March 2021

Rebuilding Trust in the Digital Ecosystem: New Mechanisms for Accountability

International Digital Accountability Council and GMF Digital

A patchwork of privacy laws globally and the lack of baseline protections in the United States undermines users' trust in the digital ecosystem and limits the transformative potential of technology. Rebuilding trust requires big changes at both levels.

Congress must pass a federal privacy law coupled with nimble implementation measures that can move at the speed of the Internet. Privacy legislation should provide for accountability mechanisms that go beyond traditional law enforcement. Independent watchdogs can play an important role in monitoring privacy practices and enforcing codes of conduct. Additionally, those offering digital products and services need an advanced understanding of privacy rules. Education and certification programs can ensure they adhere to these effectively and consistently. Independent watchdogs could help inform the curriculum.

Internationally, differing legal frameworks for privacy rules must be interoperable to ensure that personal data remains protected when transferred across borders. An enforceable code of conduct that fulfills the requirements of privacy laws in multiple jurisdictions could support interoperability.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

Introduction

The open nature of the Internet has allowed it to flourish, giving billions of people access to information and connecting us in ways that had never before been possible in human history. This free flow of information has enabled digital technologies to transform economies and societies, but it has also created unique governance challenges. As digital technologies have dramatically affected every aspect of our lives—from the economy to health-care system to education to romantic relationships—governments have struggled to implement rules that enable the growth of digital innovation while protecting consumers, users, and democratic institutions.

Increasingly, the patchwork of governance structures and accountability mechanisms seem outmatched by the challenges that emerge from the digital landscape. Cybersecurity threats leave governments, businesses, and users vulnerable to the abuses of malicious third parties, some of whom are connected to governments. Online disinformation has pushed democratic institutions worldwide to a breaking point. And lack of trust in data privacy threatens to undermine the transformative promise digital technologies offer for commerce, health care, entertainment, and education.

The largest economies have taken differing approaches to commercial data privacy, reflecting competing philosophies. The approach in the European Union, codified through the landmark General Data Protection Regulation (GDPR), differs considerably from the orientation in the United States, which has a patchwork of state- and sector-specific laws but lacks baseline protections. Emerging economic giants such as Brazil, China, and India have each taken different paths toward digital privacy. The net result of this lack of harmonization is governance gaps that leave users exposed to considerable privacy risks.

The result of this global patchwork system is a lack of trust. Eighty-one percent of Americans say that they have very little or no control over the data that companies collect about them and 79 percent that they are concerned about how companies use their personal data.[1] This lack of trust emerges from an ecosystem bedeviled by myriad risks and harms. As the Cambridge Analytica scandal demonstrated, violations of best practices in consumer data privacy can have a profound effect on democratic discourse. The recent examples of a fertility app surreptitiously transmitting user data to unseen third parties affect vulnerable users in a deeply intimate way, further eroding trust.[2]

Lack of trust in the digital ecosystem can undermine the transformative possibilities the digital revolution creates for improving people's lives. One survey found that over half of Americans do not use a product or service due to concerns for their privacy.[3] If users do not trust apps with sensitive health data, they will not enroll in digitally enabled public health programs meant to contain the global coronavirus pandemic.[4] People may be more reluctant to download their health data in connection with innovative programs like Blue Button,[5] which makes it easier for patients and their doctors to unleash the potential of health data to personalize their care. Parents may not want their children to use distance-learning apps that can enable learning during a pandemic and hold the possibility of dramatically improving the efficacy of teaching and learning by tailoring pedagogy to the needs of individual learners.[6] In the commercial space, it is easy to see how fundamental trust is to online retail, digital entertainment, and increasingly data-rich homes and businesses.

1 Brook Auxier et. al, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, November 15, 2019.

2 Tonya Riley, "A Popular Fertility App Shared Data Without User Consent, Researchers Say," The Washington Post, August 20, 2020.

3 Andrew Perrin, Half of Americans have decided not to use a product or service because of privacy concerns Pew Research Center, April 14, 2020.

4 International Digital Accountability Council (IDAC), "Privacy in the Age of COVID: An IDAC Investigation of COVID-19 Apps," 2020.

5 The Office of the National Coordinator for Health Information Technology (ONC), "Blue Button," April 8, 2019.

6 IDAC, "Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic," 2020.

Rebuilding trust in the digital ecosystem requires big changes. The next section lays out some models for reform, including past efforts at updating U.S. privacy rules. The following section lays out the critical elements of a path forward on commercial data privacy. The need for federal baseline privacy legislation is clear, and this brief describes the necessary contours of such a law, but there are other critical elements for effective reform.

Perhaps most importantly, any effort to improve data privacy will require robust, systematic accountability mechanisms that go beyond the traditional tools of law enforcement. This is not to denigrate the work of regulators and enforcement bodies such as European data protection authorities, the U.S. Federal Trade Commission, and U.S. state attorneys general and their counterparts around the world. But the vast majority of risks and harms endured by Internet users are not significant enough to attract the attention of law enforcement and regulators. In some cases, academics, journalists, and civil society groups have done valuable work in calling out misbehavior, but most privacy and security shortcomings go undetected and unresolved. There is an important role for independent watchdog organizations to play in monitoring privacy practices and enforcing codes of conduct.

Additionally, it is maddeningly difficult for developers and publishers to know what the relevant rules are. Even diligent, well-trained publishers seeking in good faith to follow the rules will quickly find murkiness, gaps, and inconsistencies. Addressing this challenge requires not just updating privacy rules but also providing education and certification programs to ensure that developers, publishers, and third parties understand what the rules require.

Finally, as the United States advances its domestic privacy framework, its privacy rules must be interoperable with the analogous rules of its trading partners. Lack of interoperability can create significant roadblocks to international commerce and dialogue with key foreign trading partners will help ensure that personal data remains private when it is transferred across borders.

Models for Reform in the United States

As the Internet matures, a new roadmap for privacy is needed in the United States and around the world. Internet governance is different in important ways from that in other areas because of the complexity, time scale, and global nature of the subject matter. From a practical standpoint, it is difficult for legislators to have a firm enough grasp of the technical subject matter to enable a thoughtful debate on nuanced rules. Internet governance has tended to work best when technologists have a seat at the table specific rules are being ironed out. One solution to this kind of problem is to have the legislature pass broad rules and then delegate regulatory authority to an expert agency. However, traditional notice-and-comment rulemaking often fails to move at the speed of the Internet. The global nature of the Internet also makes it difficult for a single sovereign entity to regulate activity that is often global in scale and effect.

In 2012, President Barack Obama's White House put forward a framework for protecting privacy and promoting innovation in the global digital economy, proposing that the Congress pass baseline privacy legislation centered around the concept of a Consumer Privacy Bill of Rights.[7] Central to this approach were strong consumer protections, multi-stakeholder collaboration, and meaningfully enforceable codes of conduct. This initiative by the executive branch led to the introduction by Senator Patrick Leahy of the Consumer Privacy Bill of Rights in 2017. Although the bill did not ultimately pass, the Obama administration framework played a significant role in framing the conversation around U.S. privacy policy.

The 34 countries in the Organization for Economic Cooperation and Development (OECD), along with Colombia, Costa Rica, Egypt, and Lithuania, have set forth governance principles that succinctly articulate some of the best practices for regulating the Internet, including ensuring the free flow of information and

7 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.

protecting human rights while pursuing domestic policy goals.[8] These principles are largely consistent with the approach laid out in the Consumer Privacy Bill of Rights. The OECD Principles for Internet Policy Making represent an important step toward international agreement and any U.S. regulatory regime should incorporate them in order to promote a globalized Internet.

In the United States, individual states have led on legislative action on privacy since 2012, particularly with the California Consumer Privacy Act of 2018. The law affords California residents rights to control their personal data, including the right to know what personal data is collected about them and the ability to request the deletion of that data.[9] Last November, the state built on this approach with the passage of the California Privacy Rights Act. The proliferation of state-level privacy laws has increased the complexity of the patchwork system in the United States while leaving many Americans unprotected. The need for federal baseline privacy legislation remains urgent.

More recent federal efforts in the United States have foundered. In 2018, Representative Ro Khanna proposed an Internet Bill of Rights, which sought to provide consumers with more control over their personal data and articulated user rights, such as the right to be fully informed of the scope of personal data usage.[10] That same year, the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act articulated consumer rights as well as more robust accountability and enforcement mechanisms to be managed by the Federal Trade Commission and state attorneys general.[11] In 2019, the Consumer Online Privacy Rights Act proposed requiring certain entities to designate a privacy and data security officer.[12] None of these initiatives found the degree of consensus necessary to become law.

A Way Forward on Data Privacy

Building on these ideas, several steps related to privacy and accountability that could help rebuild trust in digital technologies. The first is passing federal privacy legislation in the United States. The second step is enabling independent watchdog organizations to enforce codes of conduct. The third step is to create training and certification curricula for developers and publishers. The fourth step is identifying measures that the United States, the European Union, and governments should take to internationalize the work of independent watchdog organizations to ensure the interoperability of differing privacy regimes.

Federal Baseline Privacy Legislation in the United States

With a new administration and Congress in the United States, there is a window of opportunity to breathe new life into efforts toward federal privacy legislation. In a hyper-partisan era in which cooperation between Democrats and Republicans in Congress is rare, commercial data privacy holds promise for legislative progress. The Department of Commerce and the White House should reinvigorate efforts to work with Congress on an effective solution that will lead to the passage of baseline federal privacy legislation in 2021. Working on the basis of the several promising pieces of legislation currently under consideration in Congress, the new administration can help forge a compromise if it makes such legislative efforts a priority.

Federal legislation should create clear protections for consumers and greater certainty for companies, based upon globally recognized Fair Information Practice Principles (FIPPs).[13] The FIPPs were developed by the Federal Trade Commission as a part of its

8 Organization for Economic Cooperation and Development, "OECD Principles for Internet Policy Making," 2014.

9 California Consumer Privacy Act of 2018, AB 375 (CCPA).

10 Ro Khanna, "Internet Bill of Rights," 2018.

11 S.2639 – "CONSENT Act," 2018.

12 S.2968 – "Consumer Online Privacy Rights Act," 2019.

13 Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," May 2020.

efforts to promote fairness and trustworthiness in the digital marketplace. They are:

- **Individual Control**—Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- **Transparency**—Consumers have a right to easily understandable and accessible information about privacy and security practices.
- **Respect for Context**—Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- **Security**: Consumers have a right to secure and responsible handling of personal data.
- **Access and Accuracy**—Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- **Focused Collection**—Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- **Accountability**—Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights

To pass Congress, a federal privacy law must achieve consensus among consumer advocates, tech companies, and government agencies. In addition to the issues addressed in the FIPPs, legislative drafters must grapple with thorny questions relating to the portability of data and algorithmic justice. Perhaps the most challenging issues will be reconciling whether or to what extent federal privacy law should preempt state privacy laws, and whether or under what circumstances individual private plaintiffs should be allowed to bring lawsuits for privacy violations.

These issues relating to the preemption of state law and private rights of action have been the major sticking points in recent federal legislative efforts. The passage of the California Privacy Rights Act last November further underscores the necessity and challenge of reconciling state and federal laws. Consumer-privacy advocates rightly seek to ensure that federal preemption does not reduce the privacy rights afforded by state laws. At the same time, proponents of a uniform national standard urge measures to ensure that the resulting system has clear rules that apply nationwide, rather than a patchwork system. It will be a challenge to develop compromise legislation that protects consumers and attracts the support of a sufficient number of members of Congress with pro-business sensibilities.

There are opportunities for compromise. For example, one group of scholars has provided a helpful framework for finding a middle ground and proposed solutions on preemption and private lawsuits that depart from "maximalist approaches."[14] But whatever compromises are reached to overcome the current logjam, there should be clear rules and meaningful accountability mechanisms, and the privacy protections ensured by state laws should be the floor—not the ceiling—for consumer protections.

Breaking the legislative logjam requires returning to governance approaches that have been successful in the Internet context, such as those articulated in the OECD Principles for Internet Policy Making. It is unreasonable to expect Congress to iron out all the relevant rules in advance and then update legislation at the same speed as digital technology evolves. Instead, a new law should be paired with nimble implementation measures that can move at the speed of the Internet. Multi-stakeholder processes among government, technologists, researchers, and civil society will support the development of fair and effective rules that respect privacy and civil liberties.

14 Cameron F. Kerry, John B. Morris, Jr., Caitlin T. Chin, and Nicol E. Turner Lee, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," Brookings Governance Studies, June 2020.

Accountability through Independent Watchdogs and Enforceable Codes of Conduct

New thinking about accountability could also help break the congressional deadlock on federal privacy legislation. Law-enforcement and consumer-protection agencies such as the Federal Trade Commission and state attorneys general need ample resources to enforce the law. Significant privacy and security failures deserve a robust law-enforcement response and the threat of legal action creates a powerful incentive for developers to follow best practices and tell the truth. But when developers make new apps or programs quickly, there are often privacy shortcomings that do not merit a response from law enforcement. More nimble mechanisms for improving privacy and security practices can play an important role in improving developer practices.

Traditional law-enforcement efforts can be supplemented by the enforcement of established codes of conduct.[15] Enforceable codes of conduct present an alternative approach to accountability that does not rely only on lengthy legal processes that focus only on the clearest violations of established legal norms. These codes of conduct can be monitored in real time by nimble, technically savvy partners—such as independent nonprofit watchdogs—that are empowered to investigate, report, and sometimes resolve violations of the rules. Enforceable codes of conduct are not self-regulation schemes. Paired with meaningful enforcement mechanisms, enforceable codes of conduct can help foster a healthy digital ecosystem in ways that laws cannot.

Currently, no single entity has the resources and mandate to monitor compliance with existing laws, regulations, platforms' terms of service, and industry best practices as well as to work proactively with developers, platforms, and law-enforcement bodies to raise the bar on privacy practices. Independent privacy watchdogs can help alleviate some of the risks and harms that are difficult for traditional law enforcement agencies to police, while restoring consumer trust in the digital ecosystem. In addition, as described below, these watchdogs may have a valuable role to play in educating developers and ensuring international interoperability among diverse privacy regimes.

The International Digital Accountability Council

The International Digital Accountability Council (IDAC) is an example of an independent watchdog organization that monitors privacy violations and holds violators accountable. It monitors a range of digital platforms, identifying and deterring problematic activity, ideally before it becomes a public policy concern. IDAC seeks to raise the bar on the level of compliance with consumer protection and privacy standards in the digital ecosystem by proactively identifying a wide range of risks and harms. These concerns come to IDAC's attention through independent investigations, tips from third parties, media reports, and referrals. IDAC then investigates the concerns and then works to remedy them through engagement with developers, platforms, law enforcement, and the public. By monitoring consumer complaints, conducting third-party research, engaging responsible developers, and actively testing for priority concerns, IDAC raises identified concerns to the attention of app developers, educates them on best practices, and—when appropriate—brings concerns to the attention of platforms to ensure compliance with platform terms. In serious cases, IDAC raises concerns with consumer protection agencies, law enforcement, legislators, data protection authorities, and the public to ensure that consumers are protected.

Developer Education and Certification

Even with a new law providing baseline privacy rules in the United States and nimble enforcement mechanisms, developers and publishers offering digital products and services globally will need an advanced

15 Quentin Palfrey, "Watching the watchers: More accountability needed to ensure responsible COVID-19 tracing tech," The Hill, July 13, 2020.

understanding of the relevant rules. At present, it is difficult for them to know what these are. Certainly, there are some sources of authority for what is prohibited in certain cases and in some places. Developers and publishers seeking to serve the European market must comply with the GDPR; those seeking to offer services in the United States must follow U.S. jurisprudence governing unfair and deceptive trade practices under federal or state law, and individual state laws such as those in California and Illinois; those seeking to leverage platforms such as app stores or social media to reach their customers must follow the latest terms of service of companies including Amazon, Apple, Facebook, Google, and Twitter. But making sense of all these overlapping rules—as well as new rules that may take shape in federal privacy legislation—requires education and certification programs for developers, publishers, and other third parties.

A training and certification program could help ensure that individuals and organizations that create data-driven digital applications adhere to the rules effectively and consistently. Platforms such as Amazon, Apple, Facebook, Google, and Twitter should require developers operating on their platforms to participate in training and certification processes to ensure that they are knowledgeable about relevant rules and best practices, including data minimization, privacy by design, and standard cybersecurity protocols.

An enforceable code of conduct could inform the training curriculum, and an independent watchdog empowered to enforce the code of conduct could help identify case studies and troubling trends that could be incorporated into the curriculum on an ongoing basis. The curriculum would therefore be informed by the most relevant risks and harms in the digital marketplace. An education and certification scheme would help raise the bar on compliance and prevent problems before they cause risks and harms to users or litigation and public relations risks for companies.

International Interoperability

Even as the United States advances its domestic privacy framework, it will be important to ensure that new U.S. rules are interoperable with the analogous rules of its trading partners, allowing personal data to be kept private and secure when it is transferred across borders. Lack of interoperability can create uncertainty and significant roadblocks to international commerce. The U.S.-EU Privacy Shield previously regulated the cross-border transfer of personal information; 5,300 companies relied on the mechanism to transfer personal data from Europe to the United States for storage and processing. The 2020 *Schrems II* decision by the Court of Justice of the European Union invalidated Privacy Shield and cast legal doubt on several other commonly used legal tools to facilitate the cross-border transfer of personal information.[16] U.S. and EU officials are engaged in negotiations to find a legal remedy to the immediate challenge; there is an urgent need for a durable solution that provides interoperability among the privacy regimes of the United States, the EU, and other major legal systems around the world. This is no easy task, but there are two immediate steps that can be taken to move the conversation in the right direction.

First, there should be "track 1.5" conversations among government officials (operating in an unofficial capacity) and non-governmental policy and technical experts (including civil society) from the United States and the EU to explore ways of promoting interoperability between the GDPR and emerging U.S. privacy laws. In addition to addressing the challenges implicated in the *Schrems II* decision—such as questions around access to personal data by law-enforcement and intelligence authorities—these dialogues could inform international rules or standards that could allow businesses transferring data across borders to satisfy privacy-law requirements on both sides of

16 See Schrems and Facebook Ireland v. Data Protection Commissioner (Schrems II) (2020) CJEU Case C-311/18. See also: Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security," Brookings, August 5, 2020; and Kenneth Propp and Peter Swire, "After Schrems II: A Proposal to Meet the Individual Redress Challenge," Lawfare Blog, August 13, 2020.

the Atlantic while easing the difficulty of reconciling competing legal standards.

Second, there should be transatlantic, multistakeholder conversations to develop an enforceable code of conduct that fulfills the requirements of emerging U.S. privacy laws and can be accepted by the European Data Protection Board (EDPB). The EDPB has issued guidance describing the requirements enforceable codes of conduct need to meet.[17] These codes of conduct are "voluntary accountability tools which set out specific data protection rules for […] controllers and processors" subject to the GDPR. Once these rules are satisfied, compliance with the rules is tantamount to complying with the GDPR. Such codes of conduct would need to be enforced and should provide for independent watchdogs to help hold firms accountable.

Conclusion

Digital governance requires new thinking. It is unrealistic to rely on legislative bodies to lay down clear, specific, and technologically accurate rules in advance, and then to update them at the speed of technological change. Exclusive reliance on traditional regulatory structures and established enforcement models is unlikely to result in a digital ecosystem that is dynamic and trustworthy, and that enables the transformative possibilities of the digital revolution across all sectors of our economy and society.

Instead, traditional governance approaches need to be coupled with nimbler tools that have proven successful throughout the first few decades of the Internet. Baseline laws should be complemented by dynamic, enforceable codes of conduct and flexible mechanisms for accountability and enforcement. Developers and publishers need a clear understanding of the laws and rules that guide privacy practices. And the rules of the road need to be interoperable across the global Internet, which requires formal diplomatic engagement and informal processes.

Incorporating multi-stakeholder processes and enforceable codes of conduct in privacy frameworks does not have to mean self-regulatory laxity. Policymakers must fund and empower law-enforcement entities and regulators to protect users, patients, and consumers. And policymakers should also empower technologically savvy nonprofit independent watchdogs to enforce the rules. And it is necessary to engage with the regulated businesses to make sure that practitioners are trained in what the rules require. This education process should reflect the real-life examples, lessons, and priorities of watchdogs and government regulators so that practitioners such as developers and platforms have a clear understanding of enforcement priorities and can avoid the kinds of practices that are most likely to result in enforcement actions.

When there are clear rules developed in partnership with technologically savvy stakeholders, comprehensive training and certification efforts for practitioners, and robust, proactive, and credible accountability measures to ensure compliance with applicable rules, there will then be an ecosystem that individuals can trust, and that enables the transformative potential of the digital world.

17 European Data Protection Board, "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679," June 4, 2019.

About GMF Digital

The German Marshall Fund's Digital Innovation and Democracy Initiative (GMF Digital) works to support democracy in the digital age. GMF Digital leverages a transatlantic network of senior fellows to develop and advance strategic reforms that foster innovation, create opportunity, and advance an equitable society.

About the International Digital Accountability Council

Launched in April 2020, the International Digital Accountability Council (IDAC) is led by an experienced team of lawyers, technologists, and privacy experts with a shared goal of improving digital accountability through investigation, education, and collaboration. As a nonprofit watchdog, IDAC investigates misconduct in the digital ecosystem and works with developers and platforms to remediate privacy risks and restore consumer trust.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org