Technologist, Center for Democracy and Technology)

This session explored the interaction between people and technology, including the identity of different actors in the ecosystem, how people exercise choice, and how services provide transparency. Speakers discussed the nature of privacy, and how its perception may change from person to person and across cultures and geographies, and in particular how "privacy" means something different to a person than it does to a business entity. They noted that conversations about privacy have to be broad and include people from a range of different backgrounds, and communication regarding privacy has to be honest and contextual.

Speakers also discussed the dynamic in interactions about data collection, including how the benefits of giving access to personal information are immediate, while any harm may be delayed or not directly perceived. They identified the potential for tension between decisions to expand data sharing arrangements and those to respect privacy, and a need to ensure that those values are well-balanced. The conversation concluded with speaker musings about how to become proactively respectful, identifying options including adoption of baseline privacy legislation and better alignment of privacy actions and business interests.

FEDERAL PREEMPTION V. STATE INNOVATION

Moderator: Peter Swire (Holder Chair of Law & Ethics, Georgia Tech Scheller College of Business; Senior Counsel, Alston & Bird LLP)

Speakers: Ian Adams (AVP of Government Affairs, R Street Institute), Ariel Fox Johnson (Senior Counsel, Policy & Privacy, Common Sense Media), Katie McInnis (Policy Counsel, Consumer Reports), Kate Tummarello (Policy Analyst, Engine)

A debate about federal preemption of state data privacy laws highlighted the potential for tension between state legislation and market certainty. Among those in favor of preemption, speakers underscored the high cost of compliance with a patchwork of state laws, particularly for new companies. Those opposing preemption noted the historical role states have had as defenders of privacy. While some speakers emphasized the need for states to react quickly to new and emerging threats to privacy, citing the slow pace of Congress in passing federal laws, others argued that FTC rulemaking could partially compensate for that. As the discussion came to an end, speakers raised another contentious issue: whether to establish a private right of action for privacy violations, a right that has been memorialized in the California Consumer Privacy Act and requires a level of care.

CHALLENGES AND OPPORTUNITIES IN LEGISLATION

Moderator: Cameron Kerry (Ann R. and Andrew H. Tisch Distinguished Visiting Fellow - Governance Studies, Center for Technology Innovation, The Brookings Institution)

Speakers: Kendall C. Burman (Cybersecurity & Data Privacy Counsel, Mayer Brown), Ted Dean (Head of Public Policy, Dropbox), Marshall Erwin (Senior Director of Trust & Security, Mozilla Corporation), Francella Ochillo (Vice President of Policy & General Counsel, National Hispanic Media Coalition)

The final session of the day was a holistic discussion exploring the potential for a new federal privacy law. Speakers identified several issues that new federal legislation would likely address, including limitations on collection of data, restrictions on data processing, and the proper role and level of transparency. There was a call for more research on exactly how data are weaponized, and a discussion on how privacy tools today are hard to find and use, and are therefore used by very few people.

Speakers also argued that the threat that privacy legislation may pose to the economy is likely overstated, and that there are a number of ways to create incentives to protect data. As the session concluded, participants returned to a discussion of the interaction between state and federal privacy laws. One suggested that a single federal law will not fix all of the problems raised, and that the issue will need to be re-examined as tech evolves. Another panelist suggested that enacting additional comprehensive state laws may make a federal standard harder to achieve.

AT-RISK POPULATIONS, CYBERSECURITY, AND THE INTERNATIONAL ENVIRONMENT

Speakers: Cindy Southworth (Executive Vice President, National Network to End Domestic Violence), David Brody (Counsel and Senior Fellow for Privacy and Technology, Lawyers' Committee for Civil Rights Under Law), Gaurav Laroia (Policy Counsel, Free Press), Andrea Limbago (Chief Social Scientist, Virtu), Estelle Massé (Senior Policy Analyst and Global Data Protection Lead, Access Now)

In a series of lightning talks, participants discussed vulnerable populations, cybersecurity, and the global landscape. They underscored that at-risk populations are disparately impacted by harmful data harvesting practices.

Cindy Southworth delivered a compelling speech that illustrated how perpetrators of domestic violence exploit the lack of data privacy protections to harass, stalk, and further harm victims. David Brody pointed out that vulnerable groups need more robust data privacy protections, given that when civil rights laws were written, the internet had yet to be invented, and lawmakers could not foresee the rise of so-called surveillance capitalism[4] and its uniquely pernicious effects on marginalized communities. These talks served to highlight the fact that U.S. laws are not sufficient to protect those most at-risk given the rapid development of surveillance technologies that prioritize profit over people.

Andrea Limbago argued that data privacy and technological innovation are not mutually exclusive; rather, privacy is a catalyst for innovation. She added that along with along with spurring innovation, investment in data privacy protections would bring enhanced security.

4. Zuboff, S. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs.

Estelle Massé explained that nearly a year after the implementation of the GDPR, individuals were more aware of the GDPR's protections and had taken steps to benefit from these protections. Notably, there was a 60% increase in the number of complaints filed with Data Protection Authorities compared to the year before the GDPR came into effect. She explained that the GDPR has a rights-based, user-centered approach that is already demonstrating a positive impact on the economy due to an increase in the number of privacy-focused companies.

VISIONS FOR DATA PRIVACY

Speakers: Malka Older (Author, Humanitarian Worker, and PhD candidate), Representative Ted Lieu (U.S.Congressman, D-CA-33), Rohit Chopra (Commissioner at the FTC), and Amie Stepanovich (former U.S. Policy Manager at Access Now)

Finally, three keynote presentations offered visions of a future for data privacy in the U.S.

Malka Older, author of a series of science fiction novels, described the dystopian future we could see if we continue on the path of enabling privileged control of the information ecosystem. She noted that the notion of "privacy" is contextual and regional; therefore, she argued, it is of utmost importance for the social sciences to inform the design of meaningful "privacy protocols."

Representative Ted Lieu lamented the fact that the U.S. Congress lacks technological expertise. He observed that "tech" is no longer a niche policy area, as it is the underlying component of everything that touches our lives. Lieu called on companies to provide greater transparency on their data collection practices and spoke in favor of giving individuals the right to erase data collected about them.

Rohit Chopra, in conversation with Amie Stepanovich, said there is a need for stronger enforcement mechanisms and consequences for data privacy violations. He cautioned against broad federal preemption of state laws, and agreed that it is important for the voices of marginalized communities to be heard to ensure greater equity and inclusion in crafting data privacy policy.

MAJOR TAKEAWAYS AND NEXT STEPS

The Data Privacy Summit surfaced insight on the state of the debate on federal privacy protections in the U.S. As Access Now continues to monitor privacy-related developments, including the introduction of multiple draft bills for data privacy from both houses of Congress, we offer our takeaways from the summit and consider the next steps.

1.Past is prologue: notice-and-consent has failed, and we should not repeat this failure.

Lawmakers in the U.S. have historically framed privacy as a "consumer protection" issue, a company-centric lens that views people as purchasing machines, rather than framing it as a rights-based issue, a lens that centers people and their rights. This has hindered the development of robust, human rights-respecting data protection policy; the individual is the object, not the subject. The framing of people as mere "consumers" arguably led to the FTC taking primacy in the U.S. regulatory landscape in the mid-1990s through its "unfair and deceptive trade practices" authority under the FTC Act.[5] We should not repeat that mistake. Our approach to privacy must evolve, putting those at risk at the center.

2. Privacy protections implicate a variety of interests, and Congress should seek to understand all those interests, with particular regard for marginalized communities.

There is no shortage of corporate lobbying on privacy in Congress, at both the state and federal level. But other voices must be heard. Congress must seek out voices that are not traditionally represented, especially members of marginalized communities, including through organizations representing affected constituencies. Seeking a broader array of input can help Congress understand how the current regime is failing to protect vulnerable communities and identify improvements that are necessary to protect these communities against harmful, intrusive, and unwanted privacy violations. Significant work has already gone into educating Congress on this issue, through the efforts of organizations such as Color of Change, MediaJustice, Lawyers Committee for Civil Rights Under Law, Free Press, and others. But more work remains.

3. The U.S. must move beyond notice-and-consent to enact privacy protections that place the primary onus for safeguarding privacy on companies, not individuals.

The notice-and-consent privacy regime in the U.S., prevailing for the past 20 years, has shown to be an abject failure. While it may have made sense in the nascent days of the commercial internet, today it is absurd to expect people to read and understand hundreds or even thousands of pages of "Terms of Service" and "Privacy Policy" agreements that are written in complicated legalese. The onus for protecting privacy must be placed on companies and governments. Shifting responsibility may result in privacy laws that alter business models and drive innovation to reflect changing incentives.

5. U.S. Federal Trade Commission 1995 Annual Report, at 13-14. (1995, September 30). Retrieved from https://www.ftc.gov/sites/default/files/documents/reports_annual/annual-report-1995/ar1995_0.pdf ("The goal of the Consumer Protection Mission is to maintain a well-functioning marketplace that allows consumers to make informed purchase choices. Today's marketplace, however, is increasingly complex.... Evolving technologies are radically changing the way consumers learn about, buy, and pay for goods and services.... Today [consumers] are increasingly concerned with ... the potential loss of personal privacy resulting from greater use of on-line communication...").

4. There is some agreement on the substance of privacy legislation, but significant disagreements remain.

Participants at our summit appeared to agree that the U.S. needs a federal data privacy law, but there remains a general lack of consensus on the substantive rights to include in such a law, how much rulemaking authority to give to the FTC, and whether to include a preemption provision or a private right of action. For an example of the disagreements that continue to exist, compare the draft bills by Democrat and Republican members of the Senate Commerce Committee[6] and the bracketed sections of the House Energy and Commerce bill, which indicate areas where the parties could not agree.[7] It is imperative to iron out these disagreements if we hope to reach a rights-respecting federal data protection solution.

5. Workable solutions will require a deeper understanding of data protection standards and policy.

To help resolve some of those disagreements, it is incumbent on stakeholders to deepen their research and information gathering on data protection. As we pivot from privacy principles to crafting legislative language, we must ensure that language is grounded in a thorough understanding of the issues at stake.

For instance, it is evident that the principle of data minimization is a misunderstood issue. Many of the current drafts for data protection legislation include language to allow companies to continue collecting whatever data they like for advertising purposes, which would maintain the harmful status quo. Further, industry stakeholders have historically argued against including a private right of action, but there is already such a right in California's CCPA, providing a starting point for understanding the impact and determining whether and how to adopt and improve upon it. Some widely adopted policies, like notice-and-consent, provide only illusory protection, and should be understood as such. Without more education on these and other key issues, lawmakers risk passing a comprehensive privacy law that would either cement the status quo, or worse, further weaken our already weak protections.

6. Passing a poorly crafted bill in haste would do more harm than good.

A comprehensive, user-centered data privacy framework must contain robust protections for Americans' privacy and data protection, in particular for individuals most at risk of exploitation and abuse. While momentum is building to pass federal laws on this issue, pushing through a sub-par bill for the sake of "seizing the moment" is not worth the long-term damage that poorly crafted legislation would do.

6. Consumer Online Privacy Rights Act. (2019, November 26). Retrieved from https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf; United States Consumer Data Privacy Act of 2019 (staff discussion draft). (2019, November 27). Retrieved from https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf
7. House Energy and Commerce Committee Circulates Draft Privacy Bill Expanding FTC Authority. (2019, December 19). Retrieved from https://www.insideprivacy.com/united-states/congress/house-energy-and-commerce-committee-circulates-draft-privacy-bill-expanding-ftc-authority/

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.