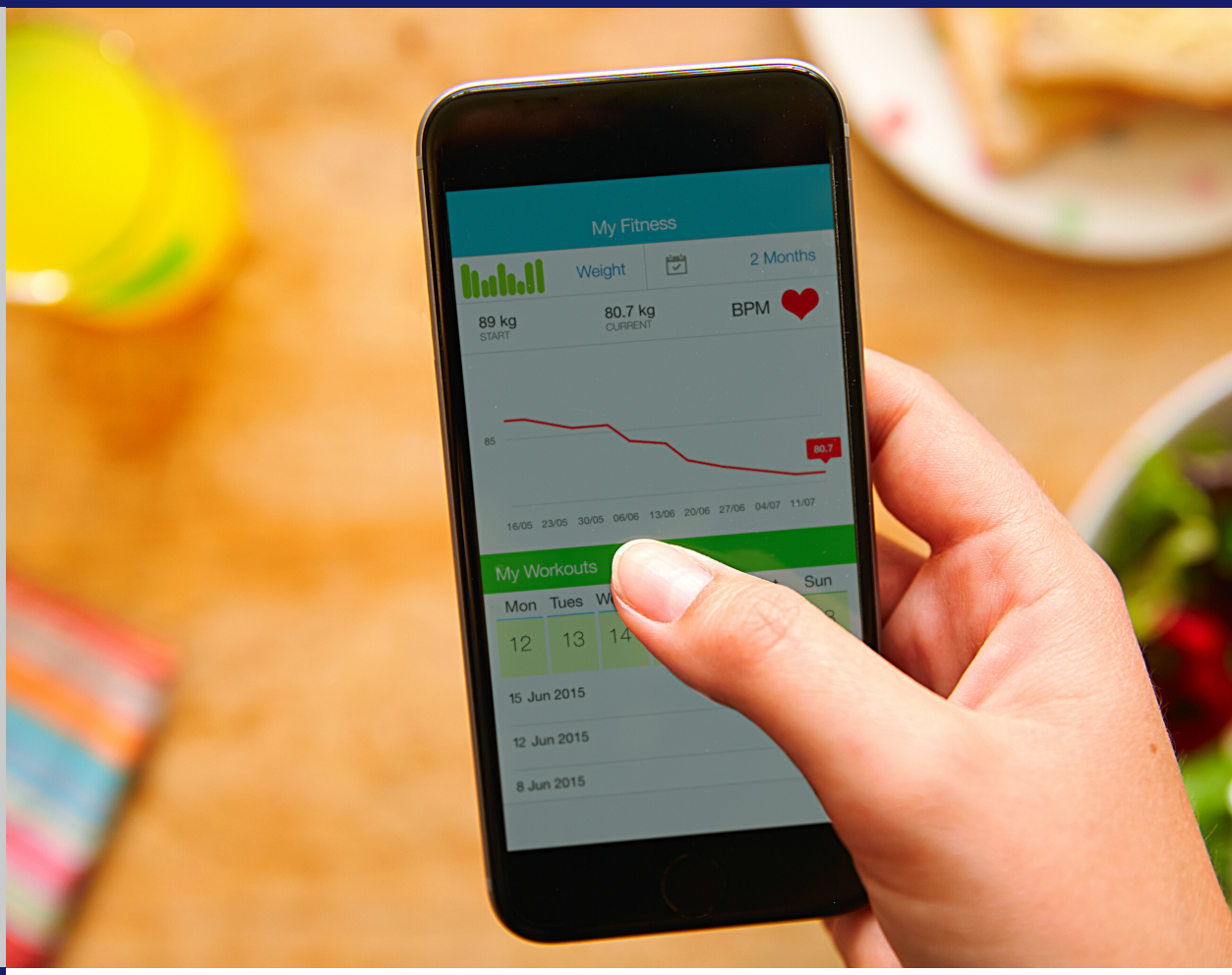
The Case for Accountability:

Protecting Health Data Outside the Healthcare System



PREPARED BY

Alice Leiter
Vice President & Senior Counsel

WITH SUPPORT FROM

Robert Wood Johnson Foundation

Table of Contents

Introduction

Every day the line between “health data” and “consumer data” is further blurred. It used to be that health data was held near-exclusively by the healthcare system – hospitals, doctors, clinics, and health insurers. But with the explosive proliferation of digital technologies – first the internet, and later consumer-facing apps, connected fitness and health tracking devices, and web-based platforms – an ever-increasing amount of health data is generated by consumers themselves, and both held and used by companies that are not bound by the obligations of the Health Insurance Portability and Accountability Act (HIPAA), the nation’s primary health privacy law.

About seven percent of searches on Google are health-related,[1] and in 2020, the top health searches unrelated to coronavirus included questions such as “how long does the flu last,” “what is HPV, ”and “what causes kidney stones.”[2] The degree to which these searches are personally sensitive depends on the individual, but many users turn to the Internet for information related not only to their medical conditions but also to their sexual preferences, mental health, and substance use. Further, some 64 percent of patients in a recent survey said they use a mobile health app to manage their health.[3]

Combining these statistics makes the staggering amount of health data stored digitally abundantly clear, but unfortunately these vast troves of valuable, sensitive health data are currently woefully under-protected by our federal legal and regulatory regime. Since the early 2000s, when HIPAA’s implementing regulations went into effect, only information collected by hospitals, insurers, doctors and clinics is covered by HIPAA and its subsequently implemented Privacy and Security rules. Most other health data stored digitally remains largely under protected and under regulated.

Digital health information, and the collection and sharing of it, is key to both individuals’ engagement in their own health and care, and in promoting care-coordination to support value-based care. But the privacy risks associated with such widespread data storage and transmission cannot remain unaddressed.

The Consumer Privacy Framework for Health Data

It was in this context of outdated privacy models that Executives for Health Innovation (EHI, formerly the eHealth Initiative) and the Center for Democracy & Technology (CDT) developed the *Consumer Privacy Framework for Health Data* (hereinafter "the Framework"), made possible by the generous support of the Robert Wood Johnson Foundation (RWJF).[4] In an effort to address the current gaps in legal protections, the Framework outlines how all types of health-related data should be used, accessed, and disclosed. Historically, many privacy models have placed too much emphasis on individuals consenting to the use of and access to their health data and company notifications. These outdated privacy models have failed to protect consumers and meaningfully inform them about how their data would actually be used.

The Framework involves a detailed set of data use limits; covers all information that can be used to make inferences or judgments about a person's physical or mental health by virtue of a broad definition of "consumer health information;" and applies to all non-HIPAA-covered entities that collect, disclose, or use consumer health information, regardless of the size or business model of the covered entity.

With a second round of funding from RWJF, CDT has been evaluating the Framework's standards through a health equity lens, culminating in a report titled, *Placing Equity at the Center of Health Care & Technology* (hereinafter "Equity Report").[5] This paper explores in depth the disproportionate impact that data misuse and biased algorithms in data analytics can have on vulnerable and marginalized populations. It is these particular risks that underscore the need for greater data protections that can not only mitigate but prevent harms, lending both credibility and urgency to the accountability proposal detailed below.

Creating Accountability Through a Private Sector Program

A central goal of the Framework is to advance a proposal with more significant impact on shoring up consumer privacy protections than existing laws, codes of conduct, or sets of best practices. Inherent in that goal is meaningful accountability for misuse of consumer health data by non-HIPAA-covered entities. Although it appears unlikely that new comprehensive federal privacy legislation is on the near-term horizon, continued and recent enforcement actions indicate that harmful data practices surrounding consumer health data show no signs of slowing. While we wait for federal action, we believe it is critical for the private sector to implement data use accountability standards based on those set forth in the Framework. As such, the Framework proposes that the data use standards, and entities' adherence to them, be governed by a new independent private-sector regulatory program.

Numerous codes of conduct and best practices have been released in recent years.[6] These are all well-intentioned and often quite meaningful in theory. But, in practice, there is no regular or consistent accountability to their provisions, even if a company "signs on" to comply with them.

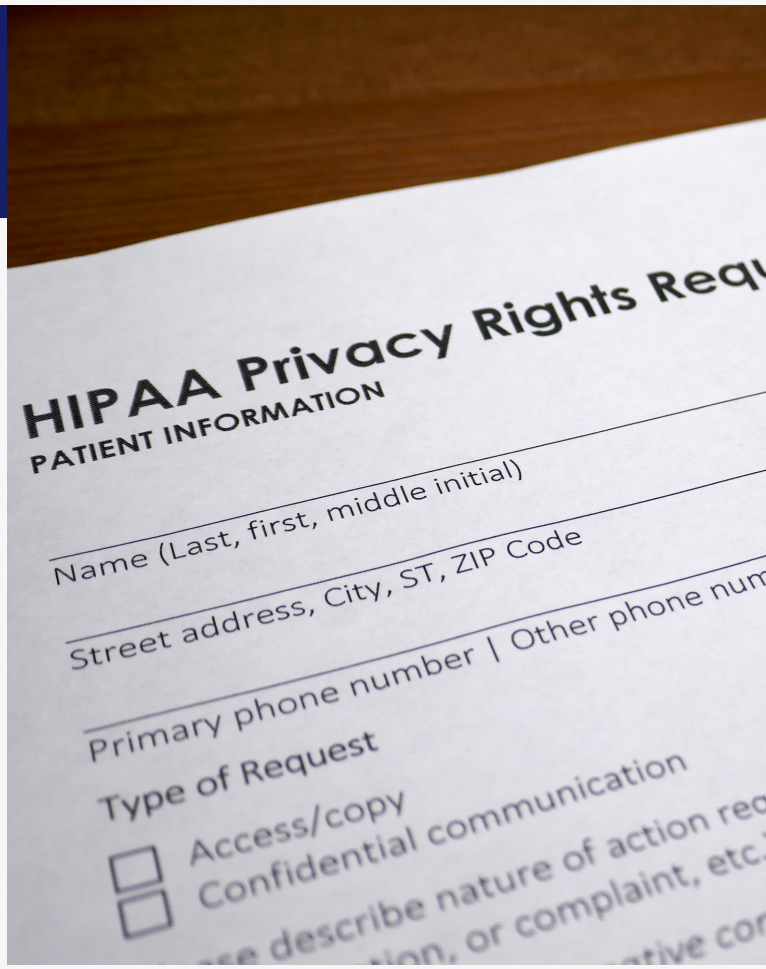
A governance body tasked with managing member companies, providing onboarding and education, conducting regular audits, and developing corrective action plans or further disciplinary actions – including direct referral to the Federal Trade Commission (FTC) for non-compliance – would provide real, consequential accountability in the absence of federal legal obligations.

Structure of This Report

This paper makes the case for why stronger data protections around consumer health data are needed now. As we wait for federal privacy legislation, the private sector can do more, including establishing a new program based on the Framework's data use standards. This report:

- Explores the current landscape of data protection and the gaps that leave health information particularly vulnerable;
- Makes the case for why, in the absence of new comprehensive federal data legislation, the burden lies squarely with the private sector to launch a regulatory model to bolster consumer protections;
- Establishes the value proposition for the Framework to four crucial constituencies: consumers, companies collecting health-related data that are not covered by HIPAA; federal enforcement authorities; and HIPAA-covered entities; and
- Concludes with a path forward, with a goal toward providing a roadmap for future federal legislation.

Section 1: Current Landscape of Protections for Health



Federal Laws

Unlike the European Union's General Data Protection Regulation (GDPR), which provides a framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union, the United States does not have an overarching legal structure governing personal data.

HIPAA and its Privacy and Security Rules apply to holders of protected health information, known as HIPAA "covered entities." These, broadly, are providers and payers, and the data covered by HIPAA is data that covered entities create or receive that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past,

present, or future payment for the provision of health care to an individual.[7] HIPAA-covered data is also specific to data that identifies, or can identify, an individual.[8] HIPAA and its regulations dictate the circumstances under which data can be shared without individual consent – primarily for purposes of treatment, payment, or broadly defined "healthcare operations."

Like most laws and regulations that are decades old, HIPAA has become outdated. Although HIPAA protects data within the traditional healthcare system, the world in which HIPAA and its regulations' obligations were written did not contemplate the technological landscape of the 2020s. Importantly, the HIPAA privacy rule does not apply to individuals, nor data they create and store in consumer-facing digital technologies – again, HIPAA applies only to covered entities and protected information they hold. As a result, the enormous amount of data that is generated, stored, and shared by consumers on personal devices such as laptops, smart-phones, and wearables enjoys none of the protections that same data would have if it were stored in a doctor's office or insurance plan.

Nor are the majority of digital health platforms covered by HIPAA. Although companies who perform services for or on behalf of a covered entity that involve the use or storage of protected health information enter into a "business associate agreement" with covered entities, extending the same HIPAA obligations to those companies, most individual health applications or platforms do not act as HIPAA business associates, and therefore have none of the legal obligations that covered entities do when it comes to keeping data private.

HIPAA is not the only federal law that protects health data. There are protections for data held by federally funded substance use facilities ("Part 2" regulations), for the human subjects of federally funded research (the "Common Rule"), for health information stored in educational records (Family Educational Rights and Privacy Act), and the FTC's Health Breach Notification Rule, which requires vendors of personal health records, health apps, and related entities to notify consumers following a breach involving unsecured information. The scope of these laws is more narrow than HIPAA, and they for the most part are complementary to HIPAA protections.[9]

While not specific to healthcare, the FTC has the authority to regulate the unfair or deceptive acts or practices of commercial entities handling consumer data, and it acts as the watchdog for misuse of such data. Specifically, the FTC may be able to bring enforcement actions against an entity "for collecting or using personal information in a deceptive or unfair manner, such as when a company's privacy practices contradict its posted privacy policy." [10] Although the FTC has used this authority to bring actions against consumer health technology products whose data practices harm consumers,[11] the FTC is not currently set up to be an efficient and nimble privacy enforcer. Its rule-making authority is limited and it lacks adequate resources.[12]

State Laws

Over the past several years, there have been periods of building momentum on Capitol Hill for new, comprehensive privacy legislation that would complement, rather than replace, HIPAA. These efforts stalled, however, in the lead-up to the 2020 election, the arrival of the Covid-19 pandemic, and a variety of other political factors. Discussions on the Hill have started up again, but no new legislation is imminent.

In the absence of federal solutions, states have been taking their own actions to shore up protections for consumer-generated health data. The patchwork of state laws, and the ways in which they interact with HIPAA, has always posed a challenge to regulators and industry alike. Although HIPAA provides a "floor" for the protection of health data, states have the freedom to implement laws that are both wider in scope and more stringent when it comes to uses and disclosures than HIPAA. These laws are sometimes in line with those of other states, but often they are not, and at times they even contradict the requirements of other states.

California has long been at the forefront of state privacy efforts. The California Consumer Privacy Act of 2018 (CCPA), which went into effect in January of 2020, gives consumers more control over the personal information that businesses collect about them. It is seen as a landmark piece of legislation, mirroring in many ways Europe's GDPR and securing new privacy rights for California consumers. These rights include: the right to know about the personal information a business collects about them and how it is used and shared; the right to delete personal information collected from them (with some exceptions); the right to opt out of the sale of their personal information; and the right to non-discrimination for exercising their CCPA rights.[13] Businesses covered by the CCPA, which include data brokers, must also give consumers certain notices explaining their privacy practices.

In early 2021, California regulators proposed legislation that would expand the privacy protections under the Confidentiality of Medical Information Act ("CMIA"), the state's primary law governing the use and disclosure of health information, to a broader range of health technology companies, including commercial websites, online services and mobile applications.[14]

In March of 2021, Virginia became the second state, after California, to enact state consumer data privacy legislation, followed shortly thereafter by Colorado. Privacy bills are active in a handful of other states, including Alaska, New York, North Carolina, Ohio, Rhode Island and Utah.[15]

Although these new state laws offer important privacy protections for their residents, and California's CMIA proposal, should it move forward this year, would be a substantial step toward closing the gaps in the state's protections for health data, if all 50 states take legislative action to shore up consumer privacy, the already entrenched web of crisscrossing, overlapping and sometimes contradictory state laws will only intensify, leading to inconsistent protections for consumers and compliance headaches.

Examples of Risks and Harms of Data Misuse

The flurry of state activity when it comes to consumer protections is based in part on the increased scrutiny on both the state and federal level of mobile applications, in California in particular. In September 2020, then-California Attorney General Xavier Becerra – now Secretary of the Department of Health and Human Services – announced a $250,000 settlement with fertility app Glow, Inc., resolving allegations that the company had "expose[d] millions of women's personal and medical information" and violated multiple laws, including [the CMIA]." A second fertility-tracking app, Flo Health, settled with the FTC early in 2021, resolving allegations that "the company shared the health information of users with outside data analytics providers after promising that such information would be kept private." This action is notable in part because the settlement required the company to provide its users with a notice of the FTC's action.[16]

These two cases are good examples of the risks inherent in storing sensitive health data in digital tools not subject to HIPAA. While fertility data may be among the most sensitive categories of health information, it is certainly not the only data for which there are health apps or digital health tools. According to data analytics firm IQVIA, "there are now over 318,000 health apps available in app stores worldwide. With over 200 health apps added each day, this is nearly double the number of apps available just two years ago."[17] Although the FTC, as part of its Flo settlement announcement, said the agency is "looking closely at whether developers of health apps are keeping their promises and handling sensitive health information responsibly," [18] the sheer volume of health apps indicates just how enormous that task is – and the subsequent risk to under-protected consumers.

Consumers freely upload information about substance abuse and treatment, mental health, nutrition and weight, sexual activity, and all types of health conditions into their personal electronic devices every day. "When data about consumer health is misused and used in ways not anticipated or expected, individuals can be harmed in myriad ways. Unregulated or inappropriate data use can produce biased data, compound historical discrimination, and yield incorrect assumptions. Unfortunately, all too often, "these risks are disproportionately borne by historically marginalized groups, including people of color, immigrants, native populations, women, individuals with a disability, and the LGBTQ community," as explained in detail by CDT's Equity Report.

As CDT details, specific harms can include:

- Embarrassment due to the release of personal, sensitive data. This can include data about conditions that are especially sensitive for specific marginalized communities because of accompanying stigmas and discrimination.
- Inaccurate data, which can disproportionately harm those whose data is not accurately or fully represented and result in lost or denied services and benefits.
- Lack of autonomy caused by data sharing, particularly for unanticipated uses. Acute harms can result when data purportedly used for one purpose is used in other ways, which may disproportionately harm marginalized communities.
- Discriminatory health treatment.
- Lack of trust in technology and health services. Although new technologies hold great promise, inappropriate data use and sharing can result in consumers losing faith and trust in new promising technologies.[19]

These very real harms, and the disproportionality with which they can befall underserved and marginalized communities, lends real urgency to the implementation of the robust accountability model presented by the Framework.

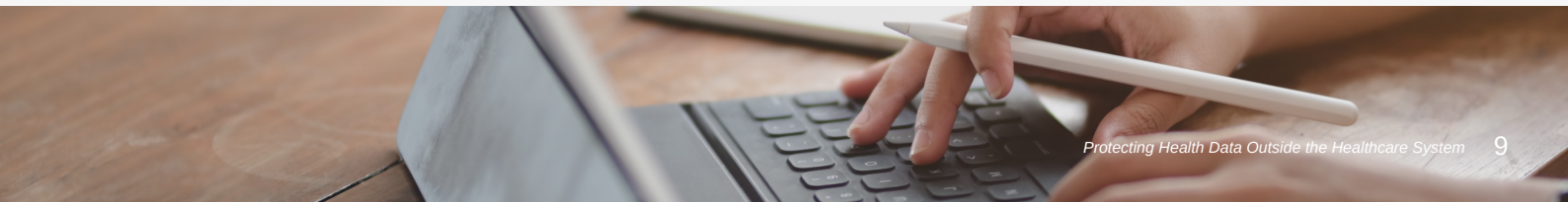
Section 2:
Value Case for an Accountability Model Based on the Consumer Privacy Framework's Data Standards

Outlined below is the value proposition of the framework for four key constituencies: consumers, companies collecting health-related data that are not covered by HIPAA, the Federal Trade Commission, and traditional healthcare system (HIPAA-covered) entities, with an emphasis on why a corporate accountability program is the most effective way to shore up meaningful consumer health protections in the absence of federal legislation.[20]

Consumers

The framework raises the bar for consumer privacy beyond existing best practices and voluntary codes of conduct by:

- Defining health information broadly enough to cover all the data that reflects mental or physical wellbeing or health, and applying to all entities that develop consumer technology and may access, hold, or use consumer health data.
- Focusing on how consumer health information is used rather than *what* information, and putting clear restrictions on the collection, disclosure, and use of consumer data. .
- Shifting the burden of privacy risk off consumers and onto the companies collecting and storing consumer data. Transparency and consent remain important elements within the Framework, but the detail, length, and density of most company privacy practices make it unrealistic and untenable for consumers to meaningfully research each technology with which they interact, nor understand the terms of use they are asked – or required – to accept before they can use each tool. While important for purposes of FTC enforcement, notices of privacy practices and terms of service are not effective consumer privacy tools, and the Framework is explicitly focused on filling that gap.
- Enabling consumers selecting health technologies to do so with less confusion and risk. The recent implementation of new rules regarding interoperability and information-blocking means that consumers will soon have greater access than ever to their own health data. The new regulations require that providers and payers quickly make individuals' health data available to them via the digital platform of their choice. It remains an open question, however, as to how consumers will choose apps to receive this data that are privacy protective, and/or how they will be educated regarding their options. The accountability program will be explicitly consumer-facing and employ a user-friendly visual representation to enable consumers to evaluate their health technology choices without having to understand the data use policies of each. This visual indicator – something akin to a "Good Housekeeping Seal of Approval" would distinguish "approved" apps that were successfully assessed by third party auditors. Given the lack of knowledge that the average person has about the legal protections of his or her health information or the privacy practices of any given app, a simple seal would provide a quick and effective way for consumers to make smart, privacy-protective choices, without having to understand the scope of HIPAA or be solely dependent upon the FTC to identify bad actors.
- Shoring up consumer confidence and trust. Once a consumer has chosen a technology that is covered by the Framework, he or she would also enjoy the confidence of knowing that independent third-party auditors are regularly evaluating the developer's privacy and data use practices, and that the needle-in-a-haystack dynamic of FTC protections was substantially bolstered by the body governing the framework.



- Creating a system to receive and review consumer complaints. An important element of the independent regulatory program would be a clear and conspicuous pathway for consumers to submit complaints or questions should they feel that their privacy had been violated in any way. The program's website would provide details regarding such a pathway, as well as a public list of framework members, and any members currently subject to a corrective action plan.

Companies Collecting Health-Related Data

Entities that elect to adopt the Framework and join the private-sector regulatory program as members would enjoy benefits both from an internal compliance perspective and from an external market perspective. By making pro-privacy decisions now, they would avoid having to make product changes down the road that could be more expensive, time-consuming, or complicated in response to future regulation. Companies in the process of developing new technologies would be deterred from collecting and using health data they do not actually need when designing a consumer-facing product, reducing legal risks in a world where consumers and enforcement agencies are increasingly expecting heightened privacy guarantees from companies that handle data. This Framework may even serve as a potential road map for future data privacy legislation, putting companies that join as participants "ahead of the curve" when adopting the Framework's policies.

Entities participating in the framework would:

- Distinguish themselves in the market by publicly employing privacy protective practices. Participating entities are likely to see significant reputational and commercial benefits.

  The program will provide participants a way to set themselves apart, nationally, in an increasingly competitive market marked by widespread consumer distrust – and power.

  According to a recent McKinsey report on consumer data protection and privacy, "the great majority of [survey] respondents—87 percent—said they would not do business with a company if they had concerns about its security practices."[22] This same survey found that consumers may "walk away from doing business with companies whose data-privacy practices they don't trust, don't agree with, or don't understand."[23]

  The McKinsey report concludes with this simple yet powerful message: "our research revealed that our sample of consumers simply do not trust companies to handle their data and protect their privacy. Companies can therefore differentiate themselves by taking deliberate, positive measures in this domain. In our experience, consumers respond to companies that treat their personal data as carefully as they do themselves."[24] Framework adherence, and membership in its accountability program, allows companies to do just that.

  Similarly, Cisco's 2022 Privacy Benchmark Study, which surveyed over 4,900 security professionals across 27 countries, determined that 'privacy has become mission critical.' The report explains that '[privacy has become a business imperative and a critical component of customer trust for organizations around the world. For the second year in a row, 90% of the respondents in our global survey said they would not buy from an organization that does not properly protect its data, and 91% indicated that external privacy certifications are important in their buying process.' Further, '[n]inety percent of all respondents said they consider privacy a business imperative.[25]

Further, “82 percent of organizations see privacy certifications as a buying factor: Privacy certifications … are becoming an important buying factor when selecting a third-party vendor.” [26]

- Enjoy some compliance certainty for companies on a national level. By adopting more forward-looking privacy practices, companies and organizations may avoid the gray or evolving areas of existing laws. Especially for smaller or newer companies having difficulty fully understanding their numerous federal and state legal obligations, which can often be unclear and/or conflicting, compliance with the Framework’s standards would position participants to stay consistent with various potential federal and state requirements.

Federal Trade Commission

The FTC, which has traditionally served more as an enforcement agency than as a regulatory agency, would benefit from companies not only committing to comply with the standards, but being assessed as to their compliance and held to a common set of publicly available data practices.

By virtue of the framework, the FTC would enjoy the benefits of:

- A neutral process to identify non-compliant actors. The work of the independent regulatory organization will identify those who agree to participate in the Framework, have fallen down on compliance obligations for whatever reason, and work with them to remedy their data practices. The independent organization will also be able to funnel those who refuse to remedy their practices directly to the FTC, enabling the Commission to better allocate its limited enforcement resources and continue its existing Unfair or Deceptive Acts or Practices (UDAP) regulatory mission.

- Assistance in its efforts to focus on consumer privacy. Particularly as tech giants continue to expand in scope, size, and influence, there has been a recent push by FTC commissioners to re-center and prioritize consumer privacy enforcement actions. FTC Chair, Lina Khan, has been outspoken in her criticism of online behavioral advertising, and how it is fundamentally misaligned with protecting consumer privacy.[27] Her appointment has been widely discussed as having the potential to signal “a new era” of more aggressive action on data protection issues,” [28] which is supported by the statement on privacy Kahn issued in October of 2021.

  “Policing data privacy and security is now a mainstay of the FTC’s work,” the statement begins, and Khan goes on to ask Congress for additional resources to beef up the agency’s ability to protect consumer privacy and security.[29] The need for more resources in order to enable increased staffing was also emphasized in a September 2021 FTC report to Congress on privacy and security.[30]

  In its list of priority areas, all of which it described as resource-intensive, the FTC cited, among other things:

  - The collection, use, and disclosure of sensitive data, including location data and health data that falls outside of the Health Insurance Portability and Accountability Act, particularly in light of the fact that the pandemic may lead consumers to increasingly turn to various health apps to manage their conditions; and
  - The overlap between racial equity issues and privacy, including the potential for algorithmic discrimination in various artificial intelligence applications, such as those that may be used for credit, healthcare, or facial recognition purposes.[31]

Congress appears to agree that an increase in resources is necessary. Sen. Maria Cantwell (D., Wash.), who chairs the Commerce Committee, argued in September of last year that Congress needs to direct additional resources to the FTC to better address issues arising from the new digital economy.[32] Also in September of last year, the House Consumer Protection Subcommittee passed a proposal that would allocate $1 billion to the FTC to staff a new bureau addressing unfair or deceptive practices related to privacy, data security, identity theft and other data abuses.[33]

Until the FTC obtains these additional resources, and even after it does, the Framework's accountability program would provide valuable support for these FTC priorities. By educating and assisting those companies that want to do the right thing, but may not fully understand what that entails, the accountability program would both raise the industry's overall compliance posture and allow the FTC to focus its limited resources on those actors that require the strong hand of law enforcement.

- Provide a strong industry partner to lend additional resources and a head-start on rule-making. Ms. Khan emphasized in her October 2021 privacy statement that "the Commission must explore using its rulemaking tools to codify baseline protections," [34] and since taking office in June of 2021 has made a number of moves to lay the groundwork for potential rule FTC rule-making. President Biden himself has ordered the FTC to look at writing competition rules in a number of areas, including "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy." [35]

  Implementation of the framework would bolster consumer privacy now, providing backup while the administration and FTC leadership make plans for the agency's future. The accountability body would provide a strong partner with expertise in consumer health privacy, perhaps informing and complementing future FTC rulemaking and compliance incentives as well.

Traditional Healthcare Entities

Finally, although the Framework is geared toward companies that operate outside the traditional healthcare system and thus are not subject to the obligations and protections of HIPAA, the Framework would benefit HIPAA-covered entities as well, by easing the burden on providers and payers working to comply with the interoperability and information blocking rules.

As noted above, these rules mean that providers and payers have new obligations to send data, at consumers' requests, to the third-party app of their choice.

Given the outsized educational role that often falls on providers in particular, whether legally required or not, a program that clearly identifies companies that have already met – and are being held accountable to – stringent data protection practices will provide an enormous benefit to these trusted messengers. Rather than having to research the various levels of integrity of the host of digital health tools available to consumers themselves, adding yet another administrative burden to these already over-taxed healthcare entities and individuals, providers and their staffs will have a new tool to help differentiate one app from another and make wise recommendations to their patients.

Section 3:
Creating Corporate Accountability Through Independent Regulation

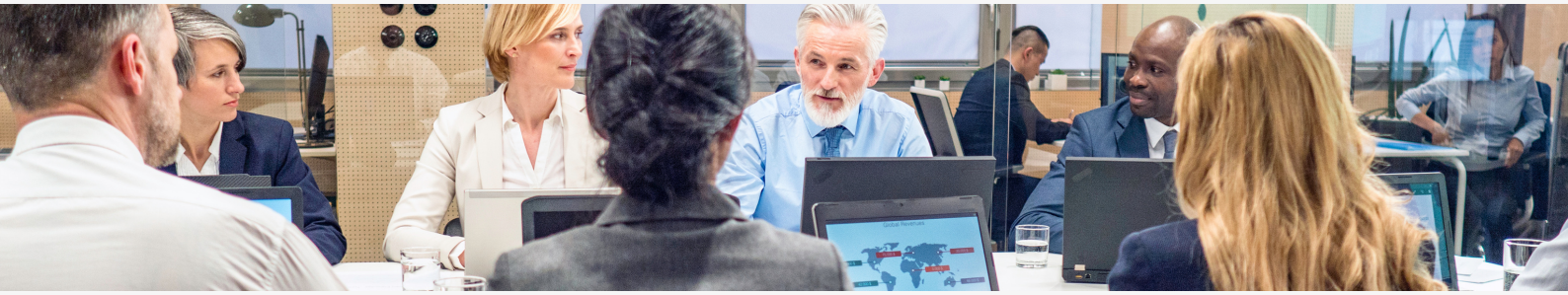
Although it is imperative that the U.S. continue its efforts to develop and pass comprehensive federal privacy legislation, there are real benefits to the private sector taking steps to better protect the privacy of consumer health information in the meantime. Industry partners are able to move quickly, be nimble, and adjust to ever-changing technological developments.

The value of the Framework resides in its direct application to entities that develop consumer technology. Consumers are in dire need of a rigorous accountability model, based on the Framework's standards, that can be applied to all companies that collect and use health data. While we wait for a federal mandate requiring accountability, the burden – and opportunity – lies with the private sector to step up to the plate and take affirmative actions to better protect the privacy of health data.

The Value of Private-Sector Regulation

Whether it is the American Bar Association, the American Medical Association (AMA), the Joint Commission, the National Committee for Quality Assurance (NCQA), or the host of programs that regulate the advertising industry, accountability models often take the form of a third-party self-regulatory body. When self-regulation is successful, it improves conditions for consumers by "establishing deliberative bodies that can act swiftly and firmly, and generate clear, enforceable codes of conduct."[36]

The prevalence of self-regulatory bodies in the advertising industry, and notably the Network Advertising Initiative (NAI) Code, reflects the relatively weak U.S. regulatory framework for information privacy that lacks generally applicable data protection and privacy legislation. The Framework's privacy program would be the only program currently focused on consumer health data.



As described by privacy scholar Ira Rubinstein, "privacy self-regulation generally involves individual firms, a trade association, or an ad hoc group of firms establishing substantive rules concerning the collection, use, and transfer of personal information, as well as procedures for applying these rules to participating firms. Self-regulation most often takes the form of industry groups promulgating voluntary codes of conduct that members agree to adhere to."[37] This is the model the Framework's program would take. The substantive rules have been established,[38] and participating firms would apply them to their data policies and practices; Framework membership would be voluntary, and accountability for compliance would be managed by a third-party independent organization.

Companies have the ability to be more nimble with respect to their data practices than do federal authorities struggling to update the legal and regulatory regime. Indeed, information privacy scholars Ken Bamberger and Deirdre Mulligan have written that "entities are more successful in protecting privacy not when regulatory agencies grow 'the number, specificity and uniformity of regulations' and their own regulatory power,"[39] but rather when they push "more of the responsibility for meaningfully defining, interpreting, and enforcing privacy back toward corporations."[40]

It is beyond the scope of this report to analyze the history of self-regulation and privacy, though there is no shortage of scholarly papers and articles that do just that, several cited herein. But to the extent that self-regulation in principle or in the privacy field specifically has been met with skepticism or opposition, it tends to be because, as Rubenstein writes, "many critics view privacy self-regulation as a failure due to an overall lack of accountability and transparency, incomplete realization of robust privacy principles, free rider issues, and weak oversight and enforcement. For these observers the real purpose of voluntary self-regulation is to avoid government regulation. Not surprisingly, they see comprehensive privacy legislation as the only viable alternative.[41]

The Framework provides a middle ground: an independently led, private-sector accountability program with robust oversight and enforcement pathways that aims to lay the groundwork – and ultimately provide support for – federal legislation.

Support for Federal Legislation

The Framework's recommendation for an independent regulatory program is not designed to avoid, supplant, or oppose government regulation or legislative action, and in fact throughout its development and finalization, EHI, CDT, and the Framework's advisory Steering Committee[42] have been vocal advocates for new legislation. But as no such legislation appears to be on the near horizon, action is urgently needed to protect consumer health data now. The private sector not only has the opportunity but also the responsibility to step up and address these protections, which are in dire need of strengthening.

The Framework's intention is to create further momentum for federal legislative action, while allowing the industry to provide a possible roadmap for it.

Addressing the Skeptics

Consumer groups have traditionally been critics of self-regulation. The "fox guarding the hen-house" perception of self-regulation worries some. But importantly, the proposed structure of the independent regulatory body is in large part focused on assuaging these worries by creating third-party, objective accountability. **Specifically, the program will be run not by an industry group or any individual member company, but by an independent third-party organization with objectivity, integrity, and experience.** Consumer input will be solicited throughout the program's design, as it was during the development of the standards.

In the absence of legislative activity on the consumer privacy front, company terms of service and notices of privacy practices comprise the entirety of consumer privacy protections. There is near-universal consensus among privacy experts that complex privacy policies contained in a single document are not an effective way to communicate with consumers about the information processing practices of a business,[43] and in recent years, the FTC has been vocally supportive of self-regulation, which encourages flexible, market-based solutions.[44]

Privacy scholar Chris Hoofnagle has hypothesized that this support stems, at least in part, from the fact that "from the FTC's perspective, even weak self-regulatory regimes assist the Agency." [45] Further, underscoring the value proposition of the Framework's accountability program to the FTC, Hoofnagle surmises that

"voluntary codes take work off the Agency's plate and bind companies to promises that, even if weak, are likely to be broken; it is easier to police broken promises under the FTC's deception authority than to employ unfairness; and voluntary codes may evolve into industry standards."[46]

As neither the Framework's standards nor its accountability program is weak, Hoofnagle's words underscore its value and necessity.

Section 4: The Path Forward

The establishment of an independent, private-sector regulatory body that is responsible for holding members of the Framework accountable to the standards has required a significant amount of groundwork. As proposed in the Framework, this body will be housed in and run by an independent, third-party organization with experience standing up and running similar self-regulatory programs. EHI and its advisory team agreed that creating a brand-new certification process or entity would pose significant start-up costs and unnecessary administrative hurdles, while taking advantage of an existing infrastructure and staffing capabilities will shorten the timelines and reduce the resources necessary to get a new program up and running.

Criteria for a Successful Program Home

EHI determined a set of mandatory criteria for any organizational home for the Framework's accountability program. The organization must be:

1. *Independent.* Although there may be an opportunity to formally align with the Federal Trade Commission or the Department of Health and Human Services at some point, at its inception this program should be run by an independent, non-partisan, third-party organization. Any organization perceived as controlled by companies being evaluated would face immediate skepticism and lack credibility.

2. *Well-established*. Launching a new regulatory program will be time- and resource-intensive, and the start-up costs, both financially and in terms of man-power, will be significantly reduced if an existing organizational home is chosen.

And it must have:

3. *Experienced staff*. Were a new program to be stood up from scratch, employees would need to be hired to: run the program; evaluate potential member companies for either current or potential adherence to the framework's data use standards; conduct educational and on-boarding efforts; develop and maintain a public-facing website; handle consumer reports of data violations; conduct annual assessments and audits; handle the development and compliance with corrective action plans; interact with the FTC in the event of egregious violations; and keep the Framework's standards current and flexible to adapt to future regulatory and private sector developments.

These duties, which are merely representative and not exhaustive, will require a substantial and skilled workforce. An organization with the understanding of the staffing needs inherent in such a regulatory program would greatly reduce the burdens of program start-up and hiring efforts.

4. *Name-recognition and reputation*. In order to be meaningfully beneficial to consumers, the program must not only be well-publicized but well-respected. Regardless of the integrity and potential of any new program, public education efforts to inform consumers, industry, and federal regulators and enforcement officials alike of a program's value takes an enormous amount of time and effort. Housing the Framework's accountability body in an organization that already has name-recognition and respect among the public, with the commercial technology sector, and with government officials will provide an important head-start to the program's efforts. Reputation is just as important, if not more, than name recognition, as the brand needs to be both tried and trusted.

5. *Experience and credibility running self-regulatory programs*. There is no perfect model with which to align the proposed health privacy regulatory program, but there are certainly successful programs in existence from which valuable lessons can be drawn. Initiatives such as the Children's Advertising Review Unit, the Digital Advertising Accountability Program, the BBB EU Privacy Shield, the American Institute of CPAs, the Financial Industry Regulatory Authority (FINRA), or the American Bar Association are examples of successfully run and well-regarded programs in other industries, and exploring their governance would be valuable to the new health data program.

6. *Experience with privacy and data use*. The BBB EU Privacy Shield program, run by BBB National Programs, enables U.S. businesses to demonstrate compliance with data protection standards when handling the personal information of consumers from the European Union, the United Kingdom, and Switzerland.[47] Given the similarity of this program and the proposed Framework accountability program, this model would be a valuable example for successful data stewardship. Technological expertise and experience related to privacy, or at the very least the ability to hire the right technologists to evaluate companies' privacy practices and adherence to the Framework, will be crucial.

Selection Process and Awardee

In early February, EHI released a Request for Proposals (RFP)[48] to select an organizational home for the Framework's accountability program. We chose this path because it had the benefit of being fully transparent, as well as providing EHI an opportunity to detail clearly the organizational capacity requirements. As hoped, this process resulted in responses from a number of exceedingly well-qualified organizations eager to assume responsibility of leading the Framework's accountability efforts.

A committee of expert, objective reviewers evaluated the applications. After careful review, the committee unanimously selected BBB National Programs to stand up the Framework's self-regulatory program. Both BBB National Programs and EHI hope also to involve the other applicants in the future of this work ahead.

BBB National Programs

Conclusion

With every day that passes, millions more pieces of sensitive, valuable data leave the protection of the HIPAA-covered healthcare space, or are created and stored on vulnerable platforms. The recent proliferation of cyber-breaches in technology underscores the urgency of action to shore up protections for health data now. Although no solution is “perfect,” remaining idle is not an option. Even the most thorough and thoughtful codes of conduct will not provide meaningful protection beyond what we have now. The Framework is one of the few efforts poised to address the lack of consumer trust in health technology.[49]

When this project launched in 2020, there was some indication that comprehensive privacy legislation might emerge as a priority on Capitol Hill.[50] As of 2022, there is no well-supported bi-partisan legislation on the horizon. Therefore, the industry itself needs to take important steps now to shore up consumer data privacy. The Framework’s robust, wrap-around data use standards are designed to prevent many of the harms caused by a lack of legislation.

The financial and advertising sectors have successfully demonstrated that harm to consumers caused by egregious data practices can be significantly mitigated by independent industry self-regulation. Similarly, our hope is that a self-regulatory model in the health technology sector will be an effective intermediate step to address harms caused by a lack of legislation.

Consumers, including those from marginalized and vulnerable populations, were involved in the design of the Framework, and meaningful accountability will provide benefits to consumers as well as the companies holding their most private and sensitive data. Ultimately, an effective program should impact consumer confidence, companies’ bottom lines, and and provide an overall benefit to our interconnected healthcare system.

About Executives for Health Innovation (EHI)

About Executives for Health Innovation Executives for Health Innovation (EHI) is a catalyst for healthcare transformation, convening diverse leaders from across the industry to unlock opportunities for collaborative innovation. EHI, along with its coalition of members, focuses on education, thought leadership, and advocacy. We believe that innovation and diverse perspectives power the transformation of healthcare. Our members are working toward consumer-centered health that is lower cost, higher quality, and more accessible for all populations. www.ehidc.org/

EHI EXECUTIVES FOR HEALTH INNOVATION

Endnotes

[1] Rawal, Amit. (2020, January 21). Google's New Health-Search Engine. Medium. https://medium.com/swlh/googles-new-healthcare-data-search-engine-9e6d824b3ccd
[2] The Top 10 Most Googled Health Questions That Aren't about Coronavirus. (2020, November 09). Vala. https://valahealth.com/posts/2020/11/09/the-top-10-most-googled-health-questions-that-arent-about-coronavirus/
[3] McCarthy, Jack. (2017, March 06). Survey: 64% of patients use a digital device to manage health. Mobihealthnews. https://www.mobihealthnews.com/content/survey-64-percent-patients-use-digital-device-manage-health
[4] Proposed Consumer Privacy Framework for Health Data. (2021, February). Center for Democracy & Technology. eHealth Initiative & Foundation. Report. Hereinafter, "Consumer Privacy Framework." https://www.ehidc.org/sites/default/files/eHIDCT_Consumer_Privacy_Framework.pdf
[5] *Placing Equity at the Center of Health Care & Technology, Center for Democracy & Technology (CDT)*
[6] See, e.g., CARIN Alliance. https://www.carinalliance.com/; Consumer Technology Association, https://www.cta.tech/Resources/Newsroom/Media-Releases/2019/September/CTA-Releases-Industry-Developed-Privacy-Guidelines
[7] Health Insurance Portability and Accountability Act of 1996. Public law 104 -191. (1996, August 20). https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
[8] Id.
[9] FTC Warns Health Apps and Connected Device Companies to Comply with Health Breach Notifications. 2021, September 15).Federal Trade Commission. Press release. (https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health
[10] COVID-19: Digital Contact Tracing and Privacy Law. (2020, July 9). Congressional Research Service. LSB10511. https://crsreports.congress.gov/product/pdf/LSB/LSB10511
[1] For example, in early 2021, the FTC brought an action against a mobile health app designed to allow users to track their reproductive health. In this case, the FTC alleged that Flo Health "shared the health information of users with outside data analytics providers after promising that such information would be kept private." In June of 2021, Flo and the FTC finalized a settlement agreement. Flo Health Inc. (2021, June 22). Federal Trade Commission. Cases and Proceedings. FTC file number: 192 3133. https://www.ftc.gov/enforcement/cases-proceedings/192-3133/flo-health-inc
[12] See, e.g., The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers, U.S. House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce, 117th Cong. (2021) (testimony of Anna Laitin). https://docs.house.gov/meetings/IF/IF17/20210427/112501/HHRG-117-IF17-Wstate-LaitinA-20210427.pdf.
[13] California Consumer Privacy Act of 2018. The California Civil Code. Title 1.18.5 (2018, June 28). https://oag.ca.gov/privacy/ccpa
[14] The Confidentiality of Medical Information Act (CMIA). Ca
lifornia Civil Code. Sections 56 – 56.16. (2013, September 9). https://irb.ucsd.edu/cmia.pdf.
[15] Status of Proposed CCPA-Like State Privacy Legislation as of March 29, 2021. Husch Blackwell. Byte Back. https://www.bytebacklaw.com/2021/03/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-march-29-2021/
[16] Flo Health Inc. Federal Trade Commission. Decision and Order. Docket No. C-4747. (2021, June 22). https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf
[17] The Growing Value of Digital Health: Evidence and Impact on Human Health and the Healthcare System. (2017, November 07). The IQVIA Institute. Report.
[18] Kraus, A., Yergin, R., Vega, O. (2021, February 08). FTC Reaches Settlement with Digital Health App, Requires First Notice of Privacy Action. Covington Digital Health. https://www.covingtondigitalhealth.com/2021/02/ftc-reaches-settlement-with-digital-health-app-requires-first-notice-of-privacy-action/
[19] *Placing Equity at the Center of Health Care & Technology,* Center for Democracy & Technology (CDT)
[20] See Consumer Privacy Framework, supra note 4.
[21] Interoperability and Patient Access final rule. Centers for Medicare & Medicaid Services. CMS-9115-F. 85 FR 25510. (2020, June 30). https://www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and
[22] Anant, V., Kaplan, J., Soller, H. (2020, April 27). The consumer-data opportunity and the privacy imperative. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
[23] Id.
[24] Id.
[25] Cisco 2022 Privacy Benchmark Study, "Privacy Becomes Mission Critical," https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2022.pdf?CCID=cc000742&DTID=odicdc000016
[26] "Cisco 2020 Data Privacy Benchmark Study Confirms Positive Financial Benefits of Strong Corporate Data Privacy Practices," available at https://newsroom.cisco.com/
[27] See, e.g., Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security, Oct. 1, 2021, (hereinafter "Khan Statement"), available at https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf.
[28] Vittorio, A. (2021, June 17). Lina Khan Bring Scrutiny to Big Tech Data Dominance as FTC Chair. Bloomberg Law. Privacy & Data Security Law. https://news.bloomberglaw.com/privacy-and-data-security/khan-to-bring-scrutiny-to-big-techs-data-dominance-as-ftc-chair
[29] Khan Statement, supra note 25.
[30] FTC Report to Congress on Privacy and Security, Sept. 13, 2021. Available at: https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf
[31] Id.
[32] See, e.g., https://www.cantwell.senate.gov/news/press-releases/at-hearing-with-facebook-safety-head-cantwell-says-children-need-stronger-protection-from-digital-abuse-harm; https://www.commerce.senate.gov/2021/10/cantwell-says-action-needed-to-stem-tide-of-id-theft-ransomware-and-security-breaches.
[33] Kaye, K. (2021, September 15). Congress moves to give $1B to FTC to fund new bureau to protect privacy in tech platform era. DIGIDAY Media. Data Regulation. https://digiday.com/marketing/congress-moves-to-give-1b-to-ftc-to-fund-new-bureau-to-protect-privacy-in-tech-platform-era/
[34] Khan Statement, supra note 25.
[35] McKinnon, J., Tracy R. (2021, September 29). FTC Weighs New Online Privacy Rules. The Wall Street Journal. Tech. https://www.wsj.com/articles/ftc-weighs-new-online-privacy-rules-11632913200
[36] Vaidhyanathan, S. (2020, May 9). Facebook and the Folly of Self-Regulation. Wired. Ideas. https://www.wired.com/story/facebook-and-the-folly-of-self-regulation/
[37] Rubinstein, I. (October 5, 2016). The Future of Self-Regulation is Co-Regulation. The Cambridge Handbook of Consumer Privacy. Cambridge University Press. Available at SSRN: https://ssrn.com/abstract=2848513
[38] Consumer Privacy Framework, supra note 4.
[39] Bamberger, K. A, Mulligan, D. K. (2015). Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. Massachusetts Institution of Technology.
[40] Id.
[41] Rubinstein, I. (October 5, 2016). The Future of Self-Regulation is Co-Regulation. The Cambridge Handbook of Consumer Privacy. Cambridge University Press. Available at SSRN: https://ssrn.com/abstract=2848513.
[42] Consumer Privacy Framework, supra note 4. See appendix for a partial list of Steering Committee members.
[43] Profiling the mobile customer: Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones? e Part II, Nancy J. King a, Pernille Wegener Jessen ba College of Business, Oregon State University, USA; b Aarhus School of Business, Aarhus University, Denmark. See Center for Information Policy Leadership, Ten Steps to Develop a Multilayered Privacy Notice 1e9 (March 2007), http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C1405%5CTen_Steps_whitepaper.pdf (last accessed, 23 July 2010); Martin Abrams et al., Memorandum, Berlin Privacy Notices (April 2004) (Berlin Privacy Memorandum), available at: http://www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf (last accessed, 23 July 2010).
[44] Layton, R. Competition and Consumer Protection in the 21st Century Hearings. (2018, August 20). Statement before the Federal Trade Commission. Project Number: P181201. https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf
[45] Hoofnagle, C. J., (2016). Federal Trade Commission Privacy Law and Policy. Cambridge University Press. Cambridge University.
[46] Rubinstein, I. (October 5, 2016). The Future of Self-Regulation is Co-Regulation. The Cambridge Handbook of Consumer Privacy. Cambridge University Press. Available at SSRN: https://ssrn.com/abstract=2848513
[47] BBB EU Privacy Shield. BBB National Programs, Inc. https://bbbprograms.org/programs/all-programs/bbb-eu-privacy-shield
[48] Attached as Appendix A.
[49] See, e.g., U.S. Data Privacy Roundup – What is on the Horizon? (2021, August 11). JD Supra, LLC. Legal News. https://www.jdsupra.com/legalnews/u-s-data-privacy-roundup-what-is-on-the-6247901/.
[50] See, e.g., Murphy, Chuck. It's Official: Consumers Don't Trust Tech. April 28, 2021. https://www.bostondigital.com/insights/its-official-consumers-dont-trust-tech.