TECHNOLOGY AND PUBLIC PURPOSE PROJECT

Understanding Data Privacy Protections Across Industries

Exploring Data Privacy Challenges and Approaches Across Areas of Practice

Stephanie Nguyen

Afua Bruce

Laura Manley

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

NEW AMERICA

PAPER
NOVEMBER 2019

Technology and Public Purpose Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/TAPP

Statements and views expressed in this report are solely those of the author and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Not for distribution or citation without the permission of the authors. This paper was derived from open sources and contains no classified material

Design and Layout by Andrew Facini

Cover Photo: Adobe Stock

TECHNOLOGY AND PUBLIC PURPOSE PROJECT

Understanding Data Privacy Protections Across Industries

Exploring Data Privacy Challenges and Approaches Across Areas of Practice

Stephanie Nguyen

Afua Bruce

Laura Manley

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

NEW AMERICA

PAPER
NOVEMBER 2019

About the Authors

Stephanie Nguyen is a research scientist at MIT Media Lab working to improve privacy architecture and design in data collecting systems and to shape meaningful choice and control in sharing personal data through policy and regulation. Stephanie led privacy design initiatives with the National Institutes of Health's million person genome project and Johns Hopkins' Precision Medicine team and served at U.S. Digital Service at the Obama White House. She earned a Masters in Public Policy at Harvard Kennedy School and a Bachelor of Arts in Digital Media Theory and Design at the University of Virginia. | Twitter: @stephtngu

Afua Bruce is the director of engineering for New America's Public Interest Technology program. Afua joined New America after spending several years working in the Federal government. From 2015 to 2017, Afua served as the executive director of the Office of Science and Technology Policy's National Science and Technology Council at the White House. While at the FBI, Afua held a variety of strategy and program management positions, leading work on data challenges and strategic change for the Bureau's engineering, lab, and financial programs. Afua holds a degree in computer engineering from Purdue University, and an MBA from the University of Michigan. | Twitter: @afua_bruce

Laura Manley is the inaugural Director of the Technology and Public Purpose Project at the Harvard Kennedy School Belfer Center for Science and International Affairs. Led by former Secretary of Defense Ash Carter, the project aims to steer rapid technology-driven change in directions that serve net, long-term public good. Previously, Laura co-founded the Center for Open Data Enterprise (CODE) in Washington DC, which is a nonpartisan research organization that works with governments to leverage data for social and economic good.Laura is an Adjunct Professor at the NYU Wagner School of Public Policy, where she teaches *Data for Social Innovation*, Instructor at the Harvard University Extension School, teaching *Data-Driven Decision Making for Business Leaders*, and Associate Lecturer at Columbia University School for Professional Studies, teaching *Open Data in the Applied Analytics Program*. | Twitter: @TAPP_Project, @Laura_Manley1

Table of Contents

Adobe Stock

Executive Summary

In May 2019, The Harvard Kennedy School's Technology and Public Purpose (TAPP) Project and New America's Public Interest Technology teams hosted a roundtable focused on data privacy in Washington, D.C. through the lens of two key questions:

1. How might organizations and legislators collaborate to bridge aspirational privacy principles to product design and development?
2. How might data privacy legislation be more effective to meet user needs?

This *Understanding Data Privacy Protections* report aims to synthesize key insights from the workshop convening and use four case studies to highlight the nuances of privacy protection through different organizations and strategies. As part of the decision to facilitate an open discussion during the workshop, we will integrate some of the discussion, questions and ideas throughout this report without attribution.

The co-led team convened a group[1] of over 40 data privacy minded advocates, academics, researchers, political and government officials, practitioners and lawyers to exchange expertise and views on personal data privacy regulation. The group developed a broad set of engaging ideas on ways organizations who handle personal data should consider or frame data rights and consent processes and explored conversations around improvements to data privacy legislation.

The event highlighted ongoing efforts in data privacy ranging from Carnegie Mellon's technical data privacy research in academia to

[1] The attendees included representatives from: AAA, ACLU, Asian Americans Advancing Justice | AAJC, Berkman Klein Center, Carnegie Mellon University, Center for Open Data Enterprise (CODE), Common Cause, Data and Society, Ethics Lab at Georgetown University, Georgetown University Law Center: Center on Privacy & Technology, Harvard Kennedy School Belfer Center Tech and Public Purpose, HWG Law, Institute for Technology Law & Policy at Georgetown Law, Joint Center for Political and Economic Studies, Lawyers' Committee for Civil Rights Under Law, Lyft, Mapbox, Mozilla Foundation, National Hispanic Media Coalition, Open Technology Institute at New America, Public Interest Technology at New America, Property Rights at New America, Results for America | Bloomberg Philanthropies' What Works Cities Initiative, Sage Bionetworks, Salesforce, Senate and House staffers, Shorenstein Center on Media, Politics and Public Policy, Simply Secure, and Tech Congress.

Mozilla's data privacy principles in practice through Firefox browser features. Lightning talks featured several experts who were involved in implementing some level of privacy-protecting features, policies or principles into their own organizations including: John Wilbanks, Chief Commons Officer at Sage Bionetworks, Tom Lee, Policy Lead at Mapbox, Jasmine McNealy, Attorney and Professor in the Department of Telecommunication at the University of Florida, Marla Hay, Director of Product, Privacy and Data Governance at Salesforce, Glenn Sorrentino, Principal UX Designer at Salesforce, and Gil Ruiz, Legislative Assistant at the office of Kirsten Gillibrand.

Following the lighting talks, the group broke up into small, curated discussion sessions designed to share expertise across sectors and delve into data privacy questions and concerns on: civil rights and liberties, privacy design, and potential legislation.

Key insights:

- Many participants expressed the challenge of attaining consent by informing end users of all complexities of the data capture, storage, transfer, and management. Organizations are looking to UX design patterns to test iconic representations, quizzes, and formative evaluation to improve the likelihood of understanding terms before proceeding.
- Unlike consumer focused platforms, Salesforce and Mapbox's main users are businesses. Both are exploring models of what it means to design more effective ways of conveying privacy information through embedding privacy features and functionality in their platform. There is a need to develop privacy protections on a business-to-business framework in addition to business-to-consumer.
- Due to the quickly changing nature of technology, organizations like CODE are exploring what specific issues need updates and improvements on existing policy and legislation like HIPAA, COPPA, and FERPA. What processes might help policymakers better structure legislation to iterate these policies in a realistic and timely way?
- Companies like Mapbox that collect telemetry data have multiple strategies and approaches with their trip data to make it "useless for [potential third parties] to [track] individuals." Through a delicate balance, hey continually study ways to "data accessible to researchers, planners and customers without compromising user privacy." Additionally, de-identification and anonymization of data are not the same[2].
- Privacy protections manifest in a variety of harms that are largely context dependent and can be themed by various types. For example, the privacy of one's financial data versus their social or religious affiliations may have different harms and impacts. As policymakers and practitioners consider privacy protecting regulation and mechanisms, these terms must be specified and defined to their uses and specific harms.
- There is a large gap to bridge aspirational privacy principles (e.g. "Embed privacy from the beginning" or "Put users in control of their data") with operationalizing those principles into practice and product development. These principles are often more stagnant than they should be iterative as technology develops.
- There are a variety of privacy-protecting metrics that companies and organizations are using such as the "degree of privacy enjoyed by users in a system [and] the amount of protection offered by privacy-enhancing technologies[3]." Privacy Impact Assessments, industry benchmarks through a set of standard criteria, number of data breaches, and customer satisfaction are other methods to measure privacy discussed at the IAPP's Global Privacy Summit[4] in March 2019.

Participants also highlighted key points of tension that often arose in their work as it relates to product and policy creation. These conversations paralleled many conceptual investigations of theoretically grounded approach of

[2] Kissner, Lea. "Deidentification versus Anonymization", International Association of Privacy Professionals, 18 June 2019, https://iapp.org/news/a/de-identification-vs-anonymization/.

[3] "Technical Privacy Metrics: A Systematic Survey." *ACM Computing Surveys* (CSUR), ACM, https://dl.acm.org/citation.cfm?id=3168389.

[4] Canter, Libbie, and Jeff Kosseff. "How Do I Measure My Privacy by Design Program's Success?", International Association of Privacy Professionals, 13 May 2014, https://iapp.org/news/a/how-do-i-measure-my-privacy-by-design-programs-success/.

Value Sensitive Design[5]: What values are implied through product design? How are various stakeholders impacted by that design? How might we engage in trade-offs in the implementation of features? On this note, here were some key trade-offs discussed at the event:

Key trade-offs and themes:

- *User Empowerment vs. Ease of use.* Empowering users may imply companies inundate users with complex tasks while user simplicity may imply a sense of paternalism and opacity.
- *Personalization vs. Anonymization.* Using the context of precision medicine, having precise medical data also does not mean there is a technically feasible way to be anonymous. The incentives between the genetic data collector and the user may be at direct odds. The word anonymization of data is often conflated with de-identification of data.
- *Benefits and Risks to Society vs. Company vs. Individual.* Using healthcare data as an example, patients often donate personal genetic data in order to learn more about ways to improve their lifestyle or prevent health related issues. Genetic data-collecting may want to collect as many points of user data as possible in order to distribute it to researchers and learn more about population level trends to identify opportunities for innovation or intervention. For profit companies may be incentivized to collect data to sell to pharmaceuticals. While both may have some overlapping interests like improving general health and wellbeing for future at-risk patients, often times the priorities are at odds.

Privacy trade-offs can correlate with conversations around benefits and costs. Researchers have conceptualized ways of understanding human needs and values like privacy in product design. An Annenberg School for Community study[6] at the University of Pennsylvania questions the premise and outlines that "a majority of Americans are resigned to giving up their data—and that is why many appear to be engaging in trade-offs." Americans consent to data-collection because the benefits are worth the costs when in reality, many feel resigned about the "inevitability of surveillance and power of marketers to harvest their data." A Value Sensitive Design concept highlighted by Friedman et al.[7] posits that humans conceive trust through analyzing the harms, the good will "others possess toward them" and whether the harms that happen "occur outside the parameters of the trust relationship." As conversations related to policy creation, many attendees went into depth about organization values, implementation and the framework for decision making.

Some attendees highlighted potential negative impacts to framing privacy protections as binary trade-offs. In terms of product design, the challenge is often to find a balance between personalization and anonymization of the service. By using this framing, one assumption is that end users must fully lose user empowerment to achieve user ease. "What is the right balance between the two?" one attendee asked. Conversely, some appreciated having the trade-off framework to highlight where some decisions may create unintended consequences and inefficiencies elsewhere.

Several members expressed the importance of not oversimplifying privacy at the cost of speed, ease, and familiarity. There must be more education and public awareness around the nuance of privacy depending on the context, users, and challenges that may uniquely exist in a certain industry. The following case studies aim to highlight some of the similarities and differences that exist across four organizations who attended the event.

[5] Friedman, Batya, et al. "Value Sensitive Design and Information Systems." SpringerLink, Springer, Dordrecht, 11 Dec. 2013, https://link.springer.com/chapter/10.1007/978-94-007-7844-3_4.

[6] Turow, Joseph, et al. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation." SSRN, 10 Aug. 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060.

[7] Friedman, Batya, et al. "Value Sensitive Design and Information Systems." SpringerLink, Springer, Dordrecht, 11 Dec. 2013, https://link.springer.com/chapter/10.1007/978-94-007-7844-3_4.

Case Studies

Case study #1: Salesforce

Integrating data privacy best practices into the Salesforce platform UI and APIs to create routine management

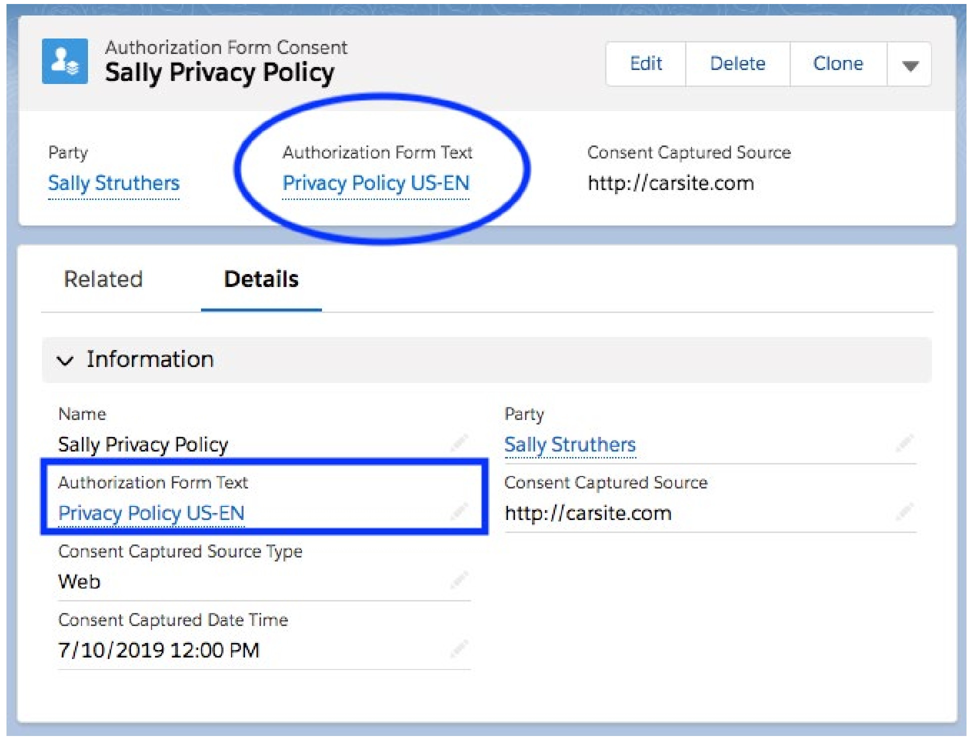
Marla Hay, Director of Product, Privacy and Data Governance, Salesforce
@marla_hay

Mission

To make it easy for companies to respect user data privacy through the Salesforce platform. Salesforce.com, Inc. is an American cloud-based software company headquartered in San Francisco, California.

Problem

- How might one ensure their products support their customer and end-user privacy needs? The Salesforce platform is highly flexible so that customers can create the interface they need, but what are the common privacy needs that can be supported in a more out-of-the-box way?
- What are the tools customers need to make it easy to give control of user data back to the end user? Currently customers have APIs and UIs to manage data, but what other low-code or no-code tools and best practices can be provided to give end users more control?



Authorization Form Consent
Sally Privacy Policy

Party: Sally Struthers
Authorization Form Text: Privacy Policy US-EN
Consent Captured Source: http://carsite.com

Information

Name: Sally Privacy Policy
Party: Sally Struthers
Authorization Form Text: Privacy Policy US-EN
Consent Captured Source: http://carsite.com
Consent Captured Source Type: Web
Consent Captured Date Time: 7/10/2019 12:00 PM

Figure A: The highlighted elements above in our recently released consent database (Consent Captured Date Time and Authorization Form Text) allow companies collecting user data to ensure that data uses have been agreed to and are restricted to those in the policy text. This allows them to incorporate data privacy more thoughtfully and consistently throughout the use of the platform.

Users

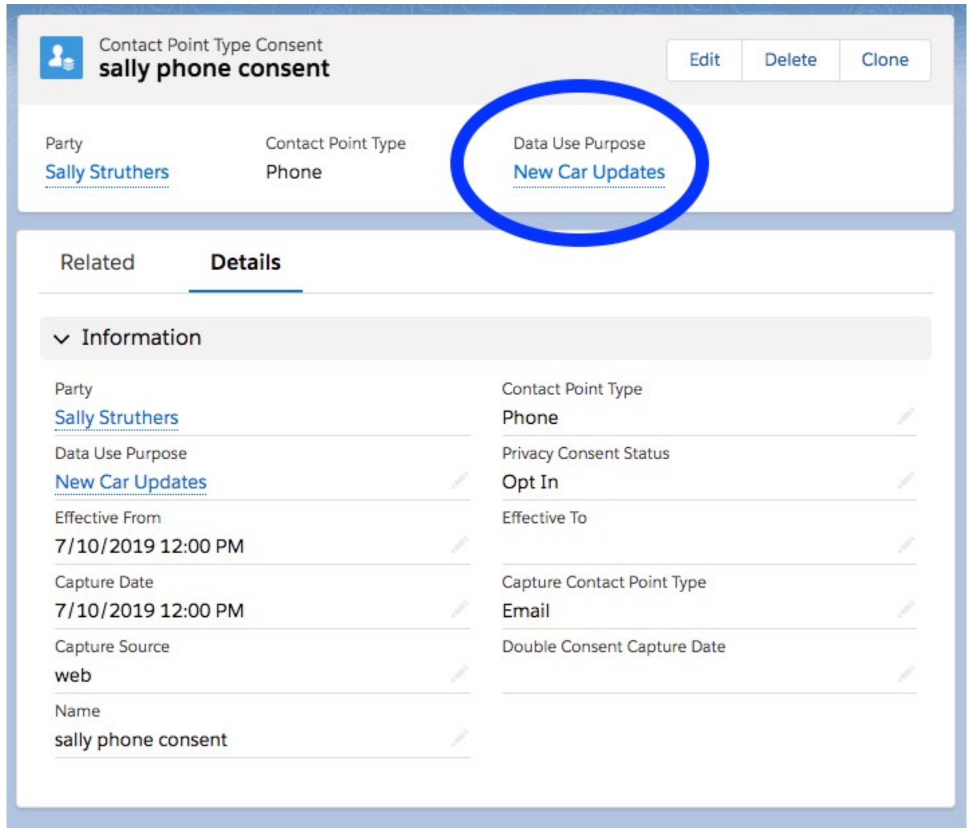
Salesforce customers are of varying sizes and industries, including nonprofits, universities, healthcare, finance, manufacturing/consumer packaged goods, B2B and retail companies. These companies use the Salesforce platform to power experiences for their own customers across sales, service, marketing, commerce and more, while also developing good data privacy practice for how they leverage their user's data. This includes: nonprofits, universities, healthcare, finance, manufacturing consumer packaged goods, B2B and retail companies.

Defining Privacy

“Privacy is personal information that belongs to an individual that should be protected and used by organizations only in accordance with the individual’s wishes.”

Approach: Embedding privacy and data governance features and functionality

Salesforce is developing privacy and data governance features and functionality through user interface, API, and application tools that provide intuitive best practices. Salesforce released a set of database objects, user interfaces, and APIs to help track consent for data captured in forms, such as privacy policies, with a discrete list of the data use purposes for those forms. Their customers can easily digitize and track who has consented to any form (e.g. a privacy policy, terms of service, or HIPAA agreement), for how long, and to what locale and version of a particular agreement. The end user can more easily see the data use purposes that are agreed to in the document.



Contact Point Type Consent
sally phone consent

Party: Sally Struthers
Contact Point Type: Phone
Data Use Purpose: New Car Updates

Information

Party Sally Struthers	Contact Point Type Phone
Data Use Purpose New Car Updates	Privacy Consent Status Opt In
Effective From 7/10/2019 12:00 PM	Effective To
Capture Date 7/10/2019 12:00 PM	Capture Contact Point Type Email
Capture Source web	Double Consent Capture Date
Name sally phone consent	

Figure B: Example user interface of the form functionality for integrated data privacy considerations. This portion of the UI allows customers to routinely set meta-data about the privacy policy that is used. The “Data Use Purpose” field reminds data-using companies and services to restrict data usage for the consent to only those outlined by the data use purpose.

Remaining Questions

- What are some best practice behaviors that Salesforce should model regarding transparency and data control? For example, what is the balance of giving the end user control vs putting onto them the onus of privacy management? Should an end user need to grant explicit consent for a cookie that manages their shopping cart, or is that something that the end user does not want to manage?
- How do end users expect consumer and business systems to behave with regard to collecting and using their data? For example, there is a divergence between the positive experience of personalization and the negative experience of having personal information used to create that experience. What is the right approach to ensure that user privacy is paramount while creating positive user experiences?

Legislative Considerations

What has been and will continue to be helpful are rules around transparency, data control, data sharing, and breaches that align organizations internationally onto a single standard. For example, GDPR outlines that a data subject has rights, such as data deletion and under what legal basis a data controller should retain data. The clarity of these rights have helped Salesforce better guide the development of their UI design, APIs, and development tools. It also outlines a process for reporting violations and the potential penalties for violators. These types of rules and clear penalties for violating those rules can help clarify for companies the guardrails in which they must operate.

Case study #2: Mapbox
Preserving user location data privacy with anonymization in the mapping industry

Tom Lee, Policy Lead at Mapbox | Twitter: @tjl

Mission

Mapbox offers a set of geospatial tools powered by location data with real-time updates, customization, and a developer-first approach. Mapbox reaches more than half a billion people every month, powering everything from the maps on weather sites to driving directions in cars' center consoles to location search in social media apps. Mapbox provides customizable building blocks to software developers who want to add location technology to their projects.

Problem

Mapping the world is an immense task that is growing larger as autonomy and ubiquitous sensors transform our cities. The removal of human operators from spatially aware systems also removes their capacity for judgment and error-correction, necessitating maps with more precision and recency than ever before. This is why Mapbox collects between two and three hundred million miles of anonymized telemetry data about end users' movements on a typical day. This data is used to find unmapped roads, observe traffic conditions, and detect vandalism in crowdsourced data. Mapbox is not the first to do this: Google Maps, Apple Maps and other competitors collect similar data from users for similar purposes, including as a default part of the iOS and Android operating systems.

Users

Unlike those large competitors, Mapbox isn't a consumer-facing company. Mapbox provides technology to businesses, who provide apps to consumers. Those consumers typically have no direct relationship with Mapbox. This means that Mapbox does not have names or emails for these consumers, nor accounts corresponding to them. Although Mapbox requires customers to provide their users with detailed disclosures about how their data is used and the ability to opt out of its collection, many users will probably never learn what Mapbox is or how anonymized data has built the maps they're looking at. Accommodating this fact shapes the company's policies and engineering decisions. According to Mapbox, "If we do our job right, users should be able to ignore us."

Defining privacy

"Users shouldn't have to worry about how their data will be used. This is central to what we think privacy means. Strong privacy controls are the way we provide that peace of mind. We collect no identifiers to connect back to an individual. The data is protected using industry-leading encryption and security practices. We use it to improve our maps--not to sell to advertisers."

Approach: Secure and anonymized telemetry

Telemetry data is collected when apps run Mapbox software. The code that does this is open source, so developers can see exactly how it works. Some identifiers (IDFA, AAID) are never collected. Others are stripped upon receipt of the data. Each trip's beginning and end is discarded. Next, the trip is segmented into chunks and any that appear stationary are discarded—these could include stops along a journey, or time spent at work or home. The remaining chunks aren't tied together by any identifier, so trips cannot be reconstructed. The resulting data--which is kept encrypted and under tight access control—is very useful for analyzing how patterns of travel happen across a city or country, but is useless for tracking individuals.

Remaining Questions

Anonymized telemetry allows Mapbox to preserve user privacy while providing accurate and reliable maps and location services. It has also enabled collaborations with researchers studying traffic patterns, and planners in Washington, D.C. working on the city's Vision Zero traffic fatality reduction plan. Mapbox believes it is capable of answering a broad set of useful questions, and is continuing to study ways to make the data accessible to researchers, planners and customers without compromising user privacy.

Legislative Considerations

Mapbox is able to compete against mapping platforms run by some of the largest corporations in the world, and can do so in part thanks to their telemetry strategy. That strategy is legally viable because most well-designed privacy laws, including GDPR, recognize the privacy advantages that come with deidentification and anonymization techniques, and treat such datasets differently.

Preserving this legal distinction is a critical concern for Mapbox. As a business-to-business company, their options for interacting with end users are limited. They have no way of connecting collected data back to the person from whom it originated, and consequently have no way to comply with data export or deletion requirements.

So far, this hasn't been a problem. Because collected data is anonymized, it is exempted from export, deletion, and similar requirements. But with congressional action on privacy reform in the U.S. looking less likely, states and even cities are beginning to draft laws of their own. Not all of these proposals are expertly crafted. Mandates that fail to recognize the privacy benefits conferred by anonymization techniques could complicate Mapbox's collection strategy. At worst, they would leave the mapping industry the sole domain of the handful of technology giants with whom virtually everyone has to maintain an account.

Case study #3: Center for Open Data Enterprise (CODE)
Protecting privacy and maximizing the public benefit of health data

Name / Contributor + Role + Twitter handle:

- **Katarina Rebello**, Director of Programs | Twitter: @kmrebello
- **Joel Gurin**, President | Twitter: @joelgurin
- **Paul Kuhne**, Roundtables Program Manager

Mission

The Center for Open Data Enterprise (CODE) is an independent nonprofit organization based in Washington, D.C. whose mission is to maximize the value of open government data for the public good.

Problem

Emerging health-related technologies—from at-home DNA testing kits to personal fitness trackers—are raising major questions about health data privacy. While the data generated through these technologies can be valuable for improving treatment, diagnosis, and patient care, it often falls outside the purview of the Health Insurance Portability and Accountability Act (HIPAA), which is the primary framework for managing health data privacy in the United States. HIPAA rules and regulations, including the HIPAA Privacy Rule, apply to health plans, healthcare providers, clearinghouses, and their business associates. Data from emerging health-related technologies is, however, increasingly being handled by stakeholders that are not covered by HIPAA, such as software vendors and third party data brokers. This situation has left several kinds of health data unregulated and vulnerable to potential misuse.

Users

CODE is looking at this health data privacy challenge through the lens of maximizing public benefit, specifically to patients and patient advocates. Gaps in health data privacy protections can directly impact the quality of care that patients receive. In some cases, software vendors and third party data brokers may have more access to health data than patients and their doctors. Patients must be empowered to make decisions about their health data - including who is using it and for what purposes. This is not currently possible given that some health data is protected under health data privacy frameworks such as HIPAA while other health data is not.

Defining privacy:

"Health data privacy is the protection of sensitive health information, such as an individual's medical conditions, health insurance records, genetic information, and fitness activities, with appropriate provisions for sharing and utilizing this information in ways that the subject of the data is aware of and has consented to."

Approach: Data privacy and access focused roundtables at HHS

Through a project on Sharing and Utilizing Data to Enhance and Protect Health and Well-Being, CODE is hosting three Roundtables during 2019 in collaboration with the Office of the Chief Technology Officer (CTO) at the U.S. Department of Health and Human Services (HHS). In July 2019, one of these Roundtables focused on how to balance health data privacy with appropriate data access in the public and private sectors. Over 60

Roundtable participants, including patients and patient advocates, shared their diverse perspectives on actionable next steps that can be taken by HHS and other key stakeholders to improve data privacy protections while enabling use. Much of the day's discussions centered around the limitations of HIPAA in today's health data environment.

Several Roundtable participants specifically emphasized the need to develop meaningful legal guidelines for health data collected by entities that are not covered by HIPAA. The legislation introduced by U.S. Senators Klobuchar and Murkowski in June 2019 is one possible route. Others noted the importance of developing targeted education for patients and stakeholders in the healthcare system about what *is* and what *is not* under the purview of HIPAA. CODE will publish a public summary report of the findings with specific recommendations for HHS and other relevant stakeholders in Fall 2019. In 2020, CODE will also disseminate the results of all three Roundtable to a broad audience, including patients and patient advocates around the country. For updates on CODE's work, please visit OpenDataEnterprise.org and follow CODE on Twitter at @odenterprise.

Remaining Question

Should HIPAA be updated to address data privacy questions around non-covered entities or should separate regulatory frameworks be developed?

Legislative Considerations

Increased public awareness about current health data privacy legislation, to understand the full scope of their existing rights, and advocate for expanded protections in the future.

Case study #4: Georgetown Ethics Lab

Learning from Non-Use: Active Resistance + Data Privacy Workshop for Designers

Jonathan Healey, Assistant Director, Georgetown University Ethics Lab

Sydney Luken, Designer, Georgetown University Ethics Lab

Mission

The Non-Use Project is an initiative led by designers at Georgetown University's Ethics Lab that develops new design practices that promote responsible development of data-collecting technologies and policies. The team works with students and designers of data-collecting technologies to flip the "user-centered design" paradigm. Instead of emphasizing how people use products or services, focusing on active resistance to these technologies as signals of potential blindspots with broad social impacts empowers students and designers to turn these signals into opportunities for responsible innovation.

Problem

The word "use," which is fundamental to the culture of computer technology, reduces the lived experience people have with technology to a measure of utility (e.g. how much a person uses an app). In this conception, people are classified as either "users", potential users, or deliberately disregarded. This limited framework contributes to how designers frame key metrics for positive "user experience" through emphasis on convenience, ease of use, and delight. When a "good" experience is so narrowly defined, morally salient concerns such as privacy are insufficiently considered. This dilutes what should be a rich conversation about individual and collective rights to a debate about the right number of checkboxes or literacy standard needed to qualify as informed consent.

Participants

To reframe conversations of use, the design team at Georgetown University's Ethics Lab has been hosting workshops for designers and researchers working on data-collecting technologies across a range of design disciplines, including interaction design, user experience design, system design, and service design. Participants have included designers from some of the largest e-commerce businesses, internet of things companies, and media companies.

Defining Privacy

Privacy is a broad concept with many conceptions (e.g. spatial, decisional, associational, etc.).[8] It is not our aim to provide a single definition, but rather to expose designers to its multitude of meanings so that they can recognize and respond to complex concerns about their products. When it comes to data-collecting technologies, privacy concerns may include control of one's data, control of one's image, freedom from tracking habits and interests, and other forms of digital surveillance."

Approach: Design Workshops to Highlight User Privacy Needs

Through an on-going series of creative workshops, The Non-Use Project is helping designers recognize and expand their user-centered mindset to imagine alternatives for the protection and promotion of privacy rights.

Throughout the series, The Non-Use Project reframes the conversation of use through non-use, with an emphasis on active resistance—defined as a positive effort to resist the undesired outcomes of using a product or its features—as essential feedback for responsible design. The Non-Use Project examines personal narratives of active resistance collected through our project team's conversations with people who maintain nuanced relationships with particular data-collecting technologies, such as social media accounts or biometric access control.

Participants practice recognizing the value claims (privacy as information control; privacy as freedom from inference, etc.) and assertions (deactivating accounts, deleting apps, using features in unintended ways, etc.) implicit in the narratives. They reflect on their own experiences as designers who may have actively resisted technology themselves to better understand the values, expectations, and sense of responsibility that shape their relationships with privacy and technology.

[8] Bert-Jaap Koops; Bryce Clayton Newell; Tjerk Timan; Ivan Skorvanek; Tomislav Chokrevski; Masa Galic, "A Typology of Privacy," University of Pennsylvania Journal of International Law 38, no. 2 (Spring 2017): 483-576. https://heinonline.org/HOL/P?h=hein.journals/upjiel38&i=489.

See also: Daniel J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review 154, no. 3 (January 2006): 477-564. https://heinonline.org/HOL/P?h=hein.journals/pnlr154&i=491.

Questions for reflection and ideation include:

1. What does privacy mean to me?
2. How do I use [a data-collecting product or service]?
3. How have I actively resisted using it?
4. How do other people actively resist using these products or services?
5. How *should* people be able to communicate their concerns about privacy through their interactions with a data-collecting product or service?

Drawing on normative and ethical insight as a source of inspiration, the workshop experience underscores the innovative potential of a values-driven process. Participants uncover "non-user research" questions to recenter problem framings around social or ethical concerns rather than measures of use. In the course of imagining new means for supporting privacy, participants often discover how prominent—and constraining—their own unconscious reflex towards "user-centered solutions" is, and in so doing discover opportunity for new creative pathways.

Remaining Questions

- Designers today understand other values, such as environmental sustainability, as core to their industries. What will it take to recognize data privacy as a core value, and express that value through every product or service they create?
- How can designers, developers, and policy leaders better engage their own status as users, non-users, and community members in order to develop and steward their products more responsibly? In other words, how can they bring their sense of right and wrong into their work, rather than leaving it at the office door?

Legislative Considerations

These workshops attempt to shape the formative process of data-collecting technology. This work would be reinforced by stronger legal protections for people who demonstrate their intent to withhold, retrieve, or delete data about themselves. Complementary legislation should provide institutional support, such as licensure, for professional communities to actively account for their responsibility to the common good, including the protection of privacy rights.

Conclusion

After the workshop, we spoke with attendees in-person and gathered survey feedback to understand the key takeaways moving forward.

It is unique to have opportunities to meet with design or engineering tech practitioners, Hill staffers and/or researchers in a collaborative environment related to data privacy. This event presented an opportunity to better bridge conversations across sectors in the future. Structured local, national and transnational efforts to share ideas, ask questions, seek advice and collaborate would be beneficial to continue bridging gaps and seek inspiration from teams who have successfully addressed similar challenges. We saw evidence of several attendees who continued to invite one another to related events in similar topics of data privacy. While the discussion in May was largely U.S. focused, more international precedence and examples could help inspire and influence different types of efforts.

Marginalized voices in policy (e.g. social justice and civil liberties groups and technical expertise) should continue to be integrated into conversations from the beginning that span legislative mandates to definitions of bias in processes or narrative construction to increase public awareness. Data collecting technologies have brought disproportionate harm to the most marginalized communities. Researchers have noted the long-term, "devastating consequences of being poor in the digital age[9]" and exposed racial disparities[10] in facial recognition technologies that can lead to imprisonment, or worse. Privacy-protecting initiatives should continue to seek diversity of voices across industries and backgrounds. Policymakers, practitioners, and academic researchers should work collaboratively on evolving policies. Attendees highlighted several ideas:, data protection regulation should enable a balance between user empowerment and legal and policy protections. There should be accountability and effective penalties on how data is collected, is processed and flows through a system. Product and backend data systems should acknowledge their incentives and abide by the intent and needs of the data subjects or end users.

A final major theme included the lifecycle and process of policy testing and implementation. How might we be able to create additional opportunities to test and research iterative technical policy requirements to align with new product creation? These questions are not new to those working in government and public sector teams. As digital technologies were introduced, gaps and improvements in policies pressed the need for quicker and more transparent feedback loops. Often, the regulatory policy cycle takes long enough that the systems are then outdated. How might we be able to continue working with iterative methods to ensure that we can parallel laws and new technological uses? Non-profit organization Code for America have championed[11] the importance of bringing user research and usability testing to the culture of product development instead of fewer, massive releases that are often the norm. Some researchers have highlighted the importance of incorporating systematic processes like Privacy Impact Assessments (PIAs)[12] between practice and policy. Across the board, attendees voiced both curiosity and the importance of learning more about how their organization could potentially be involved to contribute and enhance data privacy policies as they evolve.

The data privacy workshop offered the opportunity to foster connections and learn about common questions, themes and challenges in different subject areas. There is ample opportunity to continue spurring conversations and bridging communities across sectors. Many thanks to Belfer Center and New America Foundation for coordinating and convening this event.

[9] Madden, Mary. "The Devastating Consequences of Being Poor in the Digital Age." *The New York Times*, 25 Apr. 2019, https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

[10] Hardesty, Larry. "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems." MIT News, 11 Feb. 2018, http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[11] Pahlka, Jennifer. "Beyond Tech: Policymaking in a Digital Age." Medium, Code for America Blog, 30 Mar. 2017, https://medium.com/code-for-america/beyond-tech-policymaking-in-a-digital-age-2776b9a17b69.

[12] Clarke, Roger. "Privacy Impact Assessment: Its Origins and Development." *Computer Law & Security Review*, Elsevier Advanced Technology, 2 Apr. 2009, https://www.sciencedirect.com/science/article/pii/S0267364909000302.

Technology and Public Purpose Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/TAPP

Printed in the United States of America