ppi radically pragmatic

Why Digital Privacy Is So Complicated

JORDAN SHAPIRO
PROGRESSIVE POLICY INSTITUTE

MAY 2022

@ppi | @progressivepolicyinstitute | /progressive-policy-institute

Why Digital Privacy Is So Complicated

JORDAN SHAPIRO

MAY 2022

EXECUTIVE SUMMARY

The exact definition of digital privacy is complex, imperfectly aligned with typical understandings of privacy in an analog context. Historically, the vast majority of human actions and interactions existed beyond the scope of surveillance. Today, it's nearly impossible to go about our daily lives without digital tools that facilitate modern life, but also collect data about individuals. When this growing flood of data is linked to an individual it is called "personal identifying information" (PII), the centerpiece of the debate over digital privacy.

The discussion of digital privacy is complicated precisely because it operates on three distinct but interrelated levels. First, privacy's social and legal dimensions depend on whether individuals, corporations, or governments are assumed to hold primary rights to personal data collected about those individuals. In Europe, for example, the individual holds primary rights over their data, while in China, the state takes precedence.

The second level of the privacy discussion addresses data use and the technical protection and security of personal information to safeguard it from unwanted intrusion or theft while allowing individuals transparent access to their data. These complicated technical issues arise no matter privacy's social and legal structure.

The third level of the privacy debate deals with the economics of PII. How does the chosen privacy model interact with innovation and growth? And how can it be assured that individuals get the appropriate benefits from their data?

This paper will lay out the privacy models of the United States, Europe, and China, with smaller sections on the United Kingdom, Canada, and

India. For each area, we will discuss the social and legal structure, the technical design of security and transparency, and the economic implications of privacy and innovation.

This paper sets out a framework for PPI's ongoing privacy work. It lays the groundwork for future discussions of privacy legislation in the United States.

BACKGROUND

For much of human history, sparse information collection and dissemination created a wide margin for privacy.[1] Personal details had to be deliberately disclosed to a trusted information collector. While life was not secret, information known about individuals was limited to word-of-mouth or, when more accurate records were needed, stored on paper forms. Without any dissemination platforms, like we see today in social media, the full extent of data known and stored about historic peoples was limited to community knowledge and essential records.

Today, digital data collection has no such limits.

Aspects of public and private life that once only passed between individuals present, like visiting a friend, buying a meal, or running an errand, can now be easily shared, tracked, and stored. The data are largely collected via three major channels. First, many people voluntarily consent to share personal information by, for example, posting on social media or participating in an online survey or research study. The second is data we consent to share in exchange for services. Today, all software and hardware come with terms of service and privacy policies that are legal contracts between the consumer and service provider. The documents typically outline the degree to which data is stored, shared, or sold but are not federally required to do so.[2]

Finally, there are data collected without consent. For example, website trackers that follow internet users from site to site, collect browsing information. Other forms of non-consensual data collection include CCTV cameras on streets and in stores which scan our faces almost everywhere, storing that information in remote servers without any way to opt out.[3]

The degree to which individual information is shared via each of these collection methods raises different questions for protecting consumer privacy.[4] The internet expands the community with whom we share our information. Digital storage overcomes many of the limitations of physical storage. The requirement of data sharing to use essential everyday technologies creates a new relationship between individuals and the groups that store their data.[5]

Indeed, the greater degree of digital data collection and use has provoked concerns from consumers and legislators about legal rights to the information they view as private.[6] Despite the concerns, governments, firms, and researchers use these data to innovate and better understand consumer behavior and society. It fuels the development of revolutionary technological innovations and can lead to better policymaking, which benefit society. In short, the data are extremely valuable.

As a result, both the social and security considerations of privacy have been radically transformed, while a third consideration, the economics of privacy, has become crucially important.

Layer 1: Social/Legal

Historic repositories of personal data, ledgers stored in notebooks or personnel documents in filing cabinets, were naturally limited and constrained. People had a social expectation that most of their life that was not explicitly disclosed was unrecorded.

Modern data repositories, stored in servers worldwide, collect vast and specific information about people's characteristics and behavior, prompting uncertainty about rights, data access, and scope. Historic rules for pre-digital privacy do not currently cover the necessary scope in the digital age.[7] New digital privacy laws around the world seek to address this gap, and countries are taking very different approaches to solving the legal question of who has the right to collect, access, and use data about individuals.[8]

In the United States, at the federal level, data supplied in exchange for tools and services is held and used by the data collector or processor. Users click consent on legally binding privacy agreements, detailing the scope of data use by the firm. Unless explicitly stated in these agreements, data can be traded and sold on the market, following standard definitions of trade and exchange. In contrast, the EU gives broad legal rights to the individual to access, modify, and delete information stored about them regardless of who collects and stores the data.

We will fully explore contrasting privacy models later in this paper.

Layer 2: Security

Ledgers in notebooks and papers in filing cabinets were decentralized, difficult and expensive to copy, and primarily limited to voluntary disclosure. Stealing data had a high barrier to entry and low utility.

Today, data repositories contain sweeping details about billions of people's social and financial lives. To protect users and comply with the law, personal data must be secured against malicious access and use. As the repositories are now digital, safeguarding access is inherently technological.

None of the international privacy laws surveyed for this piece stipulate specific security technologies; instead, requiring security by design.[9,10,11,12] The strategy is twofold: first, implementing technological safeguards for personal data; second, requiring disclosure of data breaches, as no security system can be absolute.

Layer 3: Economics

In the past, it was costly in both time and money to collect private data. Its value was usually limited to narrow applications, such as business insights and administrative records. Therefore, by and large only essential data was captured. Technology has made the mass collection of data easy. It is a self-reinforcing cycle where technological development facilitates data collection, creating insights for further technological improvements.

Technological improvements can be found in every sector from health to finance to recreation. The digital economy was founded upon consumer willingness to exchange personal information for access to free services. But there is tension between the massive societal benefits of these technological innovations and the privacy concerns of citizens and governments.

There's no question that the United States needs a national privacy law to protect consumers, for cyber security, and to be a part of the global privacy conversation.[13] Balancing legal rights and

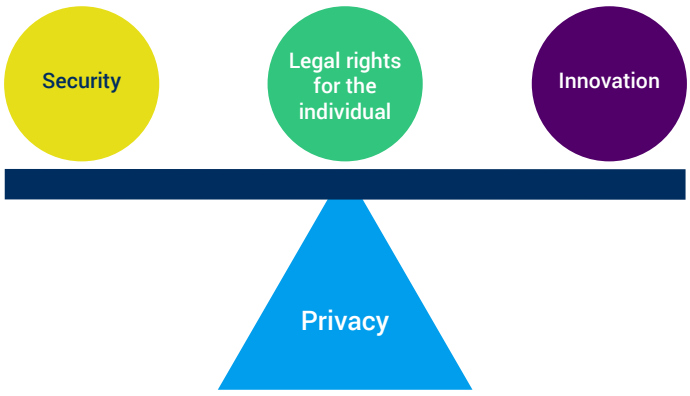
security rules to not unduly hinder innovation and successful business models is trickier. Overly restrictive data privacy laws can also create high barriers to entry for smaller and less-resourced groups and risk suppressing innovation.[14]

The following section will examine international data privacy legislation, surveying the laws that govern some of the largest markets: the United States, the European Union, and China, as well as the laws proposed by other prominent democracies: India, the United Kingdom, and Canada. It will define and analyze each nation's approach to the legal, security, and economic aspects of data privacy.

HOW IS PRIVACY DEFINED ACROSS PEER NATIONS?

Data privacy laws have cropped up in every corner of the world in response to the flood of previously unrecorded personal data about individuals' daily lives. The new data environment has become essential for economic innovation, but vast repositories of personal details and behaviors can be easily exploited in the wrong hands. As a result, privacy laws seek to regulate the interrelated layers of legal rights and security obligations around PII.

FIGURE 1: EACH COUNTRY BALANCES THE THREE LAYERS OF PRIVACY: LEGAL RIGHTS OF THE DATA SUBJECT, SECURITY, AND INNOVATION. AN IDEAL PRIVACY ENVIRONMENT WOULD BALANCE THE THREE LAYERS



United States

The United States is a global innovation leader with the greatest share of leading tech firms. Nevertheless, for various reasons, the United States has yet to pass a comprehensive digital privacy law. Ad-hoc laws from the 20th century focused on data and privacy, such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA), fail to account for a changing landscape of data collection.[15] Consumer devices, like Fitbit and Apple Watch, collect health data but aren't covered under HIPAA. Youth don't need to age-identify on websites that may be collecting their personal information. Protections for all consumers need a refresh to take into account the new digital environment.[16]

The United States addresses the three layers of digital privacy: legal rights, security, and innovation, through sector-specific laws, such as those listed above, and with market forces. In the data market, users trade personal data for online services. Trading data for services takes several different forms: voluntary, where consumers publish data about themselves on social media; necessary, where to use an essential product, like a smartphone or maps, specific data must be disclosed; and surveillant, when data is collected or sold without the explicit knowledge or consent of the data subject. After collection, as with any other economic exchange, the firm can use, store, and process the data.

Whatever the collection method, the utility of data is multi-dimensional. Equifax and Oracle collect and sell data to others, among other uses.[17] Google, for instance, uses data for targeted advertising, innovation, and improvement of products and algorithms.[18] Amazon, among other purposes, uses data to improve user experience and lower the costs of packing and sorting.[19]

In the U.S., the first layer of data privacy gives the majority of legal rights to the firms that collect or possess data. Data become goods exchanged for otherwise free services. This exchange is detailed in privacy agreements, often full of legal jargon, which define firms' rights to collect and store data but are difficult to understand or interpret by the average consumer. Data subjects, individuals about whom the data is collected, have little additional access to see, update, or delete the data about them. Because there are no comprehensive federal protections to view, update, or delete data, it's unclear how many companies may be selling or copying consumer data.[20]

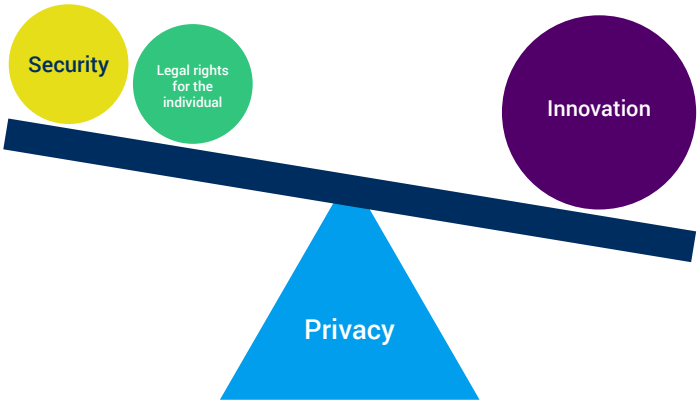
From algorithm improvement to sales, the varied uses of data can make the second layer of U.S. digital privacy, security, seem like a free-for-all. This is not the case. Data generate market insights and inform the direction of innovative technologies. Firms have a strong incentive to secure the data they possess to maintain consumer trust and safeguard their ability to compete.

Data security, however, requires adaptability and strong technological capabilities. The best safeguards available by today's standards could be hacked tomorrow. All U.S. states enforce data breach notifications; under federal law, however, only financial, health care, and telecom breaches must be reported to the consumer.[21] At the federal level, if a breach occurs, the firm may be liable for negligence. However, this must be proven in a court of law, a high barrier for individuals seeking remediation for data breaches.

This light-touch approach has strongly contributed to America's ability to be the seat of global innovation. Firms' ability to collect data about millions, and in some cases billions, of users facilitates that success. Data's flexible and multifaceted utility has become a dominant business model for the private and public sectors.[22] The technologies and insights that have arisen from the firm-driven data environment have become a self-reinforcing cycle; more data engenders more innovation, yielding massive economic value with enormous benefits to modern life.

But not everyone is happy with the new status quo driven by America's growth mentality and light-touch regulatory environment. In particular, countries worldwide see the value of data and are passing privacy laws, in part to countermand U.S. dominance.

FIGURE 2: THE UNITED STATES BALANCES INNOVATION OVER SECURITY OR RIGHTS FOR THE DATA SUBJECT



Canada

Two major federal privacy laws govern personal data use in Canada: The Privacy Act, 1985, which directs federal government data use, and the Personal Information Protection and Electronic Documents Act (PIPEDA), passed in February 2022 and governs all commercial data use.[23] Provincial governments in Canada also enforce provincial-level data protections that in some cases supersede PIPEDA, except where data flows across provincial or international borders. The two federal acts clarify data access and security for citizens.

PIPEDA grants firms broad rights to data while still giving consumers some control. The law directs companies to gain consent for data collection and gives citizens some access to their personal data. It also gives firms broad leeway to, without the consent of the individual, disclose data for investigative purposes, like a breach of contract. PIPEDA gives individuals rights to view and update their data with data collectors and permits requests to delete personal data after the company has used the data for the required purpose. If companies want to keep the data after a request to delete, they may anonymize and continue to use it.

PIPEDA requires firms to protect personal data in accordance with how sensitive the data are and to implement security adaptably as technical safeguards improve over time. In the event of a data breach, firms must notify individuals and keep records of all breaches, though firms are not liable.

The Canadian digital privacy environment is fragmented. In addition to PIPEDA and the Privacy Act, Canadian provincial governments enforce other provincial-level privacy laws. Companies operating across Canada need to comply with provincial laws as well as federal.

European Union

In 2016, the European Union announced a landmark data privacy law, the General Data Protection Regulation (GDPR). The GDPR is the most complex and consumer-focused digital privacy law globally. The comprehensive legislation covers the rules and responsibilities for data handling in all sectors, government, business, and nonprofits. Since coming into full effect in 2018, the GDPR has offered an alternative to the U.S. market approach to data.

The U.S. approach defines data as a tradeable commodity for access to digital services, giving legal rights to the entity in possession of the data. The EU model treats these rights very differently. It provides legal rights of PII to the data subject.[24] Europeans can withdraw, change, update, or delete their information even when it is no longer in their possession. Firms effectively rent or lease data from citizens. Privacy policies set out the terms for temporary use by stating the purpose of data collection. The GDPR requires firms to minimize data collection and delete it after use.

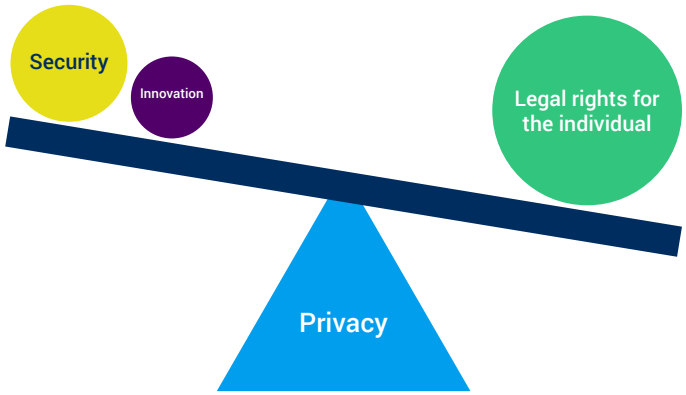
Moving to the second layer, data security is a raison d'être for the legislation. Recital 1 of the regulation states, "Everyone has the right to the protection of personal data concerning him or her."[25] Firms are permitted to rent data from individuals with a guarantee of security.

The GDPR uses a risk-based method, requiring data protection by design, building security features into every aspect of the data journey. Any firm collecting data must perform a data protection impact assessment (DPIA).[26] This means that, from the outset, any entity collecting location or behavior data, "systematically monitoring a publicly accessible place on a large scale," or processing data about immutable characteristics must conduct a risk assessment.[27] The risk assessment requires data collectors to indicate the purpose of data collection, outline the data to be collected, the duration of data storage, security features, and risk mitigation. Additional data security technical requirements under the GDPR include pseudonymization, i.e., replacing qualitative information, like names, with artificial identifiers, and encryption, digital scrambling of the remaining data. Other security measures are left to the purview of the firm.[28] A divergence from the U.S. model is that in the case of a data breach, the data controller is required to notify the data subject and could be liable for the resulting harms.[29]

The GDPR's impact on the third layer of digital privacy, innovation, continues to evolve. Some aspects, such as clarifying and improving data protection and security, benefit firms and consumers. Exemptions for public and private research, so long as data is well secured, create clear avenues for certain types of innovation.

Built into the GDPR is a requirement for data minimization, i.e., only collecting data with a clearly defined purpose: nothing superfluous.[30] Restricting the quantity and duplication of personal information collected recaptures some of the natural limits of historic data privacy. More research is needed to see how it interacts with 21st-century economic growth models and innovative technologies like machine learning, which rely on the ability to collect large, representative, datasets.[31]

FIGURE 3: THE EU WEIGHS LEGAL RIGHTS FOR THE INDIVIDUAL OVER SECURITY AND INNOVATION



United Kingdom

Since leaving the EU, the United Kingdom has followed the data protection principles of GDPR, re-branding the legislation as UK-GDPR. However, as a part of their overarching reassessments of inherited EU laws, the British government is in the process of refining digital privacy legislation.

In September 2021, the Department for Digital, Culture, Media, and Sport released "Data: A New Direction," with the goal to align transparency and security with digital innovation.[32] This report seeks to alleviate burdens on businesses and improve public sector services by reducing barriers to data flows. It does not define data rights nor indicate if it seeks to change data access from EU-GDPR, where citizens have full rights over their data.

The new UK proposal highlights the interconnectedness of security and innovation. While the reforms are still in their early stages, the UK signals a break with the GDPR, seeking instead to become a country that is both pro-growth and pro-data rights.[33] The model highlights robust transparency and security for citizens, while proactively collecting data for better public services and permitting data collection to further private sector innovation. The key, according to the report, is data availability and data responsibility. Availability highlights the need to facilitate data re-use and responsibility ensures the data isn't misused.[34]

The UK wants to explore a flexible framework, particularly to help small and medium-sized enterprises. It proposes greater leeway for data reuse so that the UK can be a secure hub for data flows.

China

The People's Republic of China passed its version of the GDPR, the Personal Information Protection Law (PIPL) on August 20, 2021.[35] It came into force just three months later, on November 1. The legislation is yet another take on data protection in the modern era; one that reflects their state-centric data model. It is important to note that China has a longstanding political contract between citizen data and the state, whereby the state is allowed to collect, view, and store any information related to its citizens. Consequently, its data protection law is focused primarily on how companies use Chinese citizens' data.[36]

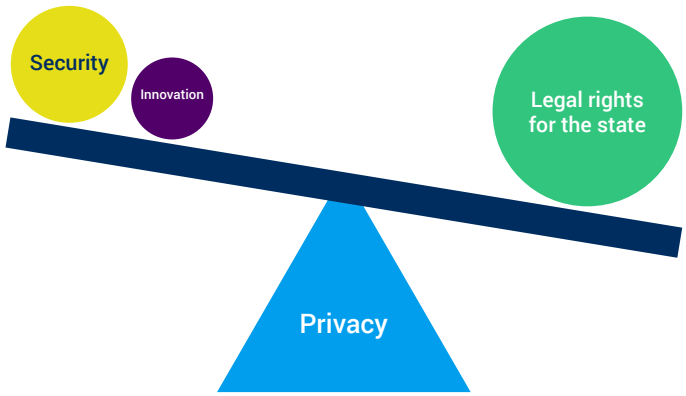
The Chinese understanding of the first layer of digital privacy, legal rights, is that rights are a co-operative between the individual and the state. Similar to the GDPR, a translated version of Article 44 of PIPL states: "Individuals have the right to know and the right to decide relating to their personal information, and have the right to limit or refuse the handling of their personal information by others."[37] PIPL, like the GDPR, gives citizens the right to update and delete their data with companies. The state, however, holds full legal rights to citizen data and acquire citizen data from firms at any time. The government has broad circumstantial discretion in legal rights to PII in China.[38]

Addressing the second layer, data security, PIPL requires strong technical protection of personal information. In the event of a breach, the data collector is liable.[39] For firms that collect large amounts (as determined by the state) of PII, the law requires a data protection officer to manage the security process. Regardless of quantity, PIPL recommends encryption and pseudonymization of data, though it does not offer further technical suggestions. If the data is fully anonymized, whereby anyone viewing the data would not be able to attribute it to an individual, PIPL does not apply.

The innovation layer of digital privacy in China is closely intertwined with the rights and security layers. PIPL imposes strict data localization as a security feature and an economic development feature, whereby data collected within China cannot be transferred or processed outside of the country without explicit consent by the government. Non-Chinese firms operating in China must appoint specific staff to process Chinese data within the country's borders.[40]

Whereas the GDPR applies to both state and private entities, PIPL only applies to companies handling Chinese citizen data. As of now, it's unclear whether these new restrictions will shift the strategy of multinationals with offices in China. The most stringent penalty for companies that violate the law could be prohibition from operating in China.

FIGURE 4: CHINA WEIGHS THE LEGAL RIGHTS OF THE STATE ABOVE OTHER CONSIDERATIONS



India

As of the writing of this paper, India has yet to pass a comprehensive privacy bill, though frameworks for legislation have been under discussion since 2017. The Indian approach considers data to be a national asset, imposing data localization and giving increased data powers to the state. India sees itself as a fourth way to the American, European, and Chinese approaches to data privacy.

The Data Protection Bill (DPB), similar to the European model, would give legal rights of PII to the data subject while, more similar to China, reserving ultimate powers for the state. Individuals, similar to the GDPR, would have broad rights to access, modify, and delete data, including the right to be forgotten. Data collectors would have the right to collect PII from citizens using consent-based data collection — the privacy policy checkboxes now ubiquitous on most websites.[41] Regardless of legal rights, the state is exempt from DPB and may impose state power to collect either personal or non-personal data at any time.

India weighs the security layer more heavily than legal rights or innovation. The DPB has similar technical specifications to the EU and China: security by design. In the Indian bill, data localization is leveraged as a primary security feature. To that end, DPB identifies three data categories: sensitive data, or PII; critical data, information important to national security; and general data, an umbrella term for the remaining data types. Each category requires different levels of localization. Sensitive data may be processed outside of India but must be stored within the country. Critical data may never leave the country's borders.[42]

India's data protection bill covers the vast majority of businesses. Similar to the GDPR, some sectors, such as journalists, researchers, statisticians, lawyers, small businesses, and the state, would be exempt from compliance with DPA. And, similar to the Chinese law, the Indian government would retain itself broad latitude to access any digital information within India, even if that information is protected by intellectual property rights.[43]

POTENTIAL CONSIDERATIONS FOR U.S. POLICY

In this piece, we've examined many approaches to digital privacy across three levels: legal rights, security, and innovation. We will not lay out a strategy in this piece except to say that all three levels are important. It is time for the United States, as a global leader in digital innovation, to begin to codify data privacy. A future law or laws should seek to close important gaps in today's patchwork of federal laws and regulations aimed at protecting personal data, and to standardize important digital privacy rights amid a confusing and potentially conflicting welter of state regulations.

In conclusion, here are some important considerations of key issues lawmakers will have to grapple with to craft a national privacy law that gives U.S. consumers greater control over their data and creates stronger safeguards against misuse of their information.

Consent-based privacy

Much of the current privacy legislation highlights the importance of consent and control for data collection. Consent-based rules allow consumers to opt-in and opt-out of data collection and to better control the flow of personal data to firms. Facebook and Google created data dashboards for users while website cookie pop-ups prevent shedding personal information on every page. Explicit consent is an appeal to consumer transparency and choice.

Data use for business is complex, multifaceted, and evolving. Consumers interact with many websites every day. Reading through and agreeing to a daunting and lengthy data usage agreement for each one of these sites is impractical and gives only an "illusion of control."[44] Illusion because consent-based privacy that users understand all the uses of data and that users have the time to explore and modify every privacy setting across every website.

Data Protection Risk Assessment

A vital aspect of the transparent and safe use of data is for regulators to have a clear sense of what information is being collected about individuals and its general purpose (i.e., sales, R&D, marketing, etc.). A risk assessment is standard across financial services and other areas where harm could befall a consumer or employee. Data should be no different.

Data localization

Data localization appears in several of the privacy models in this paper, including the E.U., China, and India. From a national security perspective, data localization allows greater control for governments. It also offers transparency to citizens that their data is not processed outside the jurisdiction of their consumer protection agencies. This is the argument of the European Union Court ruling of July 2020, Shrems II, which eliminated certain pathways for cross border data flow between the U.S. and E.U. due to concerns that U.S. data protection laws are not compliant with the GDPR.[45] As of March 2022, the U.S. and European Commission announced a new data-sharing framework, but it might face legal challenges.[46]

This report has touched on the potential impact of data localization for tech innovation and competition, but it also has significant implications for the future of the internet. The world seems headed toward a "splinternet" — the fragmenting of today's borderless internet. China already has insulated its online activity from the rest of the world, and Russia also is pursuing a closed-off internet.[47] By erecting

barriers to the essentially free exchange of ideas and information online. Data localization restricts the ability to globalize internet services and solve global problems. It can also allow governments greater control over what knowledge citizens have access to.

Data minimization and the future of artificial intelligence

A major concern by privacy advocates and consumers is the quantity of personal information collected by data collectors. The data helps them develop better products and market personalized experiences to customers. The answer throughout the privacy legislation surveyed in this piece is data minimization, or limiting the amount of personal information collected. The more identifiable information that is stored, the greater the opportunity for that data to be hacked, revealed, or shared. There are also legitimate privacy concerns around the quantity and quality of data profiling that firms may create about individual consumers.

Data collection, however, isn't just for data profiles. Data collected across the internet also powers machine learning and artificial intelligence, which are increasingly crucial in nearly every economic sector. These technologies work by using mathematical functions to find patterns in massive amounts of data that would be too complex for humans to process. Although it might seem that these machines are intelligent, they don't learn from their surroundings, only from the inputted instructions and data. And, to work correctly, they need a lot of it. There is a balance to be struck between minimizing personal information collected while still collecting sufficiently rich information to power these algorithms and generate new technologies.

Moving forward

With three major global privacy standards already in effect, the United States has an opportunity to set a new precedent for data protection. While the U.S. market approach receives pushback from countries and individuals alike, this approach's ability to innovate is very successful. But innovation is also an ability to envision and implement systemic improvements.

The U.S. can take a pragmatic approach by aligning user rights with the market needs regarding data access. An example of this would be allowing firms to retain control of the data required to offer their services while granting users transparent access to update or remove that data.

Additionally, the U.S. approach must improve data security provisions. It can learn from international legislation to include comprehensive technical security requirements and prevent harm caused by breaches from falling entirely on the individual.

Finally, developing privacy rules that maintain, and even augment, incentives to innovate is key. An unbalanced approach will lead to unsatisfactory outcomes. The U.S. has the opportunity to put forward a new approach that balances all three layers key to successful data privacy: legal rights, security, and innovation.

Our subsequent report will dive further into privacy laws within U.S. states and legislation at the federal level.

References

1 Neil Richards, *Why Privacy Matters* (New York, NY: Oxford University Press, 2022).

2 Richards, *Why Privacy Matters*, 22.

3 Richards, *Why Privacy Matters*, 22, 83-85.

4 Jamie Susskind, *Future Politics: Living Together in a World Transformed by Tech* (Oxford, UK: Oxford University Press, 2020).

5 Susskind, *Future Politics*, 61.

6 Richards, *Why Privacy Matters*, 22.

7 Richards, *Why Privacy Matters*, 90-91.

8 Cathy Cosgrove, "Global Comprehensive Privacy Law Mapping Chart," Global Comprehensive Privacy Law Mapping Chart (International Association of Privacy Professionals, November 2021), https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/.

9 "General Data Protection Regulation (GDPR)" (Proton Technologies AG, 2022), https://gdpr.eu/.

10 Rogier Creemers and Graham Webster, "Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1, 2021," DigiChina (Stanford University, January 5, 2022), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

11 Information Commissioner's Office, "Data: A New Direction," (September 10, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

12 "The Personal Information Protection and Electronic Documents Act (PIPEDA)" (Office of the Privacy Commissioner of Canada, December 8, 2021), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

13 Jennifer Huddleston, "The Importance of Balancing Privacy with Innovation, Consumer Benefits, and Other Rights in the FTC's Approach to Consumer Data Privacy," Mercatus Center at George Mason University, May 30, 2019, https://www.mercatus.org/publications/antitrust-and-competition/importance-balancing-privacy-innovation-consumer-benefits-and.

14 Luke Dascoli, Gillian Diebold, and Daniel Castro, "The Looming Cost of a Patchwork of State Privacy Laws" (Information Technology and Innovation Foundation, January 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws.

15 Richards, *Why Privacy Matters*, 50-52.

16 Syagnik Banerjee, Phil Longstreet, and Thomas Hemphill, "Wearable Devices and Healthcare: Data Sharing and Privacy," The Information Society 34, no. 1 (December 27, 2017): pp. 49-57, https://doi.org/10.1080/01972243.2017.1391912.

17 "These Are the Largest Data Brokers in America," Privacy Bee, August 30, 2021, https://privacybee.com/blog/these-are-the-largest-data-brokers-in-america/.

18 Google, "Google Ads Data and Privacy ," Google Safety Center, accessed April 18, 2022, https://safety.google/privacy/ads-and-data/.

19 "Amazon.com Privacy Notice," Amazon, last modified February 12, 2021, https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ.

20 Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (and Why It Matters)," The New York Times, September 6, 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

21 India Vincent, "Data Breach Notification Laws in the United States: What Is Required and How Is That Determined?," JD Supra, December 10, 2021, https://www.jdsupra.com/legalnews/data-breach-notification-laws-in-the-5409251/.

22 Abou Zakaria Faroukhi et al., "Big Data Monetization throughout Big Data Value Chain: A Comprehensive Review," *Journal of Big Data* 7, no. 1 (January 8, 2020): pp. 1-22, https://doi.org/10.1186/s40537-019-0281-5.

23 "The Personal Information Protection and Electronic Documents Act (PIPEDA)," Office of the Privacy Commissioner of Canada, last modified December 8, 2021, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

24 "General Data Protection Regulation (GDPR)" (Proton Technologies AG), accessed April 18, 2022, https://gdpr.eu/.

25 General Data Protection Regulation, 2022, Recital 1.

26 "Data Protection Impact Assessment (DPIA)" (Proton Technologies), accessed April 18, 2022, https://gdpr.eu/data-protection-impact-assessment-template/.

27 General Data Protection Regulation, Article 35.

28 Data Protection Impact Assessment, 2019.

29 General Data Protection Regulation, 2022, Art. 82.

30 Nicholas Martin et al., "How Data Protection Regulation Affects Startup Innovation," *Information Systems Frontiers* 21, no. 6 (2019): pp. 1307-1324, https://doi.org/10.1007/s10796-019-09974-2.

31 Castro and Dascoli, 2022.

32 "Data: A New Direction," Department for Digital, Culture, Media & Sport (GOV.UK), September 10, 2021, https://www.gov.uk/government/consultations/data-a-new-direction.

33 "Data: A New Direction," 7.

34 "Data: A New Direction."

35 Katie Nadworny, "New Data Privacy Law Will Soon Take Effect in China," Society for Human Resource Management (SHRM), October 5, 2021, https://www.shrm.org/resourcesandtools/hr-topics/global-hr/pages/china-data-privacy-law.aspx.

36 Creemers and Webster, "Translation: Personal Information."

37 Creemers and Webster, "Translation: Personal Information," Article 44.

38 Nadworny, "New Data Privacy Law."

39 Creemers and Webster, "Translation: Personal Information."

40 Jen Fulmer, "How to Comply with GDPR, PIPL and CCPA," eSecurity Planet, December 22, 2021, https://www.esecurityplanet.com/compliance/compliance-gdpr-pipl-ccpa/#pipl.

41 "The Personal Data Protection Bill, 2019," December 5, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

42 Vijay Govindarajan, Anup Srivastava, and Luminita Enache, "How India Plans to Protect Consumer Data," Harvard Business Review, December 18, 2019, https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data.

43 Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?" (Carnegie India, March 2020), https://carnegieendowment.org/files/Burman_Data_Privacy.pdf.

44 Richards, *Why Privacy Matters*, 94-95.

45 Caitlin Fennessy, "The 'Schrems II' Decision: EU-US Data Transfers in Question," International Association of Privacy Professionals, July 16, 2020, https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

46 Jennie Cunningham and Amanda Witt, "Guarded Optimism on EU-US Data Transfers: The EU and US Announce Trans-Atlantic Data Privacy Framework," JD Supra, May 9, 2022, https://www.jdsupra.com/legalnews/guarded-optimism-on-eu-us-data-6176507/.

47 Keith Wright, "The 'Splinternet' Is Already Here," TechCrunch, March 13, 2019, https://techcrunch.com/2019/03/13/the-splinternet-is-already-here/.

ABOUT THE AUTHOR

Jordan Shapiro is an Economic and Data Policy Analyst at the Progressive Policy Institute.

ppi

The Progressive Policy Institute is a catalyst for policy innovation and political reform based in Washington, D.C. Its mission is to create radically pragmatic ideas for moving America beyond ideological and partisan deadlock.

Founded in 1989, PPI started as the intellectual home of the New Democrats and earned a reputation as President Bill Clinton's "idea mill." Many of its mold-breaking ideas have been translated into public policy and law and have influenced international efforts to modernize progressive politics.

Today, PPI is developing fresh proposals for stimulating U.S. economic innovation and growth; equipping all Americans with the skills and assets that social mobility in the knowledge economy requires; modernizing an overly bureaucratic and centralized public sector; and defending liberal democracy in a dangerous world.

PROGRESSIVE POLICY INSTITUTE
1156 15th Street NW
Ste 400
Washington, D.C. 20005

Tel 202.525.3926
Fax 202.525.3941

info@ppionline.org
progressivepolicy.org