GENERAL COMMITTEE MEETING

Thursday, February 20, 2020
3:00 PM to 4:00 PM

Healthcare Leadership Council
750 9th Street, NW, Suite 500 Washington, D.C. 20001
Conference Line: 857-232-0157, **Code:** 30-40-73

1.	**Welcome and Introductions**	
2.	**Hearing**: **"Data Privacy and Portability at VA: Protecting Veterans' Personal Data"**	Attachment 1
3.	**OCR Bulletin on Coronavirus**	Attachment 2
4.	**CCPA Revised Proposed Regulations**	Attachment 3
5.	**NIST Final Privacy Framework**	Attachment 4
6.	**Data Protection Act (Sen. Gillibrand)**	Attachment 5
7.	**Articles of Interest**	Attachment 6
8.	***Ciox Health v Azar, et al***	Attachment 7

Testimony of

Tina O. Grande
Executive VP, Policy, Healthcare Leadership Council and
Chair, Confidentiality Coalition

Before the
House Committee on Veterans' Affairs
Subcommittee on Technology Modernization

Data Privacy and Portability at VA: Protecting Veterans' Personal Data.

February 12, 2020

Chairwoman Lee, Ranking Member Banks, and Members of the House Committee on Veterans' Affairs Subcommittee on Technology and Modernization (Subcommittee), thank you for the opportunity to testify today.

My name is Tina Grande. I am Executive Vice President of Policy of the Healthcare Leadership Council (HLC) and Chair of the Confidentiality Coalition (Coalition).

HLC is a coalition of chief executives representing all disciplines within American healthcare, including hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, home care providers, and information technology companies. It is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century healthcare system that makes affordable high-quality care accessible to all Americans.

The Confidentiality Coalition, founded to advance effective patient confidentiality protections, is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others. The Coalition's mission is to advocate for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. I have attached to my testimony information about the Coalition, HLC and the membership of each.

Through the breadth and diversity of our membership, HLC and the Coalition are able to provide a broad-based and nuanced perspective on any legislation or regulation affecting the privacy and security of health consumers. We work closely with key legislators and regulators to help strike the right balance between protecting privacy and allowing the appropriate sharing of health information to ensure safe, high-quality, and coordinated healthcare.

We understand that the Subcommittee is examining how the Department of Veterans Affairs (VA) manages veteran's data, including interoperability, privacy and security issues, in light of the challenges posed by changes in technology and the increasing monetization of data.

This examination is especially timely as new technologies are being marketed every day that allow for not only the generation of new data not previously available, but the ability to transmit and share data more easily, and to use it for purposes as varied as targeted advertising to developing artificial intelligence (AI) tools for the early detection of cancer and other debilitating diseases. For every promising health information technological development there is the risk of its misuse, and as the value of data increases, so does the incentive to misappropriate it. The more consumers are able to control and direct the sharing of their health data, the greater the likelihood of the data finding its way into the hands of third parties not committed or bound to protect it.

The Coalition's members having been grappling with these same challenges as they seek to use data to improve healthcare outcomes, quality and efficiencies, and to facilitate data sharing among patients, healthcare providers and other healthcare organization. Congress too, through the 21st Century Cures Act, has sought to address some of these challenges by directing the Department of Health and Human Services (HHS) to implement regulations to advance interoperability, support patient access to their electronic health records, and eliminate information blocking.

While these steps are laudable and essential, there remains the glaring oddity in our current health data regulatory scheme that certain health data is subject to robust federal privacy protections while other health data is not. As long as this disparate treatment exists, the challenges faced by an organization such as the VA to manage health data in a way that harnesses new technological innovations while maintaining the privacy and security of all this data will remain formidable, if not insurmountable.

My testimony, therefore, focuses on how this regulatory gap should be addressed, and the principles that we believe the Subcommittee and others in Congress should consider in seeking to ensure that all consumer health data is appropriately protected while at the same time being available as seamlessly as possible for necessary healthcare functions and activities.

Health data that is governed by the Health Insurance Portability and Accountability Act (HIPAA), including data held by VA covered entities, is protected by a framework that has for over 20 years provided individuals with strong privacy rights and protections.

HIPAA's well-established rules and guidance, together with its robust and consistent enforcement by HHS, has made it a trusted and accepted national standard for the protection of personal health information. It has also provided HIPAA covered entities and their business associates with a clearly delineated framework and parameters within which to operate. Therefore, any approach to health data privacy should preserve the existing HIPAA framework, and new legislation should apply only to health data not governed by HIPAA.

We support the development of new health information technologies, whether at the consumer level in the form of mobile health apps and wearable devices, or at the enterprise level, such as sophisticated new tools that aggregate and analyze vast quantities of data that can transform healthcare. These new innovations in health information technology are not only empowering consumers to be more engaged in managing their health outside of traditional healthcare settings, but are enabling healthcare organizations to develop new treatments and cures that will deliver enormous benefits to patients and greatly improve our healthcare system.

These innovations have also resulted in more and more health data falling outside the protections of HIPAA. This will be the case when the technology or services are not offered by or on behalf of a HIPAA covered entity, but rather, by developers or technology companies directly to the consumer. For example, a consumer may download a third party app to their smartphone that tracks diet, exercise and weight, and uses the app to send a summary report to their doctor before their next appointment. As long as the doctor did not hire the app developer to provide its services to the doctor's patients, the data in the app is not protected by HIPAA, even if the app is recommended by the patient's doctor.[1]

Today, consumers may not fully appreciate which of their health data is collected by an entity subject to HIPAA, and so protected by HIPAA, and which is not. To the extent personal health information is not already covered by HIPAA ("non-HIPAA health data"), privacy and security rules comparable to HIPAA should apply to it. This is not only vital to maintain consumer trust, but also necessary to honor the rightful expectations of all consumers that their health information, among the most sensitive of personal information, is appropriately safeguarded, and that they may exercise the same types of privacy rights with respect to it as they enjoy with respect to data covered by HIPAA. As the Subcommittee continues to assess the management of veterans' health data, we are pleased to share the Confidentiality Coalition's "Beyond HIPAA" Privacy Principles that outline our views on the protection of non-HIPAA health data. A copy of these principles is attached to my testimony.

[1] See The Department of Health and Human Services Office of Civil Rights Guidance documents, Health App Use Scenarios & HIPPA. February 2016 ("Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The doctor's recommendation implies her trust in the app, but there is no indication that the doctor hired the app developer to provide services to patients involving the handling of PHI. The consumer's use of an app to transmit data to a covered entity does not by itself make the app developer a [business associate] of the covered entity.")

The Coalition believes that any federal legislation to protect non-HIPAA health data should do so in a manner that harmonizes with the existing HIPAA framework. This includes HIPAA's implied consent for the use and disclosure of health information for treatment purposes, and minimum necessary information for payment and health care operation purposes. It also includes the requirement to obtain an individual's written authorization to use or disclose their protected health information (PHI) for marketing purposes or to sell their PHI. HIPAA authorizations put individuals on notice that, once disclosed, their data may no longer be protected by HIPAA. They also require HIPAA covered entities to be transparent and disclose if their marketing communications are funded by the entity whose product or services are being marketed. In addition, covered entities are required to provide individuals with a notice of privacy practices that describes the entity's privacy practices, the purposes for which it uses and discloses PHI, and the individual's privacy rights and how to exercise those rights. This transparency is an important protection that is particularly relevant as businesses seek to monetize health data.

At the same time, the HIPAA framework recognizes that health information is not a commodity, the flow of which is determined by the highest bidder. Great care was taken when establishing the HIPAA framework to balance various competing interests -- the privacy rights of the individual, the public interest served, the need for information to be used for essential health activities consistent with consumer expectations, and the burden on covered entities – and HHS repeatedly cited this balancing approach when it first issued its Privacy Rule[2] and in subsequent modifications to it. This same approach should be taken in addressing non-HIPAA health data.

Harmonization, including alignment with HIPAA concepts, definitions and standards, is critical to provide consumers with the assurance of consistent protection of all their health information, and to ensure the appropriate exchange of health information by health organizations, whether covered by HIPAA or not, is not impeded. For example, even as seemingly technical an issue as the definition of de-identified data could have potentially major ramifications if the HIPAA definition is not used. This is because data that is considered de-identified under HIPAA may not be considered de-identified under a new law and so potentially not covered by it. The unintended consequence of this is that it could seriously and adversely impact the ability of healthcare organizations to aggregate and share health data for important public policy purposes such as developing evidence-based standards, quality metrics and standards, medical research, and management of healthcare delivery, to name only a few.

The same can be said for other HIPAA definitions and concepts, including permissible uses and disclosures without explicit authorization, the requirement to be transparent

[2] See, for example, 65 Fed. Reg. 82462 (December 28, 2000) at 82464 ("The rule seeks to balance the needs of the individual with the needs of the society"); 82468 ("The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole"); 82471("Neither privacy, nor the important social goals described by the commenters, are absolutes. In this regulation, we are asking health providers and institutions to add privacy into the balance, and we are asking individuals to add social goals into the balance"); and 82472(" The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule").

about uses and disclosures in the form of a notice of privacy practices, and the right of individuals to access and receive portable copies of their electronic health records, among other things. Aligning any new legislation to govern non-HIPAA health data with the HIPAA definitions and requirements will also provide consumers with a more coherent and seamless privacy framework, allowing them to more easily understand how their health data is protected and exercise their privacy rights.

Equally important, security safeguards should be commensurate with the safeguards required by the HIPAA privacy and security standards. These require reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality of all protected health information, and the integrity and availability of electronic health information. Like the HIPAA Security Rule, any security standard should be technology neutral, scalable, and allow for a flexible risk-based approach. Robust security requirements for non-HIPAA health data are critical not only for large and sophisticated businesses that collect vast amounts of data, but also for smaller companies and start-ups developing new products and services, which should be incorporating security-by-design practices in their product development process. Whether their personal health data is covered by HIPAA or not, consumers should know that those to whom they entrust this data will keep it secure in accordance with well-vetted and accepted national security standards.

The Coalition strongly supports efforts to increase interoperability to facilitate the appropriate sharing of health data among healthcare organizations, as well as the access and availability of electronic health records to consumers themselves. This is another reason to ensure harmonization between laws governing PHI and non-HIPAA health data and to have national standards for health information privacy and security. The great promise of interoperability – using technology to engage patients, deliver meaningful insights to help in the identification and diagnosis of disease, and guide treatment decisions - depends on the ability to appropriately share health data among HIPAA covered entities and others for these purposes. This promise cannot come to fruition if these organizations are subject to, and constrained by, different standards that do not align or, potentially even conflict, with one another. This has proven to be a challenge for the appropriate sharing of patient substance use disorder information. The investment of effort at the outset when crafting legislation so as to avoid this type of misalignment will yield significant dividends in the form of improved healthcare outcomes and quality of care, not to mention a more seamless and workable privacy framework for veterans, healthcare organizations and service providers. This is particularly pertinent today as the Administration seeks to execute on the requirements of the 21st Century Cures Act to improve health information interoperability with the goal of promoting greater data sharing among patients, healthcare providers, payers, researchers, and other healthcare entities. As the Office of the National Coordinator of Health Information Technology stated in its recently released draft 2020-2025 Federal Health IT Strategic Plan:

[N]ew technologies, along with existing claims and EHR data, mean that the volume of health and health-related data being generated and available for improving care quality

has never been greater. Collecting, organizing, analyzing, interpreting, and applying this "big data" to clinical decision making is both a challenge and a significant opportunity.[3]

For the same reasons, as healthcare organizations make the transition to a nationwide, interoperable system of electronic health information, we believe it is essential to replace the current mosaic of sometimes conflicting state privacy laws, rules, and guidelines with strong, comprehensive national standards.

In closing, the HLC and Coalition commend the Subcommittee for seeking to address the challenges faced by the VA in managing veterans' health data in a world where the value of this data has never been greater, the risks posed to it more serious, or the opportunities for its beneficial use more abundant. We believe a balanced approach, compatible with and modeled upon the existing HIPAA framework, and that provides protections for non-HIPAA health data similar to that provided for PHI under HIPAA, is the best way to address these challenges and provide a comprehensive, consistent and transparent health information privacy framework for the health data of those in service and beyond.

Attachments

[3] See The Department of Health and Human Services Office of the National Coordinator of Health Information Technology document, 2020-2025 Federal Health IT Strategic Plan. January 2020

February 2020
Office for Civil Rights, U.S. Department of Health and Human Services
BULLETIN: HIPAA Privacy and Novel Coronavirus

In light of the Novel Coronavirus (2019-nCoV) outbreak, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is providing this bulletin to ensure that HIPAA covered entities and their business associates are aware of the ways that patient information may be shared under the HIPAA Privacy Rule in an outbreak of infectious disease or other emergency situation, and to serve as a reminder that the protections of the Privacy Rule are not set aside during an emergency.

The HIPAA Privacy Rule protects the privacy of patients' health information (protected health information) but is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes.

The U.S. Centers for Disease Control and Prevention (CDC) has advised: if you were in China within the past 14 days and feel sick with fever, cough, or difficulty breathing, you should get medical care. Call the office of your health care provider before you go and tell them about your travel and your symptoms. They will give you instructions on how to get care without exposing other people to your illness. While sick, avoid contact with people, don't go out and delay any travel to reduce the possibility of spreading illness to others. More information from the CDC available at: https://www.cdc.gov/coronavirus/2019-ncov/downloads/2019-ncov-factsheet.pdf.

Sharing Patient Information

Treatment Under the Privacy Rule, covered entities may disclose, without a patient's authorization, protected health information about the patient as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at 164.501.

Public Health Activities The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed protected health information without individual authorization:

- ***To a public health authority***, such as the CDC or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability. This would include, for example, the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR §§ 164.501 and 164.512(b)(1)(i). For example, a covered entity may disclose to the CDC protected health information on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have Novel Coronavirus (2019-nCoV).

- ***At the direction of a public health authority, to a foreign government agency*** that is acting in collaboration with the public health authority. See 45 CFR 164.512(b)(1)(i).
- ***To persons at risk*** of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations. See 45 CFR 164.512(b)(1)(iv).

Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification A covered entity may share protected health information with a patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care. A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death. This may include, where necessary to notify family members and others, the police, the press, or the public at large. See 45 CFR 164.510(b).

- The covered entity should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.
- For patients who are unconscious or incapacitated: A health care provider may share relevant information about the patient with family, friends, or others involved in the patient's care or payment for care, if the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. For example, a provider may determine that it is in the best interests of an elderly patient to share relevant information with the patient's adult child, but generally could not share unrelated information about the patient's medical history without permission.
- In addition, a covered entity may share protected health information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient's care, of the patient's location, general condition, or death. It is unnecessary to obtain a patient's permission to share the information in this situation if doing so would interfere with the organization's ability to respond to the emergency.

Disclosures to Prevent a Serious and Imminent Threat Health care providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct. See 45 CFR 164.512(j). Thus, providers may disclose a patient's health information to anyone who is in a position to prevent or lesson the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient's permission. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety. See 45 CFR 164.512(j).

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification In general, except in the limited circumstances described elsewhere in this Bulletin, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care

decisions for the patient). See 45 CFR 164.508 for the requirements for a HIPAA authorization. Where a patient has not objected to or restricted the release of protected health information, a covered hospital or other health care facility may, upon request, disclose information about a particular patient by name, may release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient's condition in general terms (*e.g.*, critical or stable, deceased, or treated and released). Covered entities may also disclose information if the patient is incapacitated, and if the disclosure is believed to be in the best interest of the patient and consistent with any prior expressed preferences of the patient. See 45 CFR 164.510(a).

Minimum Necessary For most disclosures, a covered entity must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.) Covered entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose, when that reliance is reasonable under the circumstances. For example, a covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have Novel Coronavirus (2019-nCoV) is the minimum necessary for the public health purpose. In addition, internally, covered entities should continue to apply their role-based access policies to limit access to protected health information to only those workforce members who need it to carry out their duties. See 45 CFR §§ 164.502(b), 164.514(d).

Safeguarding Patient Information

In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.

HIPAA Applies Only to Covered Entities and Business Associates

The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information. Business associates also include subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply.

Business Associates A business associate of a covered entity (including a business associate that is a subcontractor) may make disclosures permitted by the Privacy Rule, such as to a public health authority, on behalf of a covered entity or another business associate to the extent authorized by its business associate agreement.

Other Resources

For more information on HIPAA and Public Health, please visit:
https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html

For more information on HIPAA and Emergency Preparedness, Planning, and Response, please visit: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html

General information on understanding the HIPAA Privacy Rule may be found at:
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

For information regarding how Federal civil rights laws apply in an emergency, please visit:
https://www.hhs.gov/civil-rights/for-individuals/special-topics/emergency-preparedness/index.html

THE
NATIONAL LAW REVIEW

CA Attorney General Updates CCPA Proposed Regulations

Article By
Joseph J. Lazzarotti
Jason C. Gavejian
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- Corporate & Business Organizations

- California

Monday, February 10, 2020

Many businesses and their service providers have been awaiting final guidance from the California Attorney General concerning the California Consumer Privacy Act (CCPA). When news came last Friday of a regulatory update ("Update"), there may have been some initial disappointment that the Update did not announce final regulations, but only revisions to existing proposed regulations issued last year and a new comment period (ending February 24, instructions to submit comments here). However, while final regulations are still sometime away, initial disappointment may be softened by some of the Update's revisions.

Based on our initial review of the Update, below are some key changes to the proposed regulations:

- The Update would add guidance for interpreting defined terms under the CCPA. Specifically, the Update clarifies that determining whether information is "personal information" depends on whether the business maintains the information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or

indirectly, with a particular consumer or household." This guidance and the example provided below would address concerns many have regarding information businesses collect online.

For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

- The proposed regulations confirmed the requirement for online notices to be accessible, but the Update would require generally recognized industry standards be followed, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium.

- The proposed regulations provided businesses could not use personal information for "any purpose other than disclosed in the notice at collection." The Update would establish a less strict standard – "a purpose materially different than disclosed in the notice at collection."

- With regard to the contents of the notice at collection, the proposed regulations required (i) a list of the categories of personal information to be collected, and (ii) **for each category**, the business or commercial purposes for which it will be used. The Update would remove the requirement to list the purposes of use for each category. In other words, it appears it would be sufficient to list the business or commercial purposes for using all of the categories of personal information, not each one individually. This change would significantly simplify the notice at collection, and would be extended to the privacy policy as well.

- With regard to notices at collection for employment-related data, a "Do Not Sell My Personal Information" link would not be required. Additionally, the notice could link to the business's privacy policies for employees, applicants, etc., rather than consumers.

- The Update provides for an optional "Opt-Out Button."

- Proposed regulations required a two-step process for online requests to delete personal information. The Update would make that two-step process optional.

- With regard to the general requirement to make two or more designated methods available for submitting requests to know, the Update would relax the specific methods. At least one still must be a toll-free number. However, for website operators, the second need not be an interactive webform and could be an email address.

- The Update also tweaks the timing of certain notice requirements. For example, when confirming receipt of a request to delete or a right to know, the business would have 10 business days, while responses to such requests generally would be due in 45 calendar

- Under the Update, a business would not be required to search for personal information in response to a request to know if the business: (i) does not maintain personal information in a searchable or reasonable accessible format, (ii) maintains the personal information only for legal or compliance purposes, (iii) does not sell the information or use it for a commercial purpose, and (iv) describes to the consumer the categories of records not searched because it satisfied the three conditions above.

- The Update would clarify that service providers that receive requests to know or to delete either can respond on behalf of the business or inform the consumer that it cannot act on the request because it is a service provider.

Businesses still need to monitor the development of CCPA regulation, but the Update would seem to provide some clarity and/or relief on some points. Also, there is a new opportunity to voice concerns and pose questions concerning the guidance thus far.

Source URL: https://www.natlawreview.com/article/ca-attorney-general-updates-ccpa-proposed-regulations

Version 1.0

NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT

January 16, 2020

National Institute of Standards and Technology
U.S. Department of Commerce

Executive Summary

For more than two decades, the Internet and associated information technologies have driven unprecedented innovation, economic value, and improvement in social services. Many of these benefits are fueled by data about individuals that flow through a complex ecosystem. As a result, individuals may not be able to understand the potential consequences for their privacy as they interact with systems, products, and services. At the same time, organizations may not realize the full extent of these consequences for individuals, for society, or for their enterprises, which can affect their brands, their bottom lines, and their future prospects for growth.

Following a transparent, consensus-based process including both private and public stakeholders to produce this voluntary tool, the National Institute of Standards and Technology (NIST) is publishing this Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework), to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy. The Privacy Framework can support organizations in:

- Building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;[1]
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
- Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.

Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions. Like building a house, where homeowners make layout and design choices while relying on a well-engineered foundation, privacy protection should allow for individual choices, as long as effective privacy risk mitigations are already engineered into products and services. The Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends, such as artificial intelligence and the Internet of Things.

The Privacy Framework follows the structure of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [1] to facilitate the use of both frameworks together. Like the Cybersecurity Framework, the Privacy Framework is composed of three parts: Core, Profiles, and Implementation Tiers. Each component reinforces privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities.

- The Core enables a dialogue—from the executive level to the implementation/operations level—about important privacy protection activities and desired outcomes.
- Profiles enable the prioritization of the outcomes and activities that best meet organizational privacy values, mission or business needs, and risks.

[1] There is no objective standard for ethical decision-making; it is grounded in the norms, values, and legal expectations in a given society.

- Implementation Tiers support decision-making and communication about the sufficiency of organizational processes and resources to manage privacy risk.

In summary, the Privacy Framework is intended to help organizations build better privacy foundations by bringing privacy risk into parity with their broader enterprise risk portfolio.

Acknowledgements

This publication is the result of a collaborative effort between NIST and organizational and individual stakeholders in the public and private sectors. In developing the Privacy Framework, NIST has relied upon three public workshops, a request for information (RFI), a request for comment (RFC), five webinars, and hundreds of direct interactions with stakeholders.[2] NIST acknowledges and thanks all of those who have contributed to this publication.

[2] A complete development archive can be found at https://www.nist.gov/privacy-framework.

February 13, 2020

Confronting A Data Privacy Crisis, Gillibrand Announces Landmark Legislation To Create A Data Protection Agency

The Data Protection Act Would Create a Consumer Watchdog to Give Americans Control and Protection of Their Data, Promote a Competitive Digital Marketplace, and Prepare the U.S. for the Digital Age; U.S. Still One of the Only Democracies Without a Data Protection Agency

Washington, DC – U.S. Senator Kirsten Gillibrand today announced her landmark legislation, the *Data Protection Act*, which would create the Data Protection Agency (DPA), an independent federal agency that would protect Americans' data, safeguard their privacy, and ensure data practices are fair and transparent. The DPA will have the authority and resources to effectively enforce data protection rules—created either by itself or congress—and would be equipped with a broad range of enforcement tools, including civil penalties, injunctive relief, and equitable remedies. The DPA would promote data protection and privacy innovation across public and private sectors, developing and providing resources such as Privacy Enhancing Technologies (PETs) that minimize or even eliminate the collection of personal data. The U.S. is one of the only democracies, and the only member of the Organization for Economic Co-operation and Development (OECD), without a federal data protection agency.

Senator Gillibrand published a Medium post about her new legislation that can be **read here.**

"Technology is connecting us in new significant ways, and our society must be equipped for both the challenges and opportunities of a transition to the digital age. As the data privacy crisis looms larger over the everyday lives of Americans, the government has a responsibility to step forward and give Americans meaningful protection over their data and how it's being used," said **Senator Gillibrand**. *"Data has been called 'the new oil.' Companies are rushing to explore and refine it, ignoring regulations, putting profits above responsibility, and treating consumers as little more than dollar signs. Like the oil boom, little thought is being given to the long-term consequences. The U.S. needs a new approach to privacy and data protection. We cannot allow our freedoms to be trampled over by private companies that value profits over people, and the Data Protection Agency would do that with expertise and resources to create and meaningfully enforce data protection rules and digital rights."*

The agency will address a growing data privacy crisis in America. Massive amounts of personal information—public profiles, health data, photos, past purchases, locations, search histories, and much more—is being collected, processed, and in some cases, exploited by private companies and foreign adversaries. In some instances, the data was not given willingly, and in many others, consumers had little idea what they were signing up for. As a result, the data of everyday Americans is being parsed, split, and sold to the highest bidder, and there is little anyone--including the federal government--can do about it. Not only have these tech companies built major empires and made billions from selling Americans' data, but they spend millions of dollars per year opposing new regulations.

In recent years, major data breaches have occurred at banks, credit rating agencies and tech firms. In 2017, Equifax failed to safeguard the sensitive credit data of hundreds of millions of Americans, allowing a foreign government to steal

and expose this information. In 2018, Facebook exposed the personal information of nearly 50 million users because it reportedly ignored warnings from its own employees about a dangerous loophole in its security. Additionally, the Federal Trade Commission (FTC) has failed to enforce its own orders and has failed to act on dozens of detailed consumer privacy complaints alleging unfair practices concerning data collection, marketing to children, cross-device tracking, consumer profiling, user tracking, discriminatory business practices, and data disclosure to third-parties.

The Data Protection Agency explained:

The DPA would be an executive agency. The director would be appointed by the president and confirmed by the Senate, serves a 5-year term, and must have knowledge in technology, protection of personal data, civil rights, law, and business. The agency may investigate, subpoena for testimony or documents, and issue civil investigative demands. It may prescribe rules and issue orders and guidance as is necessary to carry out federal privacy laws. The authority of state agencies and state attorneys general are preserved in the Act.

The DPA would have three core missions:

1. Give Americans control and protection over their own data by creating and enforcing data protection rules.

- The agency would enforce privacy statutes and rules around data protection, either as authorized by Congress or themselves. It would use a broad range of tools to do so, including civil penalties, injunctive relief, and equitable remedies.
- The agency would also take complaints, conduct investigations, and inform the public on data protection matters. So if it seems like a company like Tinder is doing bad things with your data, the Data Protection Agency would have the authority to launch an investigation and share findings.

2. Maintain the most innovative, successful tech sector in the world by ensuring fair competition within the digital marketplace.

- The agency would promote data protection and privacy innovation across sectors, developing and providing resources such as Privacy Enhancing Technologies (PETs) that minimize or even eliminate the collection of personal data.
- The agency would ensure equal access to privacy protection and protect against "pay-for-privacy" or "take-it-or-leave-it" provisions in service contracts—because privacy, including online privacy, is a right that should be enforced.

3. Prepare the American government for the digital age.

- The agency would advise Congress on emerging privacy and technology issues, like deepfakes and encryption. It would also represent the United States at international forums regarding data privacy and inform future treaty agreements regarding data.

The Data Protection Act of 2020 has been endorsed by leading technology, privacy, and civil rights organizations including:

- **Electronic Privacy Information Center (EPIC)**

"The US confronts a privacy crisis. Our personal data is under assault. Congress must establish a data protection agency. Senator Gillibrand has put forward a bold, ambitious proposal to safeguard the privacy of Americans."- Caitriona Fitzgerald, Policy Director, EPIC.

- **Shoshana Zuboff, Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School**

"The Data Protection Act of 2020 by Senator Gillibrand offers a crucial bulwark against the pervasive assault on privacy that now disfigures every aspect of daily life. An overwhelming majority of Americans now think that the rampant commercial collection of personal data poses more risks than benefits, even as

there is little choice but to depend upon privacy-destroying commercial systems for effective social participation. With this Bill, Senator Gillibrand joins a history-making new wave of legislative and regulatory efforts in the US and Europe that promise to assert democratic governance over commerce in the digital age. Senator Gillibrand's leadership is critical as we embark on the pivotal decade ahead." – Shoshana Zuboff, Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School.

- **Public Citizen**

"It's no longer possible for individuals to protect themselves from intrusive online surveillance and manipulation. The FTC's response to even the most egregious privacy violations has been tepid, and so it is past time to invest in a new agency expert in how data is used and abused. As corporations gobble up more and more data as part of their day-to-day operations, we need a watchdog on the beat to stop them from breaking the law, and to provide meaningful consequences when they do. Along with new privacy laws that protect individual access to courts and don't scuttle the importance of the states, having a DPA is necessary to protect consumers in the digital age." - Robert Weissman, President, Public Citizen.

- **Color of Change**

"Current privacy laws give free rein to companies to exploit Black people's data, replicating and amplifying racial and economic injustices in the process. Senator Gillibrand's bill will advance civil rights protections for Black communities, and allow us to begin to take back our privacy in an era of unregulated big data. Federal oversight with the resources and authority to hold companies accountable to data protection obligations and tackle emerging privacy challenges is the key to ensuring our safety online." - Brandi Collins-Dexter, Senior Campaign Director, Color Of Change.

- **Consumer Federation of America**

"We support this legislation because protecting our privacy is a big job and we need an agency with the responsibility, resources and resolve to do it." - Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America.

- **U.S PIRG**

"Senator Gillibrand's proposal for a strong Data Protection Agency recognizes that consumers need a tough, independent cop to protect their data and their privacy. The FTC is not that agency." - Ed Mierzwinski, Senior Director for Consumer Programs, U.S. PIRG.

- **Center for Digital Democracy**

"Americans are losing more of their privacy daily. It is wrong to assume, as industry likes us to believe, that individual consumers can manage their privacy in a world of non-stop surveillance. It is time we had 21st century safeguards in place. That is why we need a strong and independent data protection agency that will place the interests of consumers, and those most disadvantaged, ahead of the companies that regularly take all of our information and exploit us. The FTC has totally failed to protect the public for many years—regardless of which party has been in power. We applaud Senator Gillibrand's proposal, which if enacted, could help ensure that our digital rights are protected in the U.S." - Katharina Kopp, Ph.D., Deputy Director, Director of Policy, Center for Digital Democracy.

- **Consumer Action**

"As data violations occur at warp speed and with impunity, consumers need an agency that makes data protection its primary mission. Senator Gillibrand's plan to create a Data Protection Agency is the right step to ensure that companies use

individuals' data fairly, responsibly and with accountability." - Linda Sherry, Director of National Priorities, Consumer Action.

- **Campaign for a Commercial-Free Childhood**

"The FTC has stood idly by while big tech companies have preyed upon children and families with an unfair business model based on illegal data collection and manipulative personalized marketing. Violations of the Children's Online Privacy Protection Act are rampant as everyone, from major platforms to small developers, ignores the law. We applaud Senator Gillibrand for her legislation which would create a new COPPA cop to rein in the blatant and widespread misuse of kids' personal data." - Josh Golin, Executive Director, Campaign for a Commercial-Free Childhood.

- **Parent Coalition for Student Privacy**

"We endorse this important bill that takes the protection of our children's personal data out of the hands of the FTC, which has proven itself incapable of ensuring their privacy, and into the hands of a new federal agency which will be empowered to enforce the law, respond to parents' complaints when their children's privacy is put at risk, and analyze the potentially discriminatory impacts of current data practices." - Leonie Haimson, Co-chair, Parent Coalition for Student Privacy

- **Professor Anita L. Allen, Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania Law School**

"It is critical that Americans' personal data and communications finally be protected through the coordinated expertise of a dedicated federal agency." - Professor Anita L. Allen, Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania Law School

- **Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School**

"Data centers in the U.S. are vulnerable to attack, and as a country we need to do a much better job with data security. That's why the U.S. needs a data protection agency." - Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School.

- **Professor Francesca Bignami, Leroy Sorenson Merrifield Research Professor of Law, The George Washington University Law School**

"Just like 19th-century Americans got a federal regulatory agency to curb the power of the railway magnates, 21st-century Americans deserve one to tackle the problems of the tech industry. This Data Protection Agency is a vital step for protecting privacy and liberty in today's digital economy." - Professor Francesca Bignami, Leroy Sorenson Merrifield Research Professor of Law, The George Washington University Law School

The full text of the legislation may be found here.

BROOKINGS

Report

Why protecting privacy is a losing game today—and how to change the game

Cameron F. Kerry Thursday, July 12, 2018

Summary

Recent congressional hearings and data breaches have prompted more legislators and business leaders to say the time for broad federal privacy legislation has come. Cameron Kerry presents the case for adoption of a baseline framework to protect consumer privacy in the U.S.

Kerry explores a growing gap between existing laws and an information Big Bang that is eroding trust. He suggests that recent privacy bills have not been ambitious enough, and points to the Obama administration's Consumer Privacy Bill of Rights as a blueprint for future legislation. Kerry considers ways to improve that proposal, including an overarching "golden rule of privacy" to ensure people can trust that data about them is handled in ways consistent with their interests and the circumstances in which it was collected.

Table of Contents

There is a classic episode of the show "I Love Lucy" in which Lucy goes to work wrapping candies on an assembly line. The line keeps speeding up with the candies coming closer together and, as they keep getting farther and farther behind, Lucy and her sidekick Ethel scramble harder and harder to keep up. "I think we're fighting a losing game," Lucy says.

This is where we are with data privacy in America today. More and more data about each of us is being generated faster and faster from more and more devices, and we can't keep up. It's a losing game both for individuals and for our legal system. If we don't change the rules of the game soon, it will turn into a losing game for our economy and society.

More and more data about each of us is being generated faster and faster from more and more devices, and we can't keep up. It's a losing game both for individuals and for our legal system.

The Cambridge Analytica drama has been the latest in a series of eruptions that have caught peoples' attention in ways that a steady stream of data breaches and misuses of data have not.

The first of these shocks was the Snowden revelations in 2013. These made for long-running and headline-grabbing stories that shined light on the amount of information about us that can end up in unexpected places. The disclosures also raised awareness of how much can be learned from such data ("we kill people based on metadata," former NSA and CIA Director Michael Hayden said).

The aftershocks were felt not only by the government, but also by American companies, especially those whose names and logos showed up in Snowden news stories. They faced suspicion from customers at home and market resistance from customers overseas. To rebuild trust, they pushed to disclose more about the volume of surveillance demands and for changes in surveillance laws. Apple, Microsoft, and Yahoo all engaged in public legal battles with the U.S. government.

Then came last year's Equifax breach that compromised identity information of almost 146 million Americans. It was not bigger than some of the lengthy roster of data breaches that preceded it, but it hit harder because it rippled through the financial system and affected individual consumers who never did business with Equifax directly but nevertheless had to deal with the impact of its credit scores on economic life. For these people, the breach was another demonstration of how much important data about them moves around without their control, but with an impact on their lives.

Now the Cambridge Analytica stories have unleashed even more intense public attention, complete with live network TV cut-ins to Mark Zuckerberg's congressional testimony. Not only were many of the people whose data was collected surprised that a company they never heard of got so much personal information, but the Cambridge Analytica story touches on all the controversies roiling around the role of social media in the cataclysm of the 2016 presidential election. Facebook estimates that Cambridge Analytica was able to leverage its "academic" research into data on some 87 million Americans (while before the 2016 election Cambridge Analytica's CEO Alexander Nix boasted of having profiles with 5,000 data points on 220 million Americans). With over two billion Facebook users worldwide, a lot of people have a stake in this issue and, like the Snowden stories, it is getting intense attention around the globe, as demonstrated by Mark Zuckerberg taking his legislative testimony on the road to the European Parliament.

The Snowden stories forced substantive changes to surveillance with enactment of U.S. legislation curtailing telephone metadata collection and increased transparency and safeguards in intelligence collection. Will all the hearings and public attention on Equifax and Cambridge Analytica bring analogous changes to the commercial sector in America?

I certainly hope so. I led the Obama administration task force that developed the "Consumer Privacy Bill of Rights" issued by the White House in 2012 with support from both businesses and privacy advocates, and then drafted legislation to put this bill of rights into law. The legislative proposal issued after I left the government did not get much traction, so this initiative remains unfinished business.

The Cambridge Analytica stories have spawned fresh calls for some federal privacy legislation from members of Congress in both parties, editorial boards, and commentators. With their marquee Zuckerberg hearings behind them, senators and congressmen are moving on to think about what do next. Some have already introduced bills and others are thinking about what privacy proposals might look like. The op-eds and Twitter threads on what to do have flowed. Various groups in Washington have been convening to develop proposals for legislation.

This time, proposals may land on more fertile ground. The chair of the Senate Commerce Committee, John Thune (R-SD) said "many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing." A number of companies have been increasingly open to a discussion of a basic federal privacy law. Most notably, Zuckerberg told CNN "I'm not sure we shouldn't be regulated," and Apple's Tim Cook expressed his emphatic belief that self-regulation is no longer viable.

For a while now, events have been changing the way that business interests view the prospect of federal privacy legislation.

This is not just about damage control or accommodation to "techlash" and consumer frustration. For a while now, events have been changing the way that business interests view the prospect of federal privacy legislation. An increasing spread of state legislation on net neutrality, drones, educational technology, license plate readers, and other subjects and, especially broad new legislation in California pre-empting a ballot initiative, have made the possibility of a single set of federal rules across all 50 states look attractive. For multinational companies that have spent two years gearing up for compliance with the new data protection law that has now taken effect in the EU, dealing with a comprehensive U.S. law no longer looks as daunting. And more companies are seeing value in a common baseline that can provide people with reassurance about how their data is handled and protected against outliers and outlaws.

This change in the corporate sector opens the possibility that these interests can converge with those of privacy advocates in comprehensive federal legislation that provides effective protections for consumers. Trade-offs to get consistent federal rules that preempt some strong state laws and remedies will be difficult, but with a strong enough federal baseline, action can be achievable.

Snowden, Equifax, and Cambridge Analytica provide three conspicuous reasons to take action. There are really quintillions of reasons. That's how fast IBM estimates we are generating digital information, *quintillions* of bytes of data every day—a number followed by 30 zeros. This explosion is generated by the doubling of computer processing power every 18-24 months that has driven growth in information technology throughout the computer age, now compounded by the billions of devices that collect and transmit data, storage devices and data centers that make it cheaper and easier to keep the data from these devices, greater bandwidth to move that data faster, and more powerful and sophisticated software to extract information from this mass of data. All this is both enabled and magnified by the singularity of network effects—the value that is added by being connected to others in a network—in ways we are still learning.

This information Big Bang is doubling the volume of digital information in the world every two years. The data explosion that has put privacy and security in the spotlight will accelerate. Futurists and business forecasters debate just how many tens of billions of devices will be connected in the coming decades, but the order of magnitude is unmistakable—and staggering in its impact on the quantity and speed of bits of information moving around the globe. The pace of change is dizzying, and it will get even faster—far more dizzying than Lucy's assembly line.

Most recent proposals for privacy legislation aim at slices of the issues this explosion presents. The Equifax breach produced legislation aimed at data brokers. Responses to the role of Facebook and Twitter in public debate have focused on political ad disclosure, what to do about bots, or limits to online tracking for ads. Most state legislation has targeted specific topics like use of data from ed-tech products, access to social media accounts by employers, and privacy protections from drones and license-plate readers. Facebook's simplification and expansion of its privacy controls and recent federal privacy bills in reaction to events focus on increasing transparency and consumer choice. So does the newly enacted California Privacy Act.

This information Big Bang is doubling the volume of digital information in the world every two years. The data explosion that has put privacy and security in the spotlight will accelerate. Most recent proposals for privacy legislation aim at slices of the issues this explosion presents.

Measures like these double down on the existing American privacy regime. The trouble is, this system cannot keep pace with the explosion of digital information, and the pervasiveness of this information has undermined key premises of these laws in ways that are increasingly glaring. Our current laws were designed to address collection and storage of structured data by government, business, and other organizations and are busting at the seams in a world where we are all connected and constantly sharing. It is time for a more comprehensive and ambitious approach. We need to think bigger, or we will continue to play a losing game.

Our existing laws developed as a series of responses to specific concerns, a checkerboard of federal and state laws, common law jurisprudence, and public and private enforcement that has built up over more than a century. It began with the famous Harvard Law Review article by (later) Justice Louis Brandeis and his law partner Samuel Warren in 1890 that provided a foundation for case law and state statutes for much of the 20th Century, much of which addressed the impact of mass media on individuals who wanted, as Warren and Brandeis put it, "to be let alone." The advent of mainframe computers saw the first data privacy laws adopted in 1974 to address the power of information in the hands of big institutions like banks and government: the federal Fair Credit Reporting Act that gives us access to information on credit reports and the Privacy Act that governs federal agencies. Today, our checkerboard of privacy and data security laws covers data that concerns people the most. These include health data, genetic information, student records and

information pertaining to children in general, financial information, and electronic communications (with differing rules for telecommunications carriers, cable providers, and emails).

Outside of these specific sectors is not a completely lawless zone. With Alabama adopting a law last April, all 50 states now have laws requiring notification of data breaches (with variations in who has to be notified, how quickly, and in what circumstances). By making organizations focus on personal data and how they protect it, reinforced by exposure to public and private enforcement litigation, these laws have had a significant impact on privacy and security practices. In addition, since 2003, the Federal Trade Commission—under both Republican and Democratic majorities—has used its enforcement authority to regulate unfair and deceptive commercial practices and to police unreasonable privacy and information security practices. This enforcement, mirrored by many state attorneys general, has relied primarily on deceptiveness, based on failures to live up to privacy policies and other privacy promises.

These levers of enforcement in specific cases, as well as public exposure, can be powerful tools to protect privacy. But, in a world of technology that operates on a massive scale moving fast and doing things because one can, reacting to particular abuses after-the-fact does not provide enough guardrails.

As the data universe keeps expanding, more and more of it falls outside the various specific laws on the books. This includes most of the data we generate through such widespread uses as web searches, social media, e-commerce, and smartphone apps. The changes come faster than legislation or regulatory rules can adapt, and they erase the sectoral boundaries that have defined our privacy laws. Take my smart watch, for one example: data it generates about my heart rate and activity is covered by the Health Insurance Portability and Accountability Act (HIPAA) if it is shared with my doctor, but not when it goes to fitness apps like Strava (where I can compare my performance with my peers). Either way, it is the same data, just as sensitive to me and just as much of a risk in the wrong hands.

As the data universe keeps expanding, more and more of it falls outside the various specific laws on the books.

It makes little sense that protection of data should depend entirely on who happens to hold it. This arbitrariness will spread as more and more connected devices are embedded in everything from clothing to cars to home appliances to street furniture. Add to that striking changes in patterns of business integration and innovation—traditional telephone providers like Verizon and AT&T are entering entertainment, while startups launch into the provinces of financial institutions like currency trading and credit and all kinds of enterprises compete for space in the autonomous vehicle ecosystem—and the sectoral boundaries that have defined U.S. privacy protection cease to make any sense.

Putting so much data into so many hands also is changing the nature of information that is protected as private. To most people, "personal information" means information like social security numbers, account numbers, and other information that is unique to them. U.S. privacy laws reflect this conception by aiming at "personally identifiable information," but data scientists have repeatedly demonstrated that this focus can be too narrow. The aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them. The result is that today, a widening range of data has the potential to be personal information, i.e. to identify us uniquely. Few laws or regulations address this new reality.

Nowadays, almost every aspect of our lives is in the hands of some third party somewhere. This challenges judgments about "expectations of privacy" that have been a major premise for defining the scope of privacy protection. These judgments present binary choices: if private information is somehow public or in the hands of a third party, people often are deemed to have no expectation of privacy. This is particularly true when it comes to government access to information—emails, for example, are nominally less protected under our laws once they have been stored 180 days or more, and articles and activities in

plain sight are considered categorically available to government authorities. But the concept also gets applied to commercial data in terms and conditions of service and to scraping of information on public websites, for two examples.

As more devices and sensors are deployed in the environments we pass through as we carry on our days, privacy will become impossible if we are deemed to have surrendered our privacy simply by going about the world or sharing it with any other person. Plenty of people have said privacy is dead, starting most famously with Sun Microsystems' Scott McNealy back in the 20th century ("you have zero privacy ... get over it") and echoed by a chorus of despairing writers since then. Without normative rules to provide a more constant anchor than shifting expectations, true privacy actually could be dead or dying. The Supreme Court may have something to say on the subject in we will need a broader set of norms to protect privacy in settings that have been considered public. Privacy can endure, but it needs a more enduring foundation.

The Supreme Court in its recent *Carpenter* decision recognized how constant streams of data about us change the ways that privacy should be protected. In holding that enforcement acquisition of cell phone location records requires a warrant, the Court considered the "detailed, encyclopedic, and effortlessly compiled" information available from cell service location records and "the seismic shifts in digital technology" that made these records available, and concluded that people do not necessarily surrender privacy interests to collect data they generate or by engaging in behavior that can be observed publicly. While there was disagreement among Justices as to the sources of privacy norms, two of the dissenters, Justice Alito and Gorsuch, pointed to "expectations of privacy" as vulnerable because they can erode or be defined away.

How this landmark privacy decision affects a wide variety of digital evidence will play out in criminal cases and not in the commercial sector. Nonetheless, the opinions in the case point to a need for a broader set of norms to protect privacy in settings that have been thought to make information public. Privacy can endure, but it needs a more enduring foundation.

Our existing laws also rely heavily on notice and consent—the privacy notices and privacy policies that we encounter online or receive from credit card companies and medical providers, and the boxes we check or forms we sign. These declarations are what provide the basis for the FTC to find deceptive practices and acts when companies fail to do what they said. This system follows the model of informed consent in medical care and human subject research, where consent is often asked for in person, and was imported into internet privacy in the 1990s. The notion of U.S. policy then was to foster growth of the internet by avoiding regulation and promoting a "market resolution" in which individuals would be informed about what data is collected and how it would be processed, and could make choices on this basis.

Maybe informed consent was practical two decades ago, but it is a fantasy today. In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't.

It is not simply that any particular privacy policies "suck," as Senator John Kennedy (R-LA) put it in the Facebook hearings. Zeynep Tufecki is right that these disclosures are obscure and complex. Some forms of notice are necessary and attention to user experience can help, but the problem will persist no matter how well designed disclosures are. I can attest that writing a simple privacy policy is challenging, because these documents are legally enforceable and need to explain a variety of data uses; you can be simple and say too little or you can be complete but too complex. These notices have some useful function as a statement of policy against which regulators, journalists, privacy advocates, and even companies themselves can measure performance, but they are functionally useless for most people, and we rely on them to do too much.

Maybe informed consent was practical two decades ago, but it is a fantasy today. In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't.

At the end of the day, it is simply too much to read through even the plainest English privacy notice, and being familiar with the terms and conditions or privacy settings for all the services we use is out of the question. The recent flood of emails about privacy policies and consent forms we have gotten with the coming of the EU General Data Protection Regulation have offered new controls over what data is collected or information communicated, but how much have they really added to people's understanding? Wall Street Journal reporter Joanna Stern attempted to analyze all the ones she received (enough paper printed out to stretch more than the length of a football field), but resorted to scanning for a few specific issues. In today's world of constant connections, solutions that focus on increasing transparency and consumer choice are an incomplete response to current privacy challenges.

Moreover, individual choice becomes utterly meaningless as increasingly automated data collection leaves no opportunity for any real notice, much less individual consent. We don't get asked for consent to the terms of surveillance cameras on the streets or "beacons" in stores that pick up cell phone identifiers, and house guests aren't generally asked if they agree to homeowners' smart speakers picking up their speech. At best, a sign may be posted somewhere announcing that these devices are in place. As devices and sensors increasingly are deployed throughout the environments we pass through, some after-the-fact access and control can play a role, but old-fashioned notice and choice become impossible.

Ultimately, the familiar approaches ask too much of individual consumers. As the President's Council of Advisers on Science and Technology Policy found in a 2014 report on big data, "the conceptual problem with notice and choice is that it fundamentally places the burden of privacy protection on the individual," resulting in an unequal bargain, "a kind of market failure."

This is an impossible burden that creates an enormous disparity of information between the individual and the companies they deal with. As Frank Pasquale ardently dissects in his "Black Box Society," we know very little about how the businesses that collect our data operate. There is no practical way even a reasonably sophisticated person can get arms around the data that they generate and what that data says about them. After all, making sense of the expanding data universe is what data scientists do. Post-docs and Ph.D.s at MIT (where I am a visiting scholar at the Media Lab) as well as tens of thousands of data researchers like them in academia and business are constantly discovering new information that can be learned from data about people and new ways that businesses can —or do—use that information. How can the rest of us who are far from being data scientists hope to keep up?

As a result, the businesses that use the data know far more than we do about what our data consists of and what their algorithms say about us. Add this vast gulf in knowledge and power to the absence of any real give-and-take in our constant exchanges of information, and you have businesses able by and large to set the terms on which they collect and share this data.

Businesses are able by and large to set the terms on which they collect and share this data. This is not a "market resolution" that works.

This is not a "market resolution" that works. The Pew Research Center has tracked online trust and attitudes toward the internet and companies online. When Pew probed with surveys and focus groups in 2016, it found that "while many Americans are willing to share personal information in exchange for tangible benefits, they are often cautious about disclosing their information and frequently unhappy about that happens to that information once companies have collected it." Many people are "uncertain, resigned, and annoyed." There is a growing body of survey research in the same vein. Uncertainty, resignation, and annoyance hardly make a recipe for a healthy and sustainable marketplace, for trusted brands, or for consent of the governed.

Consider the example of the journalist Julia Angwin. She spent a year trying to live without leaving digital traces, which she described in her book "Dragnet Nation." Among other things, she avoided paying by credit card and established a fake identity to get a card for when she couldn't avoid using one; searched hard to find encrypted cloud services for most email; adopted burner phones that she turned off when not in use and used very little; and opted for paid subscription services in place of ad-supported ones. More than a practical guide to protecting one's data privacy, her year of living anonymously was an extended piece of performance art demonstrating how much digital surveillance reveals about our lives and how hard it is to avoid. The average person should not have to go to such obsessive lengths to ensure that their identities or other information they want to keep private stays private. We need a fair game.

As policymakers consider how the rules might change, the Consumer Privacy Bill of Rights we developed in the Obama administration has taken on new life as a model. The Los Angeles Times, The Economist, and The New York Times all pointed to this bill of rights in urging Congress to act on comprehensive privacy legislation, and the latter said "there is no need to start from scratch ..." Our 2012 proposal needs adapting to changes in technology and politics, but it provides a starting point for today's policy discussion because of the wide input it got and the widely accepted principles it drew on.

The bill of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission: individual control, transparency, respect for the context in which the data was obtained, access and accuracy, focused collection, security, and accountability. These broad principles are rooted in longstanding and globally-accepted "fair information practices principles." To reflect today's world of billions of devices interconnected through networks everywhere, though, they are intended to move away from static privacy notices and consent forms to a more dynamic framework, less focused on collection and process and more on how people are protected in the ways their data is handled. Not a checklist, but a toolbox. This principles-based approach was meant to be interpreted and fleshed out through codes of conduct and case-by-case FTC enforcement—iterative evolution, much the way both common law and information technology developed.

As policymakers consider how the rules might change, the Consumer Privacy Bill of Rights developed in the Obama administration has taken on new life as a model. The bill of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission.

The other comprehensive model that is getting attention is the EU's newly effective General Data Protection Regulation. For those in the privacy world, this has been the dominant issue ever since it was approved two years ago, but even so, it was striking to hear "the GDPR" tossed around as a running topic of congressional questions for Mark Zuckerberg. The imminence of this law, its application to Facebook and many other American multinational companies, and its contrast with U.S. law made GDPR a hot topic. It has many people wondering why the U.S. does not have a similar law, and some saying the U.S. should follow the EU model.

I dealt with the EU law since it was in draft form while I led U.S. government engagement with the EU on privacy issues alongside developing our own proposal. Its interaction with U.S. law and commerce has been part of my life as an official, a writer and speaker on privacy issues, and a lawyer ever since. There's a lot of good in it, but it is not the right model for America.

There's a lot of good in the GDPR, but it is not the right model for America.

What is good about the EU law? First of all, it is a law—one set of rules that applies to all personal data across the EU. Its focus on individual data rights in theory puts human beings at the center of privacy practices, and the process of complying with its detailed requirements has forced companies to take a close look at what data they are collecting, what they use it for, and how they keep it and share it—which has proved to be no small task. Although the EU regulation is rigid in numerous respects, it can be more subtle than is apparent at first glance. Most notably, its requirement that consent be explicit and freely given is often presented in summary reports as prohibiting collecting any personal data without consent; in fact, the regulation allows other grounds for collecting data and one effect of the strict definition of consent is to put more emphasis on these other grounds. How some of these subtleties play out will depend on how 40 different regulators across the EU apply the law, though. European advocacy groups were already pursuing claims against "*les GAFAM*" (Google, Amazon, Facebook, Apple, Microsoft) as the regulation went into effect.

The EU law has its origins in the same fair information practice principles as the Consumer Privacy Bill of Rights. But the EU law takes a much more prescriptive and process-oriented approach, spelling out how companies must manage privacy and keep records and including a "right to be forgotten" and other requirements hard to square with our First Amendment. Perhaps more significantly, it may not prove adaptable to artificial

intelligence and new technologies like autonomous vehicles that need to aggregate masses of data for machine learning and smart infrastructure. Strict limits on the purposes of data use and retention may inhibit analytical leaps and beneficial new uses of information. A rule requiring human explanation of significant algorithmic decisions will shed light on algorithms and help prevent unfair discrimination but also may curb development of artificial intelligence. These provisions reflect a distrust of technology that is not universal in Europe but is a strong undercurrent of its political culture.

We need an American answer—a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy. The Consumer Privacy Bill of Rights offers a blueprint for such an approach.

Sure, it needs work, but that's what the give-and-take of legislating is about. Its language on transparency came out sounding too much like notice-and-consent, for example. Its proposal for fleshing out the application of the bill of rights had a mixed record of consensus results in trial efforts led by the Commerce Department.

It also got some important things right. In particular, the "respect for context" principle is an important conceptual leap. It says that a people "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." This breaks from the formalities of privacy notices, consent boxes, and structured data and focuses instead on respect for the individual. Its emphasis on the interactions between an individual and a company and circumstances of the data collection and use derives from the insight of information technology thinker Helen Nissenbaum. To assess privacy interests, "it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."

We need an American answer—a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy.

Context is complicated—our draft legislation listed 11 different non-exclusive factors to assess context. But that is in practice the way we share information and form expectations about how that information will be handled and about our trust in the handler. We bare our souls and our bodies to complete strangers to get medical care, with the understanding that this information will be handled with great care and shared with strangers only to the extent needed to provide care. We share location information with ride-sharing and navigation apps with the understanding that it enables them to function, but Waze ran into resistance when that functionality required a location setting of "always on." Danny Weitzner, co-architect of the Privacy Bill of Rights, recently discussed how the respect for context principle "would have prohibited [Cambridge Analytica] from unilaterally repurposing research data for political purposes" because it establishes a right "not to be surprised by how one's personal data issued." The Supreme Court's *Carpenter* decision opens up expectations of privacy in information held by third parties to variations based on the context.

The Consumer Privacy Bill of Rights does not provide any detailed prescription as to how the context principle and other principles should apply in particular circumstances. Instead, the proposal left such application to case-by-case adjudication by the FTC and development of best practices, standards, and codes of conduct by organizations outside of government, with incentives to vet these with the FTC or to use internal review boards similar to those used for human subject research in academic and medical settings. This approach was based on the belief that the pace of technological change and the enormous variety of circumstances involved need more adaptive decisionmaking than current approaches to legislation and government regulations allow. It may be that baseline

legislation will need more robust mandates for standards than the Consumer Privacy Bill of Rights contemplated, but any such mandates should be consistent with the deeply embedded preference for voluntary, collaboratively developed, and consensus-based standards that has been a hallmark of U.S. standards development.

In hindsight, the proposal could use a lodestar to guide the application of its principles—a simple golden rule for privacy: that companies should put the interests of the people whom data is about ahead of their own. In some measure, such a general rule would bring privacy protection back to first principles: some of the sources of law that Louis Brandeis and Samuel Warren referred to in their famous law review article were cases in which the receipt of confidential information or trade secrets led to judicial imposition of a trust or duty of confidentiality. Acting as a trustee carries the obligation to act in the interests of the beneficiaries and to avoid self-dealing.

A Golden Rule of Privacy that incorporates a similar obligation for one entrusted with personal information draws on several similar strands of the privacy debate. Privacy policies often express companies' intention to be "good stewards of data;" the good steward also is supposed to act in the interests of the principal and avoid self-dealing. A more contemporary law review parallel is Yale law professor Jack Balkin's concept of "information fiduciaries," which got some attention during the Zuckerberg hearing when Senator Brian Schatz (D-HI) asked Zuckerberg to comment on it. The Golden Rule of Privacy would import the essential duty without importing fiduciary law wholesale. It also resonates with principles of "respect for the individual," "beneficence," and "justice" in ethical standards for human subject research that influence emerging ethical frameworks for privacy and data use. Another thread came in Justice Gorsuch's *Carpenter* dissent defending property law as a basis for privacy interests: he suggested that entrusting someone with digital information may be a modern equivalent of a "bailment" under classic property law, which imposes duties on the bailee. And it bears some resemblance to the GDPR concept of "legitimate interest," which permits the processing of personal data based on a legitimate interest of the processor, provided that this interest is not outweighed by the rights and interests of the subject of the data.

The fundamental need for baseline privacy legislation in America is to ensure that individuals can trust that data about them will be used, stored, and shared in ways that are consistent with their interests and the circumstances in which it was collected. This should hold regardless of how the data is collected, who receives it, or the uses it is put to. If it is personal data, it should have enduring protection.

The fundamental need for baseline privacy legislation in America is to ensure that individuals can trust that data about them will be used, stored, and shared in ways that are consistent with their interests and the circumstances in which it was collected.

Such trust is an essential building block of a sustainable digital world. It is what enables the sharing of data for socially or economically beneficial uses without putting human beings at risk. By now, it should be clear that trust is betrayed too often, whether by intentional actors like Cambridge Analytica or Russian "Fancy Bears," or by bros in cubes inculcated with an imperative to "deploy or die."

Trust needs a stronger foundation that provides people with consistent assurance that data about them will be handled fairly and consistently with their interests. Baseline principles would provide a guide to all businesses and guard against overreach, outliers, and outlaws. They would also tell the world that American companies are bound by a widely-accepted set of privacy principles and build a foundation for privacy and security practices that evolve with technology.

Resigned but discontented consumers are saying to each other, "I think we're playing a losing game." If the rules don't change, they may quit playing.

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

Report Produced by **Center for Technology Innovation**

Attachment 6

Are Our Privacy Laws Asking Too Much of Consumers and Too Little of Businesses?

12/13/2019

In the last few weeks in the US, Democrats and Republicans from the Senate Commerce Committee have each released draft comprehensive federal privacy legislation bills, and there is a considerable amount of overlap between them. In the Committee's recent hearing the two sides appeared closer than ever to a bipartisan compromise on a privacy bill. But despite this potential breakthrough, it's important that lawmakers take the necessary time to ensure they get this groundbreaking legislation right before it becomes law.

In our complex data-driven society, privacy laws will not be able to provide effective privacy protections if they continue to be rooted in notice and choice. That model no longer scales to our near-constant interactions with data, and it has proven to be a failure for a variety of reasons. Unfortunately, lawmakers appear to be doubling down on the outmoded individual control paradigm of privacy that many experts have deemed ineffective. California's Consumer Privacy Act (CCPA) features notice and choice as its main protection, and most proposed privacy bills at the federal and state levels in recent months have done the same. But, with only one comprehensive state privacy law on the books, and an unsettled federal privacy landscape, there still is time to direct the US privacy approach towards one that will protect and empower individuals more effectively. An accountability-based model, which places the burden on organizations, not individuals, to prevent privacy harms, delivers far stronger privacy protections.

Of course, the logic behind notice and consent appears sound enough: companies provide individuals information about how their personal data will be used to empower them to make informed decisions, and individuals choose whether to consent to handing over their data based on that information. It may have served us well for a while, but at this stage it is time to abandon this approach. In fact, many privacy regulators and experts from civil society and academia have come to recognize that the notice and consent model of privacy protection is no longer workable. For example, FTC Commissioner Rebecca Slaughter has repeatedly outlined the limitations of notice and consent in her speeches and testimony. Similarly Professor Woodrow Hartzog noted in his testimony before the Senate Commerce Committee in February that "notice and consent has failed." Consent places an immense burden on individuals to protect themselves and understand what is happening with their data, and they simply cannot make informed decisions in each and every one of the countless daily online interactions involving their personal information. The sheer volume of personal data collected, inferred, used and shared in the digital economy makes this impossible.

opt-out of the sale of personal information, and requires consumers to inform themselves and act upon that information to protect themselves. While it certainly provides Californians with some new privacy protections not provided by existing U.S. laws, it ultimately asks too much of individuals while ignoring available tools that are better-suited for providing effective protections. Similarly, several federal proposals such as Rep. DelBene's Information Transparency and Personal Data Control Act and Rep. Eshoo's and Lofgren's recently-introduced Online Privacy Act of 2019 rely on notice and consent as their primary method to protect consumer privacy. Similarly, the two most recent bills by Senator Cantwell and Senator Wicker make notice and consent (both opt-in and opt out) a prominent feature in the protections they provide.

Effective privacy protections cannot be based upon the premise that consumers know what they're consenting to (or failing to consent to) when all research shows that they aren't actually reading privacy policies. And simply improving notice and consent mechanisms (for example through shorter, easy to understand pop-up notices) is not the answer either. Such improvements, though laudable, cannot address the consent fatigue caused by the onslaught of privacy notices and consent requests. In the context of cookie notices, which have become more detailed and prominent since the introduction of the GDPR, we have seen that consumers are likely to accept the terms just to get a pop-up off their screen, especially when they show up again and again. Consumers are tired of these notices and just want the content they're trying to access. Indeed, when the choice is between accepting the terms or not gaining access to the service, is that choice even meaningful?

This is not to say that there is no role for notice and choice in future privacy laws. But it must be limited to where it is truly meaningful - perhaps in the context of sharing some types of highly sensitive data for a purpose unrelated to that for which it was collected, such as a pharmacy selling customer information to a lifestyle brand. But for the vast majority of information uses, privacy laws should include different and superior requirements that would actually result in empowering individuals and delivering more effective protections for their data and privacy.

- **Enhanced User-Centric Transparency** - Ensuring that individuals have visibility into what data is being collected on them and how it's being used is essential for engendering trust in the digital economy and creating accountability. Appropriate disclosures and information should absolutely remain a priority for both lawmakers drafting privacy laws and companies using personal data. Organizations must be transparent not only about what information they collect and how they use and share it, but also about the accountability mechanisms they employ to protect consumers from harm and, importantly, what rights individuals have and they can obtain redress when harm occurs. Privacy policies must also provide sufficient information to regulators about organizations' data practices so that they can be evaluated and enforced against. Thus, transparency has an important role beyond just enabling consent.

- **Individual rights** – Appropriate access, correction, deletion and portability rights empower individuals and give them control over their personal data without undermining organizations ability to work with data. These rights have already been enshrined in the GDPR and, to some extent, the CCPA, and should be adapted to the US context in any new legislation. In addition, individual empowerment can be significantly safeguarded through improved complaint-handling requirements and redress rights for individuals who have experienced privacy harms. Combined with the other accountability-based obligations described in this article that would shift the primary burden of protecting privacy on organizations, this approach would reduce the constant pressure on individuals to make ex ante guesses about what choices will protect them and replaces it with effective and efficient remedies if something does go wrong.

- **A Risk- and Harm-Based Approach** - Privacy laws should require organizations to focus on preventing privacy harms to individuals by identifying the potential risks of their data uses and removing or mitigating them through appropriate mechanisms and tools such as anonymization, de-identification, appropriate use limitations, effective redress mechanisms, and employing privacy by design. This approach puts individuals at the center of an organization's information management practices and results in better protection for individuals, particularly in instances where consent is neither effective nor feasible. Significant modern privacy laws such as the EU GDPR and the Brazil LGPD already incorporate obligatory risk assessments, including through requirements to conduct formal Data Protection Impact Assessments (DPIAs) in certain contexts, also known more generally as Privacy Impact Assessments.

benefits to the organization or a third party are not outweighed by the interests and risks of harm to individuals. This ground for processing is one of the several co-equal grounds for processing both in the EU GDPR and the Brazilian LGPD (with consent being another one). Including a legitimate interest ground for processing in a US law would provide a formal mechanism for organizations to process data for beneficial purposes as long as they have demonstrably mitigated any risks to individuals. This mechanism requires organizations to consider, in advance, whether processing is likely to result in injury, unfairness or discrimination to individuals, and thus ensures organizations are considering impacts to individuals in their decision-making process. It would also enable responsible data uses where other grounds (like consent) are ineffective and unavailable, such as in the case of previously unanticipated uses of data like in the context of big data analytics and AI and machine learning. To ensure legal certainty and accountability, regulatory guidance could define the risks and harms that would have to be avoided, as well as establish appropriate methodologies for assessing and weighing the involved risks and benefits.

- **Fair Processing** – Fair processing is a separate data protection principle in many privacy laws around the world. The US FTC Act also includes a variant of this principle by prohibiting unfair business practices, including in the context of using personal data. While "fairness" has been difficult to define, spelling out parameters for fair processing presents another vehicle for requiring organizations to focus on the impact of their data uses and to prevent harm, including discrimination. Thus, any new privacy law should include appropriate fair processing requirements, potentially as further defined through regulatory guidance.

- **Accountability** – All major modern privacy laws (GDPR, Brazil's LGDP, India's draft privacy law, etc.) require companies to have comprehensive privacy management and compliance programs. This is often referred to as "organizational accountability." In fact, this should be a core component of any modern privacy law as it will provide the structure and processes required for compliance and delivering effective protections to individuals. Such accountability-based privacy programs would include all of the above and other measures to address all key elements of accountability: leadership and oversight; risk assessment; written policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement (e.g. complaint handling). Indeed, through its privacy consent orders, the US FTC has also embraced organizational accountability mediated through comprehensive privacy programs. See, for example, the recent FTC consent orders against FB and Equifax, imposing strong accountability-based privacy compliance programs. Of course, the specifics of these programs can and must be tailored and scaled to the size and nature of the organization and the way in which it uses personal data.

Some have noted that an accountability and risk-based privacy framework places too much faith in companies to do the right thing. But with clear substantive rules set forth both in the law or through regulations and guidelines (defining, for example, the harms that must be prevented), coupled with rigorous enforcement by the Federal Trade Commission, state attorneys general, and possibly even consumers in some instances, companies will have to implement strong privacy practices.

The U.S. might be the only first world country without a comprehensive privacy law, but that means it can learn from and improve upon the laws other countries have put into place. Doubling down on what's proven to be an ineffective notice and consent regime won't result in a privacy law that gives consumers the protections they need and will result in unnecessary impediments to effective and beneficial uses of personal data. To deliver strong privacy protections and enable innovation, we need a framework that empowers consumers beyond consent through a range of accountability measures that place the burden of protecting individuals against actual harms on the organizations that process personal data.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Comments are closed.

Search

Archives

December 2019

Categories

All
Accountability
Data Processing
Individual Rights
Legitimate Interest
Transparency
US Privacy

RSS Feed

CIPL Accountability Q&A

This document addresses some commonly asked questions about the concept of organizational accountability in data protection.

1. What is "accountability"?
2. What is "accountability" not?
3. What must organizations do to be "accountable"?
4. What are the core elements of accountability?
5. What specifically do the core elements of accountability require of companies?
6. How does the risk-based approach to privacy relate to accountability?
7. Is accountability enforceable?
8. Accountability is in the GDPR – is it a foreign concept to US law?
9. Is accountability just another way of saying "comply with the law"?
10. How can organizations implement and demonstrate accountability?
11. Is accountability only feasible for large organizations with lots of resources?
12. What formal accountability schemes are available to help companies be accountable?
13. How does accountability benefit companies?
14. How does accountability benefit individuals?
15. How does accountability help privacy enforcement authorities?
16. What benefits do formal accountability schemes, such as CBPRs, offer?
17. Why should lawmakers and regulators provide companies with incentives to be accountable?

1. What is "accountability"?

- **Accountability is globally recognized as a key building block for effective privacy and data protection regulation**. It requires organizations to implement a comprehensive privacy program governing all aspects of collecting and using personal information and to be able to verify and demonstrate the existence and effectiveness of such programs internally (to Board and senior level management) and externally on request (to privacy enforcement authorities, individuals and business partners).

- **Accountability gives effect to legal requirements and data privacy laws**. Having a comprehensive privacy program in place is the foundation for compliance with all applicable privacy obligations established by law, regulation or other standard. The specific core elements of accountability-based privacy programs, such as risk assessment, ensure ongoing privacy compliance and that the program remains current when technologies and business practices change over time.

- **Accountability delivers "corporate digital responsibility" fit for the 21st century and modern data driven economies**. It ensures effective protection for individuals and their data and enables digital trust and responsible use, sharing and flows of data. Moreover, accountability provides the tools for protecting personal information and places the responsibility of doing so on organizations that use such information, while also facilitating appropriate individual choice and control over such information.

2. What is "accountability" not?

- **Accountability is not self-regulation**. Rather, it operationalizes and translates principles-based legal rules into concrete policies, procedures, controls and governance to deliver compliance. It sits on top of and is in addition to other legal requirements – it does not replace them. Because laws that include accountability may be principles-based (rather than being overly detailed), they enable the adaptation of such principles to specific industry sectors and differing levels of risk, either through additional guidance by a regulator or by companies themselves through risk assessments and other accountability tools, as appropriate.

- **Accountability is also not a "carte blanche" or free pass to use data in any way an organization wants**. It requires organizations to be thoughtful about uses of data, to implement all applicable data protection requirements (including risk assessments and appropriate mitigations) and to be able to demonstrate that implementation. Accountability demands that organizations commit to acting responsibly in respect of both the use and protection of data.

- **Accountability is not a self-serving concept pushed by industry**. Accountability provides significant benefits for privacy enforcement authorities, individuals and society.

- **Accountability is not an excuse for when things go wrong**. It minimizes the risk of non-compliance and prepares organizations to be responsive and responsible when data incidents do occur. Demonstrated accountability can serve as a mitigating factor in enforcement but it does not give organizations a get out of jail free card and is fully enforceable.

3. What must organizations do to be "accountable"?

Accountability requires organizations to:

- Implement within the company a comprehensive privacy program covering all core elements of accountability that enables compliance with applicable laws, regulations or industry standards;

- Verify the effectiveness and delivery of such a privacy program and ensure continuous improvement; and

- Be able to demonstrate the existence and effectiveness of such a program internally (to Board and senior level management) and externally on request (to regulators, business partners and individuals).

4. What are the core elements of accountability?

- The core elements of accountability are: leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement.

- A privacy law typically addresses each of these elements in some fashion. Ideally, the law will provide enough flexibility for a company to tailor each of these elements to their specific risks and requirements through their own risk assessment processes that are part of their accountability-based privacy programs.

- Even in the absence of a law, organizations can create privacy programs that incorporate and address each of the core elements of accountability and implement such programs as a matter of corporate policy and practice.

CIPL Accountability Wheel Demonstrating the Essential Elements of Accountability

5. What specifically do the core elements of accountability require of companies?

Companies must take concrete steps to establish policies, procedures and controls that apply the above core elements of accountability to the collection, use, sharing and any other processing and protection of personal information. These include:

- **Establishing leadership and oversight for data protection and the responsible use of data**, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's accountability program and report to management and the board.

- **Assessing and mitigating the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology and other factors and adapting the program to changing levels of risk.

- **Establishing internal written policies and procedures** that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards as well as the organization's values and goals.

- **Providing transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, the rights of individuals in relation to their data and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners and third parties about the organization's privacy program.

- **Providing training for employees** to ensure awareness of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.

- **Monitoring and verifying the implementation and effectiveness of the program and internal compliance** with the overall privacy program, policies, procedures and controls through regular internal or external audits and redress plans**.**

- **Implementing response and enforcement procedures** to address inquiries, complaints, data protection breaches and internal non-compliance, and to enforce against acts of non-compliance.

6. How does the risk-based approach to privacy relate to accountability?

- An effective privacy law must be risk based. That means that companies must be required to assess the risks of harm to individuals associated with their proposed information uses, weigh them against the desired benefits of the uses and devise appropriate measures to reduce or eliminate such risks as much as possible. Understanding the risks of their specific information uses allows companies to create more effective protections against the actual risks at hand.

- The risk-based approach also enables companies to prioritize and calibrate their compliance and accountability measures specifically to their context as opposed to engaging in one-size-fits-all and potentially wasteful and unnecessary compliance activities. This approach increases privacy protections for individuals and maximizes the productivity of available compliance dollars in companies in areas where the risk is higher.

- Risk assessment and the risk-based approach to privacy compliance is a core element of accountability. Organizations must build, implement and calibrate their privacy program based on risk to individuals, as well as the risk to organizations from non-compliance. As such, accountability and the risk-based approach to privacy go hand in hand.

7. Is accountability enforceable?

- Yes. Accountability is enforceable. Where a law requires accountability, the absence of a verifiable and demonstrated privacy program or any demonstrable policies and procedures for complying with the legal requirements in that law would be an enforceable violation in and of itself, even if no other violation occurred. Thus, accountability requires that organizations have a comprehensive internal compliance program that they can demonstrate on request.

- Even in the absence of formal requirements to have privacy programs, most privacy enforcement authorities now expect responsible companies that handle personal data to have comprehensive internal programs governing their information uses in place. In an investigation or enforcement context, such authorities will look to whether the company has implemented such a program.

- Many privacy frameworks and data protection laws have incorporated accountability as a matter of basic obligation or best practice and provide the means to enforce the requirement. Further, the U.S. Federal Trade Commission in its enforceable consent decrees requires, when relevant, that companies implement the full range of accountability measures through privacy programs and mandated periodic audits to verify compliance.

8. Accountability is in the GDPR – is it a foreign concept to US law?

- No. Accountability is one of the "Fair Information Practices Principles", which is guidance for data governance developed in the United States in the 1970s that has formed the basis for law, regulation and international agreements governing privacy, data protection and data flows, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework. Since the early 2000's policymakers, data privacy enforcement authorities, experts, companies and advocates have engaged in an effort – led by policymakers and experts in the United States – to further define and describe how accountability can be relied on to protect data in a way that takes into account the realities of 21st century data technologies, business models, collection and use.

- As noted above, in the U.S., the FTC has traditionally spelled out many of accountability's key features through its consent decrees. Practically every consent decree resulting from an FTC privacy case has included a requirement to establish and implement a written privacy and security program, with many of these incorporating the essential elements of organizational accountability. [1]

- Moreover, the elements of accountability have been relied on in other areas of U.S. corporate law and compliance, including anti-corruption, white-collar crime and corporate fraud, anti-money laundering, healthcare, export control and competition law. U.S. organizations, regulators and courts have used these elements to determine whether an organization has maintained an effective and comprehensive compliance program in any given regulatory area.[2]

- Finally, accountability is also a core component of the APEC Cross-border Privacy Rules (CBPR) system, which was developed through an international process in which the United States was a key player.

9. Is accountability just another way of saying "comply with the law"?

No. Accountability is a framework that enables organizations to implement governance, policies, procedures and controls that enable legal compliance, give effect to high-level legal principles and requirements and protect data and individuals. In addition, while accountability's first goal is to deliver compliance, it also drives privacy practices beyond legal compliance to incorporate additional protections that are based on a company's additional policies and ethical considerations. Thus, it accomplishes two principal objectives:

- It requires companies to implement a comprehensive and demonstrable program that enables them to comply with the full range of applicable privacy requirements, consistent with the size of their business and nature of information uses.

- It promotes a general culture of privacy that may go above and beyond what is required by law and incorporate additional considerations of best practice, consumer interest, fairness and business ethics where appropriate.

10. How can organizations implement and demonstrate accountability?

- Accountability can be implemented within organizations through a variety of mechanisms. Organizations can implement their own custom-made internal policies and programs tailored to their company's size, structure and data processing activities. In addition, organizations may also participate in formal accountability schemes involving some form of third party review and approval, which help to demonstrate accountability, such as Binding Corporate Rules (BCRs), APEC Cross-border Privacy Rules (CBPRs), APEC Privacy Recognition for Processors (PRPs), ISO standards or other privacy certifications that set forth specific requirements.

- Such formal accountability schemes can help companies of all sizes (including micro-enterprises and SMEs) meet relevant legal and accountability requirements without developing their own custom-made program. They also enable organizations to readily demonstrate accountability and their program to regulators, business partners, clients and individuals.

- Organizations can also take advantage of officially recognized enforceable codes of conduct that may be developed by trade associations or professional organizations in the future.

11. Is accountability only feasible for large organizations with lots of resources?

- No. Accountability is a scalable concept that can be implemented by organizations of all sizes. The risk-based approach, which is a key component of accountability, means that organizations must build their program to address the relevant risks they face. Smaller companies handling smaller amounts of personal data will not need to build a program to the degree that a large multinational company would.

12. What formal accountability schemes are available to help companies be accountable?

Companies seeking a formal accountability scheme instead of, or in addition to, a custom-made internal program have a range of options. These include:

- Binding Corporate Rules (BCRs)
- APEC Cross-border Privacy Rules (CBPRs)
- APEC Privacy Recognition for Processors (PRPs)
- The U.S. Privacy Shield
- ISO Standards
- Third party certification programs
- Recognized codes of conduct

13. How does accountability benefit companies?

Accountability benefits companies by:

- Requiring them to establish comprehensive internal privacy programs designed to achieve compliance with all relevant legal requirements, other external standards and/or company-specific privacy goals;
- Helping them to demonstrate legal compliance to privacy enforcement authorities and business partners;
- Acting as a mitigating factor in enforcement actions or in the setting of fines by demonstrating good faith efforts to comply with the law and to deal with data responsibly;
- Promoting more effective privacy protections by requiring organizations to set program priorities based on risk and to define and implement mitigation measures based on risk;
- Fostering a culture of internal privacy compliance within the company and constructive engagement with privacy enforcement authorities;
- Generating trust with the public and with privacy enforcement authorities that the organization is processing personal data responsibly, thereby enhancing brand and reputation;
- Enabling organizations to better harmonize their privacy policies and practices with the requirements of the various jurisdictions in which they do business;
- Enabling organizations to engage in broader beneficial uses of personal data, including research for the public social good and AI and machine learning, by minimizing the risks of new data uses and requiring companies to demonstrate responsible data use to data privacy enforcement authorities;
- Providing legal certainty with regard to cross-border data protection when implemented through recognized accountability frameworks, such as the CBPR;
- Serving as a due diligence tool for data controllers (companies that control the collection and use of personal information) by identifying qualified and accountable data processors, service providers or vendors that are certified under formal accountability schemes, such as the CBPR and PRP; and
- Improving the overall level of privacy behaviors of organizations which creates a network of companies with mature and responsible privacy practices across the data marketplace and ecosystem.

14. How does accountability benefit individuals?

Accountability delivers real and effective protections for individuals and their data. Specifically, accountability:

- Assures individuals that companies are complying with the law and enhances their trust in organizations' use of their data;
- Shifts the burden of protecting individuals more explicitly to organizations and away from individuals;
- Addresses "consent fatigue" caused by excessive reliance on "individual control" and "consent" requests by providing for alternative mechanisms (e.g. risk assessments; transparency; redress) that more effectively protect individuals in many contexts.
- Ensures that individuals' data is protected even when it is transferred across borders;
- Helps individuals decide whether to give their personal information to organizations by making accountability a benchmark for that decision; and
- Makes enforcement of privacy laws more effective both within the U.S. and across borders.

15. How does accountability help privacy enforcement authorities?

Accountability provides benefits to privacy enforcement authorities by:

- Reducing the oversight, complaint-handling and enforcement burdens of privacy enforcement authorities through the overall enhanced privacy practices of companies and by involving approved third parties to carry out some of the oversight and complaint-handling tasks in the context of formal accountability schemes, such as the CBPR or other privacy certifications or codes of conduct;
- Allowing privacy enforcement authorities to be selective and strategic in their enforcement decisions in light of their limited resources;
- Enabling them to engage in a positive and constructive way with accountable companies;
- Streamlining investigations and enforcement by requiring companies to document their internal privacy programs and decision-making and to be able to demonstrate these to privacy enforcement authorities on request;
- Creating a more uniform data protection environment that streamlines investigations and enforcement actions, including across borders; and
- Encouraging a data protection race to the top rather than to the bottom.

16. What benefits do formal accountability schemes, such as CBPRs, offer?

- Independent from the benefit they may have as cross-border transfer mechanisms in some jurisdictions, formal accountability schemes, such as Binding Corporate Rules (BCRs), APEC CBPRs, APEC PRPs, codes of conduct or certifications and ISO standards can benefit companies that may not have the resources or expertise to independently devise fully-fledged internal privacy programs without the assistance of a third party. By meeting the requirements of these mechanisms, companies establish within their organizations the conditions necessary to be accountable and set themselves up to successfully comply with applicable privacy laws or standards.

- As these schemes are formally recognized by data privacy enforcement authorities or laws, these mechanisms offer companies the legal certainty necessary to process personal information lawfully and with confidence.

- In addition, these formal accountability mechanisms foster trust with data privacy enforcement authorities and individuals.

17. Why should lawmakers and regulators provide companies with incentives to be accountable?

- Accountability provides many concrete benefits to all stakeholders – companies, privacy enforcement authorities and individuals. Many of the benefits to companies (e.g. enabling data driven innovation, providing a reputational advantage and generating trust), as well as the risk of enforcement, will motivate companies to properly implement accountability throughout their organization. However, given its critical importance to the digital economy, lawmakers and privacy enforcement authorities should provide specific additional incentives that encourage companies to adopt accountability measures and reward those that invest in privacy and accountability.

- Such incentives could include recognizing demonstrated accountability or participation in formal accountability schemes (e.g. CBPR and other privacy certifications) as mitigating factors in enforcement contexts or in the setting of fines, or recognizing participation in such accountability schemes as evidence of due diligence when selecting third party processors or vendors to whom it is safe to transfer personal information.

- Providing incentives for companies to be accountable will speed its adoption and promote the benefits of accountability that accrue to companies, individuals and data privacy enforcement authorities as well as generally raise the level of compliance and accountability across the digital economy.

If you would like to discuss this Q&A in more detail or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.

Additionally, for more detailed information on accountability, please see CIPL's white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society"[3] and "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability".[4]

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 77 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/.

References

[1] Organizational Accountability in Light of FTC Consent Orders, 13 November 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf.

[2] Organizational Accountability - Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law, 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_-_existence_in_us_regulatory_compliance_and_its_relevance_for_a_federal_data_privacy_law__3_july_2019.pdf.

[3] The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

[4] Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

THE
NATIONAL LAW REVIEW

OCR Comments on Recent Ciox Case Vacating Certain Omnibus Rule Regulations and Guidance Relating to Fees for Providing Patient Records

Robinson+Cole
Article By
Melissa Lisa Thompson
Robinson & Cole LLP
Health Law Diagnosis

- Health Law & Managed Care
- Communications, Media & Internet
- Litigation / Trial Practice

- All Federal
- District of Columbia

Wednesday, January 29, 2020

The HHS Office for Civil Rights (OCR) issued an *Important Notice Regarding Individuals' Right of Access to Health Records* through its email list serve on January 29, 2020. In the Notice, OCR addressed the recent memorandum Opinion issued in *Ciox Health v. Azar, et al,* No. 18-cv-00040 (D.D.C. January 23, 2020).

In that case, Ciox Health, LLC, a specialized medical records provider, had challenged certain provisions of the 2013 Omnibus Rule, including provisions pertaining to what can be charged for delivering records containing protected health information (PHI). One issue was whether the limitations on fees for these services applied only to requests for PHI that are made by the patient, for use by the patient (the Patient Rate) or whether the limitations also applied to PHI to be delivered to third parties.

An OCR guidance document published in 2016 (the 2016 Guidance) stated the Patient Rate would apply to patient requests, even where the requests directed the delivery of PHI to third parties. The 2016 Guidance noted that the Patient Rate would not apply to requests being made by a third party pursuant to a HIPAA authorization signed by the patient, but cautioned against circumventing the fee

limit by treating individual requests for access like other HIPAA disclosures, such as by having an individual fill out a HIPAA authorization when the individual requests access to PHI, including directing a copy to a third party. The 2016 Guidance also described the types of labor costs recoverable, and identified methods for calculating the Patient Rate. The case additionally challenged a regulation in the 2013 Omnibus Rule that required PHI sent to the third parties be provided in the form and format requested by the patient, if readily producible in that form and format.

The Court ruled in favor of OCR on one of the issues — holding that identifying the methods for calculating the Patient Rate was not a reviewable final agency action.

The Court vacated — and declared unlawful the "Patient Rate expansion" in the 2016 Guidance and the Omnibus Rule's "mandate broadening PHI delivery to third parties regardless of format." The Court held:

(1) HHS's 2013 rule compelling delivery of PHI to third parties regardless of the records' format is arbitrary and capricious insofar as it goes beyond the statutory requirements set by Congress; (2) HHS's broadening of the Patient Rate in 2016 is a legislative rule that the agency failed to subject to notice and comment in violation of the APA; and finally, (3) HHS's 2016 explanation concerning what labor costs can be recovered under the Patient Rate is an interpretative rule that HHS was not required to subject to notice and comment.

The Court cited to the HITECH Act, noting that it is silent on the allowable fees for PHI when an individual requests or directs the information be provided to a third party and, instead, restricts the fee to labor costs for "*providing such individual*" a copy of the information.

As OCR explained in its recent Notice, as a result of the Court's ruling, "the fee limitation set forth at 45 C.F.R. § 164.524(c)(4) will apply only to an individual's request for access to their own records, and does not apply to an individual's request to transmit records to a third party." OCR cautioned, however, that the right of individuals to access their own records and the fee limitations that apply in that context "are undisturbed and remain in effect" and that OCR will "continue to enforce the right of access provisions in 45 C.F.R. § 164.524 that are not restricted by the court order."

Source URL: https://www.natlawreview.com/article/ocr-comments-recent-ciox-case-vacating-certain-omnibus-rule-regulations-and-guidance