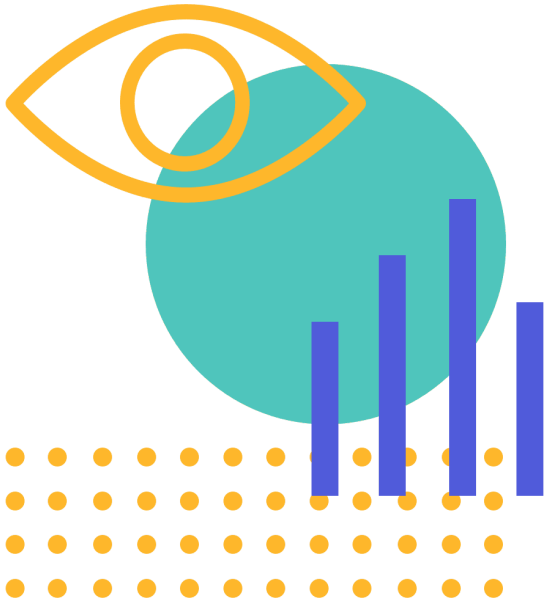
Project Let's Talk Privacy
Full Report

Exploring how privacy and data governance policies translate into practice



Anna Chung
Dennis Jen
Jasmine McNealy
Pardis Emami Naeni
Stephanie Nguyen

June 2020

Table of contents

Style, Deliverables, and Key Concepts

Style & how to read this document

Citations in the full report	Online native and news are hyperlinked. Scholarly works are accompanied by APA note citations.
We, us, our	Our team who conducted and authored the report (See Section 8: Team)

Research deliverables

Full report	This document contains the full comprehensive outputs of our research aimed at academics, researchers, and policymakers who may be interested in diving into more details of our research grounding, methodology, in-depth themes and recommendations. (Section 1-5) = rationale, process, methodology. (Section 6) = insights, findings, recommendations.
Report summary	https://letstalkprivacy.media.mit.edu/research We created a document in between the high level glimpse of a one-pager and a full report with ~50 pages that provides more detail in a digestible format. This is also aimed at researchers, policymakers, and a more general audience who are interested enough to see the prioritized findings with some nuance, without the detail of methodology and a comprehensive view on all of the themes and recommendations we compiled. We anticipate that this document will summarize our research in a readable, quick, and prioritized format.
Recommendations one-pager	https://letstalkprivacy.media.mit.edu/research We created a one-pager aimed at a policy, media and industry practitioner audience. The goals of the one-pager are to

	synthesize high level themes and recommendations on one page, optimized for skimming. While this document does not include substantive detail, it provides an opportunity to prioritize the takeaways of the report and mimic many one-pager policy documents that are already an industry norm in policy environments.
Policy prototyping guide	https://letstalkprivacy.media.mit.edu/research We created a downloadable guide to give policymakers a template process for prototyping bills to help them iteratively improve policies before publishing. We include a high level process diagram, an outline of the ideal team and roles, and a skeleton structure that policymakers can use to integrate prototyping in their processes. This document is meant to be modified depending on the resources available for each team.
Website	https://letstalkprivacy.media.mit.edu/ We created a website aimed at a more general, non-technical and non-policy audience interested in learning about privacy policies and how they might translate into different experiences with online platforms. We designed the website for quick skimming so that people could explore different bills as desired. We highlight the high-level summary of the bills, prototypes, research, and people involved in the project.

Glossary

Bills	Bills are draft laws. We interchangeably use the term "legislative proposals" or "bills". What we refer to in the report are bills AND draft bills (since some proposals were not formally introduced).
CCPA	California Consumer Privacy Act
COPRA	Consumer Online Privacy Rights Act

COVID-19	On February 11, 2020 the World Health Organization announced an official name for the disease that is causing the 2019 novel coronavirus outbreak, first identified in Wuhan China. The new name of this disease is coronavirus disease 2019, abbreviated as COVID-19. Source: CDC
DPA	Digital Privacy Agency - one of the possible recommendations for the Online Privacy Act
GDPR	General Data Protection Regulation
OPA	Online Privacy Act
Prototype or Prototyping	A sample version of how a product or service would look, often used to gather feedback and test with people before deploying a final version
SMART Act	Social Media Addiction Reduction Technology Act
User (Person, Individual, Human, etc.)	When we **referred to** “user”: We mean the individual using the product or service. For specific use cases and recommendations on designing and developing tools and related policies, we use the word "user" since the terms have specific meaning in the context we use it in. We also did not replace it where “user” was used as an adjective as opposed to more of a noun. For example: User research, User experience, User data, User interface are all words we maintained. Additionally, where we quote people who used “user” - we kept. When we **did not refer to** “user”: We made an attempt to avoid using “user” when talking about the people, individuals, who use or are influenced by technologies, platforms, processes or services. Why? We recognize the term may unintentionally put people into a category of “research subjects” as opposed to humans with rights and the agency of choice, etc.. Instead, we interchangeably used other terms such as: individual, person, human, etc.

UX - User Experience	Interactions a person has with a product or service, which can affect their attitudes and emotions towards it
UI - User Interface	Graphical layout of an application that a user directly interacts with
UR - User Research	Methods aimed at understanding user behaviors, needs, and motivations

1. Executive summary: Project Let's Talk Privacy

Project Let's Talk Privacy explores how the implementation of privacy and data protection policies might impact people and communities in practice. Our project title reflects our work in engaging a more diverse set of voices into conversations around privacy and data governance. How do these policies translate in practice? How might they affect us? To find out, we interviewed 41 people – including lawyers, designers, engineers, advocates, policymakers, and stewards of sensitive data (social workers, pediatricians) – about three federal draft data and privacy related bills. Our objectives were to 1) explore intersections of privacy policy and design through visual prototypes; 2) identify the challenges of translating policy to platform changes based on the specific background and industry skill set of the interviewees; and 3) understand broader perspectives of privacy and control in technology.

Recommendations for policymakers

1. Build on existing policymaking resources and processes. Processes currently exist for people to provide feedback to Congress at the federal level. For legislation, Americans can call or write to their Representative or Senator directly. Legislators also often reach out to stakeholders for feedback, but we urge increased cross collaboration and more proactive ways to reach out to communities to better understand how to effectively communicate policy to design and development. We recognize there are several existing efforts to bridge the divide between technology practice and policy, including TechCongress, The Aspen Tech Policy Hub, AAAS Fellows, Code for America, Mozilla Fellowships, New America's Public Interest Technology team, and more. Congressional committees, the Congressional Research Service or the Office of Technology Assessment (if revived) may be well positioned to house staff to prototype policies.

2. Talk to stakeholders who may experience data-related harm first-hand and integrate their perspectives into the policymaking process. A lack of engagement with constituents currently exists in policymaking. The voices of the individuals are often translated second- or third-hand in reports or mediated through advocacy organizations. Policymakers must gather insights directly from individuals with lived experience and/or data stewards (pediatricians, social workers, librarians) who understand impacts of marginalized or vulnerable communities who may be most adversely impacted by policy. Rather than ask for *solutions*, policy teams should attempt to understand the nature of the data stewards' work with regard to data privacy and how policies have impacted people. Data stewards can provide concrete use cases where policies have negatively impacted and continue to negatively impact their communities.

3. Continue to collaborate directly with individuals and privacy-minded experts in advocacy organizations, industry, academia, and government *throughout your policy process*. Loop in existing networks and broaden contacts in advocacy organizations, industry, academia, and government, branching out to different perspectives along the way**.** Policymakers should solicit

help from industry practitioners and community advocates to design and test policies with low fidelity versions of prototypes — when relevant and possible. This may allow policies to be tested in small, low-risk, time-boxed environments that relate to a bill's intended audience. Reaching out to collaborators can help provide policy implementation examples, frameworks, studies, and stories of trial and error to help advance policy work.

To assist with 2 & 3: We created a Policy Prototyping Guide (Appendix C), a roadmap for the roles needed and the step-by-step process that policymakers can follow to pilot bills in practice. This Guide is meant to be modified as needed. Alterations in the policy research, prototyping, and drafting process may allow for better alignment of policy needs with actual outcomes.

4. Recognize the need for precision and evidence: major findings from our interviews highlight a strong desire to link policy action to research and evidence. First, policymakers need to articulate the specific problems and associated harms they are trying to solve. Second, it should be clear from both the bill language and public discussion that policymakers have consulted with research to ensure that the regulations that they are attempting to create are viable. Speeches, press releases and, more importantly, committee hearings can be better tools to highlight research to help create the case for more viable policy recommendations.

5. Implement human-centered practices in the policy design process. Bills can be summarized with messaging aimed at industry practitioners and advocacy organizations, without oversimplifying the law's focus and the governance process. When possible, prototype policies and work with practitioners to design and test policies with low fidelity prototypes. Explore how to test policy and prototype processes on a larger scale by partnering with academic institutions and other organizations for beta testing to see if it is possible to test the policies in small, low-risk, time-boxed environments. Continuously integrate feedback by collaborating with privacy-minded experts in advocacy organizations, industry, and academia throughout policy development.

6. Strike a balance to avoid being overly specific and future-proof for evolving technologies. When possible include examples in the legislative history and common use cases illustrating what terms may mean or look like in practice. This gives more fidelity to obscure topics without anchoring policymakers to information that is too specific. At the same time, policymakers should avoid being overly specific. If too granular, the specificity in bill language can be seen as arbitrary. Language should consider changes in future technology. Definitions of key terms are incredibly helpful, but some terms, if defined, may quickly become outdated due to evolving technologies. For instance, one policymaker we spoke with said the term "sensitive data" is difficult to define. A decade ago, people may not have considered geolocation data sensitive because it was not as pervasive and easily aggregated with other data points from platforms as it is now. This issue is further exacerbated in that many of the bills focus on one major aspect of data collection and privacy — usually the social — and neglect environmental data collection.

Recommendations for design practitioners and technology organizations

1. Recognize that individuals want to be empowered to control what can be done with data, without overburdening or diminishing the platform experience. Organizations must consider individual and community impacts of changing user control between passive (enabling privacy forward settings by default) and active (requiring individuals to update their settings). Understanding this will require investigating how people understand the process that organizations use to collect, use, and share personal information. To better empower individuals, organizations should enhance their transparency practices by informing people (both users and the public in general) about their rights and offering them data protection choices: control over data sharing, data selling, data deletion, and more. Of paramount importance is that organizations codify choice – enshrining individual decisions into the design of the system. Organizations should, for example, provide granular controls for the kinds of information an individual chooses to share, practice data minimization, or not collect data at all without allowing individuals to decide whether or not they wish to participate in the data use scheme.

2. Develop shared vocabulary and patterns across industries. Designers within organizations should also work with other industry personnel, those in advocacy, and policymakers to develop a common vocabulary, which can be useful for understanding and explicating data governance and information privacy. The U.S. Web Design System, for example, created a "shared design vocabulary" for web design. This resource is an open source repository for any government agency (aimed at the federal level) to build accessible, mobile-friendly government websites and includes components, design tokens, utilities and page templates.

On individuals who or are impacted by these systems:
We decline to offer recommendations to users (and non-users) beyond contacting their representatives, in recognition of the power asymmetries between individuals and platforms, governments, and other organizations. It cannot be incumbent upon individuals to protect themselves from technologies deployed upon them, particularly when they are increasingly required to use several forms of technology to navigate work, entertainment, healthcare, banking, and other parts of everyday life.

2. Intro letter from the team: Why now?

When we began this project in September 2019, policymakers in the U.S. were exploring the possibility of comprehensive federal privacy policy. Both the General Data Protection Regulation (GDPR), which was enacted in April 2016 but went into effect in May 2018, and the California Consumer Privacy Act (CCPA) that went into effect in January 2020, attracted attention from privacy experts in academia, law, industry and advocacy interested in following the impacts of these laws on industry and the rest of society.

During the months we've been working on this project, privacy and data protection conversations have evolved daily. From international privacy legislation, to historic penalties against large tech platform companies, to child safety with Pokémon Go — these events have shaped conversations around privacy norms and structures in our governing institutions and homes. Now the tenor of these discussions has changed.

Starting around late January 2020, countries around the world began following the exponential transmission of the coronavirus, which would later be the first time the World Health Organization would declare a pandemic outbreak since the H1N1 swine flu over a decade ago. Governments and organizations around the globe turned to geolocation technologies to map and monitor infected people and interactions, sparking concerns around surveillance, intrusive tracking, and unwelcome data sharing to unknown third parties.

China began to require citizens to install software on their smartphones that issued people color codes to indicate health status and "appears to share information with police," reported the New York Times. NSO Group, an Israeli malware and spyware vendor and Clearview AI, a controversial facial recognition company linked with global law enforcement agencies has been in talks to institute COVID-19 tracking. Academic research teams like Private Kit (2020) from MIT, COVID Symptom Tracker (2020) from King's College London, Singapore's Government Digital Services, and FluPhone (2003) from University of Cambridge are currently or have previously instituted tracking apps to follow the pandemic spread. The hopes for any of these tracking apps are to elucidate and reduce the spread of the virus in communities around the world through crowdsourcing large data sets in real-time. In addition to contact tracing, people are working from home more and using tools that contribute to an increased digital and data footprint.

With pandemic tracking, there is growing concern about the risks to individual privacy. Policymakers have responded to take a stance to protect people's privacy. Representatives Anna Eshoo, and Suzan DelBene, along with Senator Ron Wyden, and Senator Markey wrote letters to the President and Vice President, urging the adoption of a set of privacy principles that focus on management, use, and best practices during a pandemic. Republican Senators are proposing to submit a U.S. privacy bill related to contact tracing. Similarly, thirteen advocacy organizations galvanized and wrote to Congress, highlighting their tenets for user data

protections. Everyday people continue to grapple with the complexities of such data privacy trade-offs during a dangerous public health crisis. For example, Consumer Reports has reported that videoconferencing systems like Skype, Webex, and Meet have flaws across the board — there is no single trusted platform. While our work began several months ago, the insights and questions that our research surfaces are both timely and relevant to the current pandemic.

There are two sets of issues to be considered. First, we categorize the privacy issues that were germane *before* COVID-19 which these proposals sought to address, and which we explore in this research. Second, there are a set of issues specific to COVID-19, such as rules around public health data collection from government entities and technical contact tracing capabilities, which are beyond the scope of this study at this time. It is important to note that privacy policy discussions both before and after COVID-19 are not mutually exclusive; the issues overlap around strengthening privacy protections from technical implementations in the public sphere. The emergent conversations around government surveillance and privacy during this pandemic are mentioned here as an important reminder of why privacy is such an important and fraught space.[1]

These findings and recommendations, where implementation is possible, may bring us closer to understanding privacy nuances across contexts, and provoke us to explore opportunities to prototype policies with the goal of making new and existing laws work for individuals and organizations.

[1] We also recognize the differences and relationships between data privacy and data protection. While data privacy refers to use of personal data, data protection focuses on information security.

3. Motivations: Problem, Objectives, Goals

We focus on two key problems we have identified through our work and our research: First, operationalizing privacy policies into practice is nebulous and challenging. How do we translate, measure, and test values and high level aspirations into a human interface? Second, there is a natural silo between industries making integration across industry, policy, and academic research difficult. How do we bring these sectors together to better serve everyday people?

One objective we set out to accomplish was to explore intersections of privacy policy and design through visual prototypes. We also aimed to understand the challenges of translating policy to platform changes based on the specific background and industry skill set of the interviewees. Lastly, we sought out to understand broader perspectives of privacy and control on social media.

Based on the objectives above, we outlined more granular goals of the project:

- Show how realistic designs can define the selected draft privacy policy.
- Analyze and explain the impact of draft bill language and designs they inspire.
- Educate and engage the public on recent draft privacy bills and the challenges of implementing policy to practice.

4. Grounding in related privacy, policy, design work

For much of modern history, informational privacy has often been controlled by the powerful and designed by the minority, as demonstrated by the dominance of particular platforms and technology organizations. Today, in just 60 seconds, the world produces 4.5 million Google searches, 1.4 million Tinder swipes, and 277 thousand Instagram stories. Platform and organizational dominance, coupled with the massive volume of personal data used for businesses, government agencies, and civil society organizations, make individuals uniquely vulnerable to data collection, manipulation, and insecurity. For context, data breaches in 2019 exposed 4.1 billion records which came in the form of data, including banking information, login credentials, and location data to name a few. Much of the tangible risk that comes from these data breaches is the exposure of individual credentials in the form of email and passwords. “Email and password re-use across various services is rampant simply because it is hard for people to remember too many passwords,” explains Peter Dolanjski, former Director of Privacy & Security products at Mozilla. “This leads to credential stuffing or spear-phishing attacks, enabling the attacker to gain access to sensitive accounts such as email or financial accounts.”

Personal data is used in decision-making technologies in various sectors, including healthcare, finance, education, and entertainment systems[2]. To provide recommendations to individuals and communities, these systems are typically trained on data that may provide granular insight

[2] See O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Broadway Books.

into the lives of individuals—often without them being fully aware that data is being collected.[3] It is well documented that this kind of data collection and usage can lead to several kinds of harm ranging from loss of economic opportunity to social stigmatization to discriminatory criminal justice outcomes.[4] Along with harms possible from algorithmic and machine learning systems, organizations continue to inflict more common privacy harms on people. In response, both state and federal legislators have proposed an increasing number of draft bills aimed at protecting privacy. Many of these bills focus on data protection through the lens of design.

By design we mean that these proposed laws focus in whole or in part on system processes and user experience. For instance, a design feature used by many social media platforms is rating mechanisms (up or down vote) or "like" buttons. The visual design of a "like" allows the individual to bookmark information or to send a graphically based response to someone else's post. At the same time, "likes" and their permutations provide organizations with data allowing for the creation of inferences about an individual's affinities, including political affiliations,[5] mood and emotions,[6] and possible purchasing behavior,[7] and can identify trusted people who could ultimately influence them. This data, then, has implications for how an individual may experience the site, from the advertisements shown to the kinds of content and posts they encounter — much of it in an attempt to persuade the individual to spend more time and, therefore, disclose more data.

Dark patterns — designs aimed at persuading individuals to behave in desired ways counter to what might be beneficial to them[8] —– have come under increased scrutiny with the rise of data-collecting products and services. Called *dark* because people may not recognize the persuasive qualities of the specific design element, these features may provoke surreptitious manipulation of people. Additionally, the options that people may most desire (like deleting an account or unsubscribing their email) are sometimes obscured or hard to find. The purpose of the manipulation may include to force continuity in email subscriptions or shame people into compliance or misdirect people to enable data mining and maximum data collection. These actions created through design may be counterintuitive to someone's preferred intentions with data sharing. Design in general is motivated by a variety of factors from data collection incentives to profit models to desired individual behaviors and goals. A design element itself is

---

[3] Gurses, S., & Hoboken, J. van. (2016, August 9). Privacy after the Agile Turn. Retrieved May 11, 2020, from https://osf.io/preprints/socarxiv/9gy73/

[4] Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. N.Y.U. L. Rev. Online, 94(15) pp. 15-55.

[5] Kristensen, J. B., Albrechtsen, T., Dahl-Nielsen, E., Jensen, M., Skovrind, M., & Bornakke, T. (2017). Parsimonious data: How a single Facebook like predicts voting behavior in multiparty systems. PloS one, 12(9).

[6] Bazarova, N. N., Choi, Y. H., Schwanda Sosik, V., Cosley, D., & Whitlock, J. (2015, February). Social sharing of emotions on Facebook: Channel differences, satisfaction, and replies. In Proceedings of the 18th ACM conference on computer supported cooperative work & social computing (pp. 154-164).

[7] Zhang, Y. & Pennacchiotti M. (2013). Predicting purchase behaviors from social media. In Proceedings of the 22nd international conference on World Wide Web (WWW '13). Association for Computing Machinery, 1521–1532. DOI:https://doi.org/10.1145/2488388.2488521

[8] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-14).

difficult to distill as “dark” or not, as the design often depends on the intent of the designer or institutional culture in which they are embedded. However, people have questioned motivations of organizations that appear to engage in human deception and covert data collection. “This is particularly problematic given the power imbalances and information asymmetries that already exist between many service providers and their users,” reports the Norwegian Consumer Council in 2018. “Most users cannot accurately ascertain the risks of exposing their privacy.” Placing a focus on privacy design reveals that processes of data collection are not created with an emphasis on individual privacy protection.

Human computer interaction researchers have studied and created privacy design with a focus on improving individual awareness and behaviors,[9] by visualizing past personal privacy disclosures.[10] These include approaches like nutrition labels,[11] privacy icons, and nudging[12] to improve individual choices online. Scholars like Helen Nissenbaum and others explored measuring and implementing[13] the concept of privacy as contextual integrity[14] and showed how it can be both measured and implemented in practice. In 2009, Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canadia, created Privacy by Design (PbD)—a framework of 7 principles aimed at calling for privacy to be considered at all points of the systems engineering process.[15] Though criticized as being vague as well as prioritizing the interests of corporations over the interests of consumers in understanding privacy by design,[16] PbD principles have been codified in the European General Data Protection Regulation.[17]

Foundations, governments, and nonprofit organizations have instituted various initiatives to raise awareness of the importance of privacy design and policy. For example Electronic Frontier Foundation and Mozilla wrote a public letter to Venmo to change their “public-by-default” sharing feature based on design research that spurred a petition that garnered over 25,000 signatures. Access Now created a list of design and development recommendations to “guide

[9] Florian Schaub, Rebecca Balebako, Adam Durity, and Lorrie Faith Cranor. A Design Space for Effective Privacy Notices. SOUPS 2015, Ottawa, Canada, July 22-24, 2015, 1-17.
[10] J. Kolter, M. Netter and G. Pernul, "Visualizing Past Personal Data Disclosures," 2010 International Conference on Availability, Reliability and Security, Krakow, 2010, pp. 131-139.
[11] Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009, July). A" nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security (pp. 1-12).
[12] Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon et al. "Nudges for privacy and security: Understanding and assisting users’ choices online." ACM Computing Surveys (CSUR) 50, no. 3 (2017): 1-41.
[13] Kumar, P. (2018, September). Contextual Integrity as a Conceptual, Analytical, and Educational Tool for Research. Retrieved April 8, 2020, from https://privaci.info/symposium/Kumar-PrivaCI-Paper-Final.pdf
[14] Barth, A., Datta, A., Mitchell, J. C., Nissenbaum, H., Stanford University, Stanford University, ... New York University. (2006, May 1). Privacy and Contextual Integrity: Framework and Applications. Retrieved from https://dl.acm.org/doi/10.1109/SP.2006.32
[15] Cavoukian, A. (2009). Privacy by design. Take the challenge. Information and privacy commissioner of Ontario, Canada, available at: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf.
[16] van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2012, October). Designing privacy-by-design. In Annual Privacy Forum (pp. 55-72). Springer, Berlin, Heidelberg.
[17] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

decision-makers, developers, and auditors in their evaluation of contact tracing apps." In terms of highlighting dark patterns, the Norwegian Consumer Council conducted a report on dark patterns through case studies, showing their prominence and how they give the "illusion of control", and Consumer Reports created an evaluation framework, putting repeated pressure on companies to require consent when asking for more data or provide privacy friendly options available as the default. Mozilla served as a bridge between researchers & the EU Commission to develop recommendations for what a good ad transparency product should look like.

There is momentum to explore the space of privacy, design, and policy through work across academia, the public, and private sectors. The context above outlines the creative work happening in this space and the types of impact the findings have on industry,social, and legal norms. We specifically positioned this research to explore more of the impacts and responses on society as draft privacy bills continue to address features such as dark patterns and privacy by design and default. These related works have given us perspectives as well as grounding and jumping-off points to shape the research we are doing today.

5. Research Methodology

5.1 Initial project brief

We began the project with our hypothesis on initial context, problems, questions, goals and outputs in order to collaborate with public policy staff, advocacy groups, and recruit more team members. Once we had a set of core team members, we held weekly meetings to better scope the project based on a review of problem areas, interest, time, and capacity to execute during the academic year. The result of those meetings were a set of research questions.

5.2 Research questions

Based on the motivations outlined in the previous section, our team came together to outline our high level research questions to guide the project:

I. Question 1: How do roles in various industries use and think about privacy in practice?
II. Question 2: What are the strengths, challenges of various privacy bills + prototypes?
III. Question 3: How do different stakeholders perceive proposed legislation aimed at modifying social media design?

5.3 IRB approval

The research study design was proposed and approved by our respective Institutional Review Boards — the interviews focused on collecting policy and design feedback that posed minimal risks to adults over 18. What we did collect were anonymized transcripts (accessed only by the core project team of 5) that followed roughly a similar script for each of the participants, who were identified by a number in any of the writing we produced. The themes and insights below

were based on an aggregation of quotes with direct consent and approval along with findings across the transcripts. The survey we sent out to better understand the diversity of demographics (see 5.4) did not collect names or identifiers of the participants. We also implemented a process for securing data collection and reached out individually to ensure that any information shared in the public report or the website was disclosed publicly, only with permission from participants.

5.4 Interview recruitment

Our team recruited a variety of participants from various backgrounds (academia, advocacy, government, for-profit industry, law, nonprofit, policy) and demographics (age, gender, race, expertise both with data privacy or with little to no technology and data-related background or expertise). We sent out an anonymous survey to try and understand demographics and diversify our perspectives as much as possible. Based on this survey, most of our participants (57%) were between 25-34 years old, (64%) were women, (52%) were white, and (69%) reported a postgraduate or professional degree (See Appendix A for detailed demographic information of interviewees). For future research, we recognize the opportunity to improve the diversity, perspectives, and voices of the insights gathered.

5.5 Selecting bills to design and prototype

To learn more about which bills we should choose, we spoke with several privacy advocacy members, staffers in Congress, and privacy researchers about which U.S. federal privacy bills to consider that may be impactful or include a variety of angles of regulation. We independently conducted a review on the latest U.S. Federal public draft bills from 2018 - 2020. This included sourcing information from Congressional Research Service's "A Comparison of Privacy in the 116th Congress" and the International Association of Privacy Professionals (IAPP) "US State Comprehensive Privacy Law Comparison." Our group created a set of bill criteria to make our decision to choose which bills to analyze. This criteria is explained in more detail under Section 6.2.2.

In the future, we would consider prototyping more bills as well as using a mix of state and federal bills. We could, for example, highlight bills from locations that are home to tech behemoths such as Microsoft and Amazon in Washington state and Google, Facebook and YouTube in California.

5.6 Designing hypothetical bill prototypes

After selecting three bills to focus on, we sketched prototypes based on some of the key tenets outlined in the bill press releases. We captured some of the physical sketches (**Figure 1**), and transferred these wireframes into a slide deck. We captured five versions that we iterated through over several months.

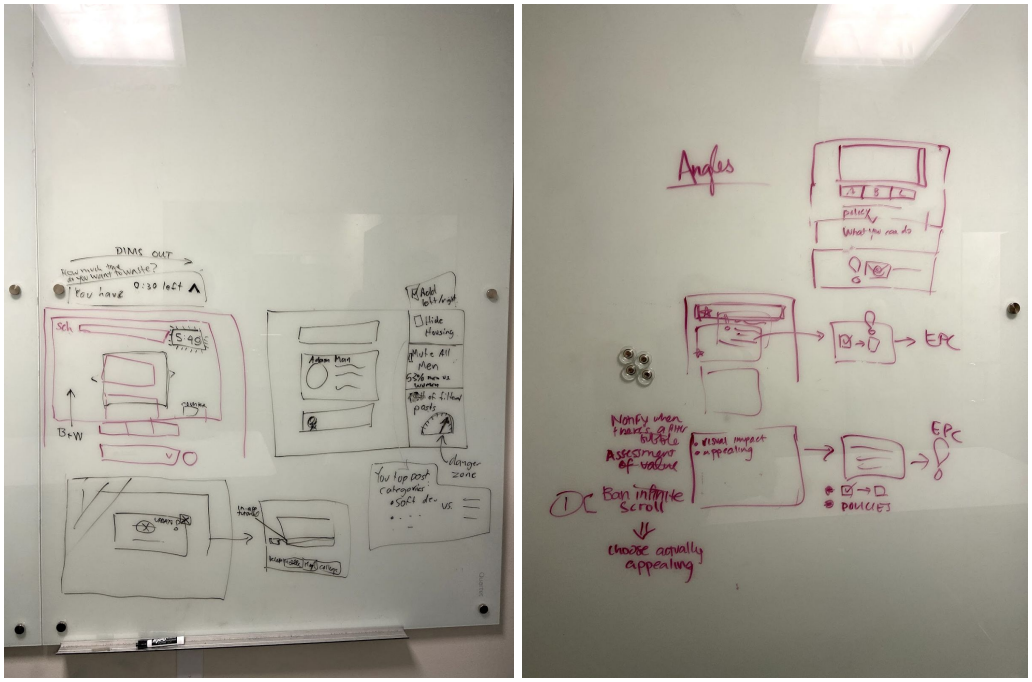


Figure 1: *Some of our first prototypes on the whiteboard. We explored what it would look like to ban certain common functionality within social media platforms. December 2019*

5.7 Conducting Interviews

We conducted 41 one-on-one interviews to gather feedback, quotes, insights, and challenges based on showing our design prototypes. Interviews lasted 45-60 minutes and were conducted via phone, with accompanying prototypes that the participant was able to click through in a Google Slides document. The interview process spanned roughly 3 months between January - March 2020. Four researchers conducted semistructured interviews following a protocol that was expanded based on the responses in each interview. We made room for additional probing to get more details about certain thoughts, feelings, and opinions that came up during the conversation. Throughout the insights & recommendations (Section 6), we highlight quotes (all approved for attribution) from interviewees. The interviews consisted of three main parts: summary of the bill, visual examples of some of the bill concepts, and privacy bill prototypes.

5.7.1. Part 1: Summary of the bill

For Part 1 of the research session (focused on bill summaries, see Appendix B), our goal was to maintain as much of the language of the Congressional documents while trying to convey a brief summary of the bill (**Figure 2**). We sourced the press releases for the *Social Media Addiction Reduction Technology* (SMART Act) and the Online Privacy Act (OPA) to balance the intended communications with a summarized version of the key insights of the bill that the Congressional authors wanted to convey to the media and general public. For the *Consumer Online Privacy Rights Act (COPRA)*, we compiled the summary through concepts outlined in

the table of contents of the full bill, as their one-page summary contained too much information to fit on one slide for our 45-60 minute user research session.

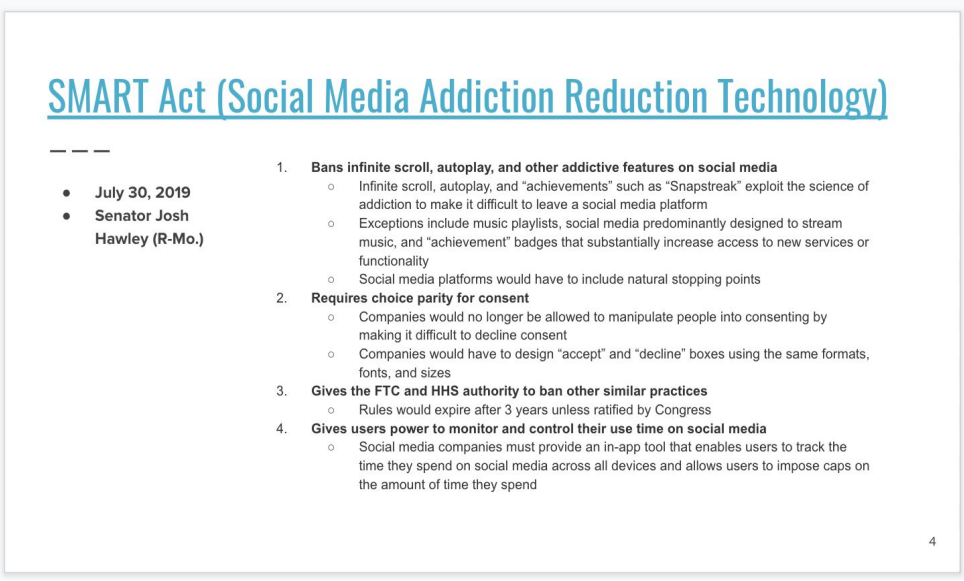


Figure 2: *Text summary of SMART Act, shown to participants during interviews.*

5.7.2. Part 2: Visual examples of some of the bill concepts

For part 2 of the session, we included some visual examples of features mentioned in the draft bills (**Figure 3**). Since we were interviewing people ranging from extensive to no technical expertise, we wanted to ensure we leveled the conversation around what some of the concepts may look like. These included examples of what more uncommon terms such as "right to access, control or delete data" or "infinite scroll" might look like in an online platform.

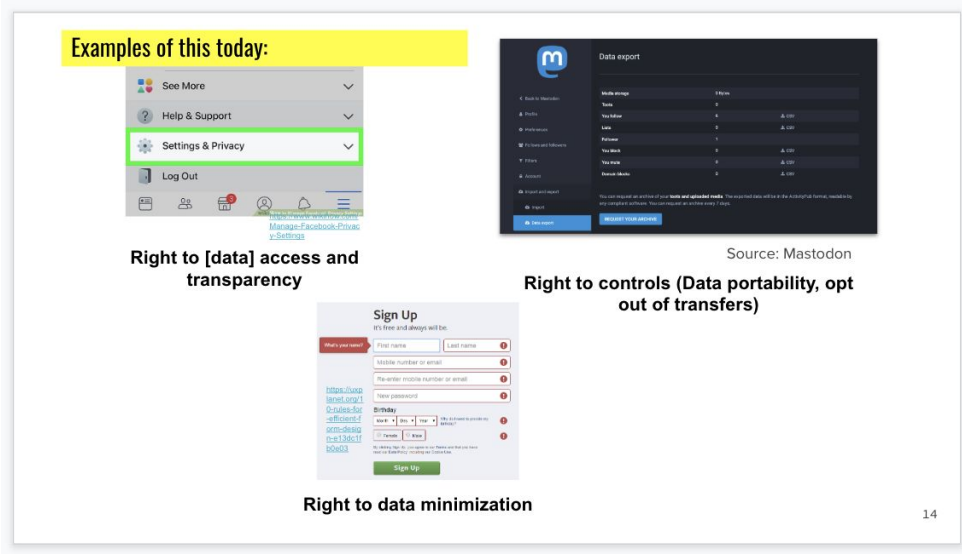


Figure 3: *Visual examples of relevant concepts in COPRA, shown to participants during interviews.*

5.7.3. Part 3: Privacy bill prototypes

After showing interviewees the bill summary and example features, we then revealed the privacy bill prototypes (**Figure 4**). These prototypes aimed to show one of many ways that privacy policy can be translated into features in online platforms. For this research, we chose to design prototypes that challenged existing design paradigms on large social media platforms. This is because the bills often were geared toward large platforms as shown by some of their thresholds with revenue and consumer data collection which would not apply to smaller companies. Through these prototypes, we present alternative interfaces for these platforms, which challenge popular features like infinite scroll.

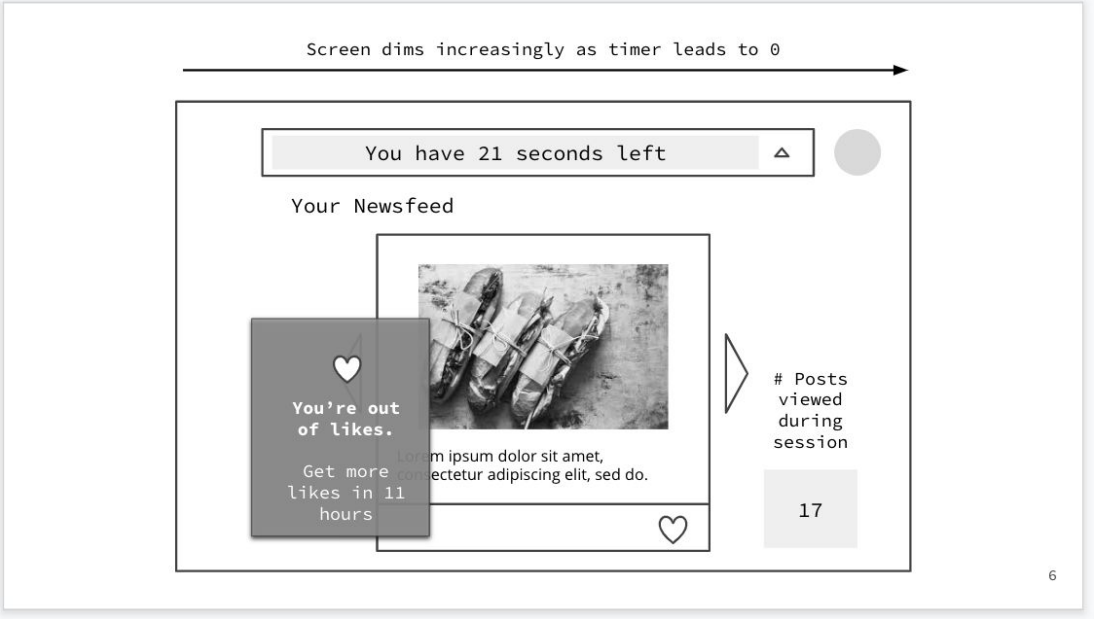


Figure 4: *Prototype of the SMART Act, shown to participants during interviews.*

5.8 Qualitative analysis

This research explores individual perspectives about the implications of proposed legislation on people and organizations, and how the provisions of law could be designed for sociotechnical systems. The goal of this investigation is to provide a rich and detailed description of these various perspectives. It is important to note that the goals of qualitative research do not include generalizability – the ability to extend the results of an investigation to a larger population of statistical significance. Qualitative research does, however, allow researchers to recognize patterns and describe fundamental processes, as well as to understand how an intervention functions in practice and/or what a concept, design, or word might mean to different people. In other words, these in-depth interviews help us uncover the possible reasons people think a certain way and what they may do in the context of a design interface — they will not determine exactly what people will do in every scenario.

We chose to use qualitative research methods, specifically in-depth, semi-structured interviews, because of these methods' utility in helping to understand thought processes and

examining social phenomena. In particular, we were interested in understanding reactions not only to proposed legislation but also to prototypes of how designers might implement some of the provisions in the bills on recognizable online platforms. We chose to use a modified grounded theory methodology for data collection and analysis. First, we transcribed all 41 interviews using the Otter.ai transcription service. We then anonymized and divided the transcripts among the three research team members for analysis. All transcripts were given multiple close-readings.

- We used in vivo coding – taking the language that the participants used to begin identifying important ideas or concepts in the data. It was important to use in vivo coding at the beginning of our analysis because this kind of coding prioritizes the voices of the participants.
- After in vivo coding we engaged in axial coding – constructing categories of the ideas from the in vivo codes. These categories reflected key ideas that emerged from close readings of the interview transcripts, as well as considerations of the sectors/industries represented by the participants (context).
- In a final round of coding, members of the research team met five times to form consensus on the selective codes – the key concepts and themes – and to answer our research questions. During these sessions, team members reported the findings from their portion of the transcript coding(s) and compared them with those of other team members. Findings were then distilled into higher-level themes reported across each section.[18]

During the coding process(es), and in conjunction with the website team, we selected quotes from interview participants that helped to illustrate the concepts or themes we found. Many of these quotes are used throughout the site and are being used within this report. Quotes were selected based on whether they met one, or both, of two purposes: proof and provocation. Proof quotes are those that help to describe the concepts that we identified in analyzing the transcripts. Provocative quotes are those that are compelling or best illustrate the phenomena being discussed.

5.9 Website process

We designed and developed a public website to present our work both with visual simplicity and plain language for a general audience with little background on data privacy related topics. This is directly related to one of our goals of the project: to educate the public on recent draft privacy bills by transforming vague policy into design implementation. In terms of process, we

[18] We note the existence of debates on whether or not calculating intercoder reliability for qualitative research. As it adds no value to our research report and we are not intending to communicate methodological reliability, although we assert the quality and transparency of our research. For further reading on interrater reliability in social science and human-computer interaction please see, McDonald, N., Schoenebeck, S., & Forte, A. (2019). Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-23.

took an iterative development approach, where we worked in 1-2 week sprints to design, build, and evaluate working prototypes. We began each sprint with a group design session (**Figure 5**) where members of the team created paper prototypes (**Figure 6**) that addressed the goals of the iteration. We set up a continuous feedback cycle during each sprint by deploying test versions of the site and garnering feedback as we made progress. Throughout the process, we employed guerilla usability testing to collect and incorporate feedback from students and researchers at MIT, as well other people within our close social networks. After deploying the website, we also collected and incorporated feedback from members of our advisory board.

Figure 5: *Photo taken during a group design session for prototyping the website. January 2020.*

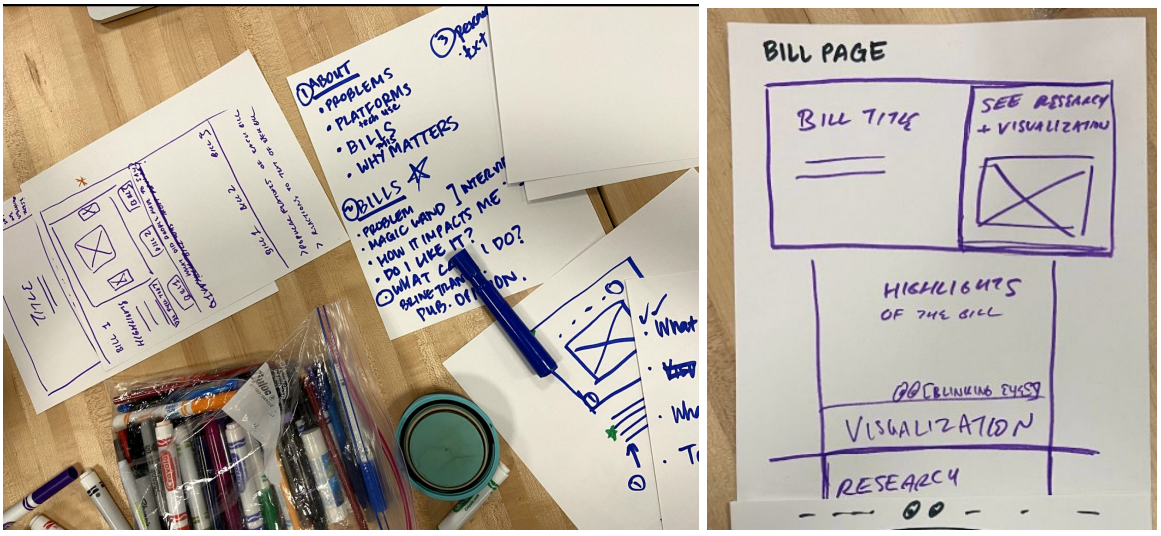


Figure 6: *Early paper prototypes of the website, focusing on content organizing and layout.*

5.9.1. For the bills section, we show the bill descriptions and mockups at the top of each bill page. Our aim in this section was to first provide a general audience with an introduction to the policies, which are often inaccessible and difficult to read (**Figure 7**). We also wanted viewers

to see the actual prototypes that we showed our participants. We then presented insights on how people responded to these bills and design prototypes through short summaries and quotes (**Figure 8**).

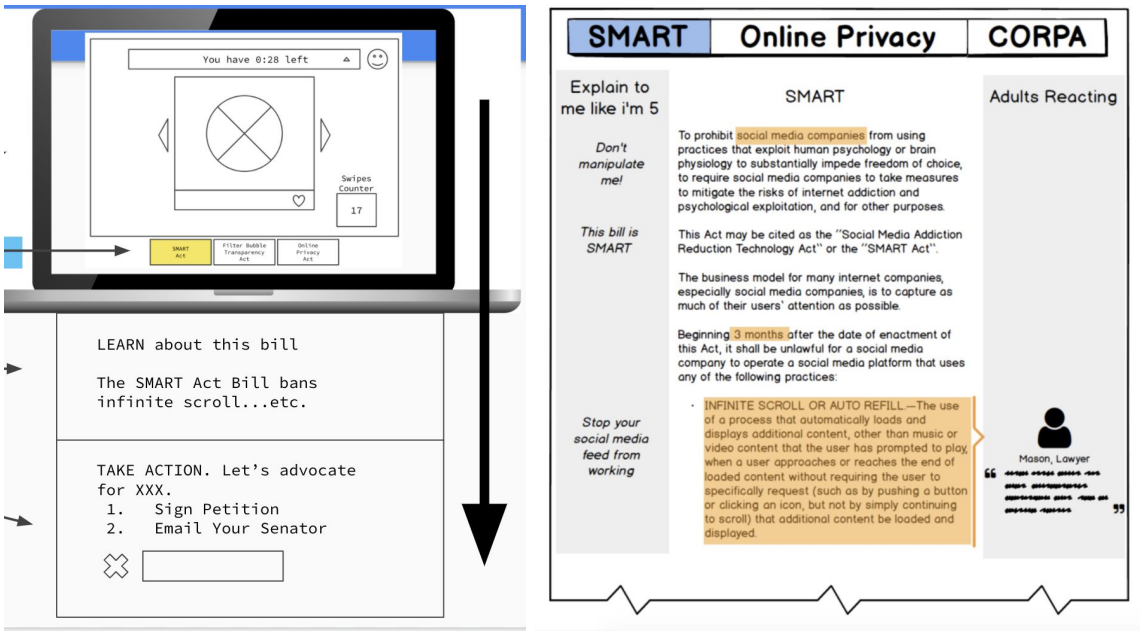


Figure 7: *Early website wireframes that explored different ways of presenting bill descriptions and mockups, as well as feedback from interviewees. The first wireframe (left) focuses on presenting the bill mockups front and center as well as offering a call to action tied to each bill. The second wireframe (right) focuses on presenting extended bill descriptions, which are annotated with feedback from interviewees.*

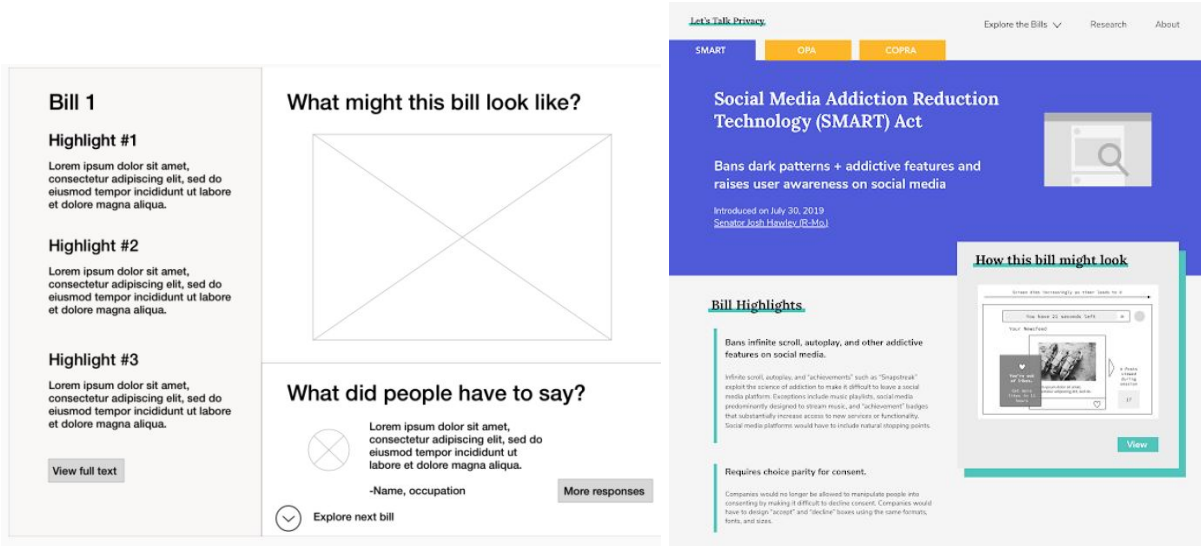


Figure 8: *Website wireframe of the bill page (left), which balances presenting bill highlights, mockup, and feedback. This wireframe informed the final version of the bill page (right) that was deployed on the website.*

5.9.2. For the research section, we provide a high-level summary of our report and an easy way to download our full report and 1-page summary. Our goal for this section was to make our research as accessible as possible to researchers, policymakers, and the general public. In this section, we also summarize our process and recommendations generated from our research (**Figure 9**).

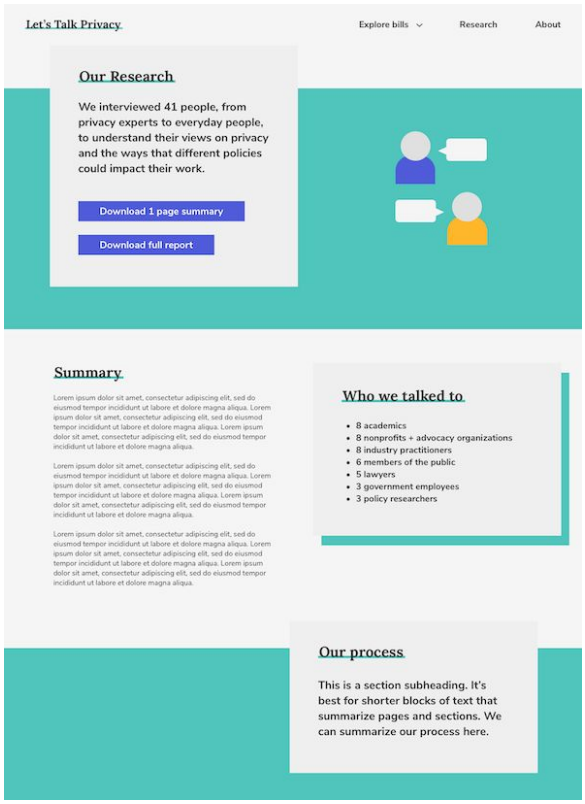


Figure 9: *High-fidelity mockup of the website research page, which summarizes our research process and findings. In total, we went through 8 iterations of the website from sketch to wireframe to full color mockups.*

5.10 Final deliverables and outputs

Full report	This document contains the full comprehensive outputs of our research aimed at academics, researchers, and policymakers who may be interested in diving into more detail of our research grounding, methodology, in-depth themes and recommendations. (Section 1-5) = rationale, process, methodology. (Section 6) = insights, findings, recommendations.
Report summary	https://letstalkprivacy.media.mit.edu/research We created a document in between the high level glimpse of a one-pager and a full report with ~50 pages that provides more detail in a digestible format. This is also aimed at researchers, policymakers, and a more general audience who are interested enough to see the prioritized findings with some nuance, without the detail of methodology and a comprehensive view on all of the themes and recommendations we compiled. We anticipate that this document will summarize our research in a readable, quick, and prioritized format.
Recommendations one-pager	https://letstalkprivacy.media.mit.edu/research We created a one-pager aimed at a policy, media and industry practitioner audience. The goals of the one-pager are to synthesize high level themes and recommendations on one page, optimized for skimming. While this document does not include substantive detail, it provides an opportunity to prioritize the takeaways of the report and mimic many one-pager policy documents that are already an industry norm in policy environments.
Policy prototyping guide	https://letstalkprivacy.media.mit.edu/research We created a downloadable guide to give policymakers a template process for prototyping bills to help them iteratively improve policies before publishing. We include a high level process diagram, an outline of the ideal team and roles, and a

	skeleton structure that policymakers can use to integrate prototyping in their processes. This document is meant to be modified depending on the resources available for each team.
Website	https://letstalkprivacy.media.mit.edu/ We created a website aimed at a more general, non-technical and non-policy audience interested in learning about privacy policies and how they might translate into different experiences with online platforms. We designed the website for quick skimming so that people could explore different bills as desired. We highlight the high-level summary of the bills, prototypes, research, and people involved in the project.

6. Insights & Recommendations

6.1. Research question 1: How do roles in various industries use and think about privacy in practice?

6.1.1. Defining Privacy

The word "privacy" is without universal meaning. In the United States, our understanding of privacy is shaped by an 1890 *Harvard Law Review* article in which the distinguished jurists Samuel Warren and Louis Brandeis called for courts to recognize "a right to be let alone."[19] The two men were directing their ire at invasive news gathering techniques bolstered by emerging technology – at that time the instantaneous camera – and the harms of reporting on matters deemed personal. As at the turn of the 20th Century, technological innovations are shaping our ideas of privacy, though the "data" may have changed in volume and scope – no longer solely photos, but aggregate personal details from which organizations can make inferences. In the middle of the last century, Professor of Law & Government Alan Westin describes the four states of privacy as "solitude, intimacy, anonymity and reserve,"[20] all of which find a grounding in the ideas of individual choice and control much like Warren and Brandeis' idea of privacy.

Privacy itself, though, continues to be vague. A more modern approach to understanding privacy is that of Professor Daniel Solove who acknowledges that there are many different ways of approaching privacy, but that a pluralistic conception of privacy is beneficial.[21] Instead of one definite construction of privacy, Solove offers a view of privacy as contextual. Professor Helen Nissenbaum explicates privacy in socio-technical systems as contextual integrity – requiring an understanding of social context and informational norms.[22] Professor Anita Allen's work[23] highlights "how individuals have a moral obligation to respect other people's privacy but also their own." Allen also explains[24] how information privacy is "rendered utterly implausible by current and likely future Big Data practices", which is a theme of this research exploration. Within the scope of this project we examine the importance of context – both an individual's profession or industry, as well as private versus professional life.

The participants we spoke with represented different professions – from design to academia, health to civil society organizations – providing an array of different experiences and insights, both personal and industry-related. We asked all participants several questions to understand what privacy meant to them and their organization, and the contexts in which they were speaking, including:

- How do you define privacy?

[19] Brandeis, L. and Warren, S., 1890. The right to privacy. *Harv. L. Rev.*, 4(5), 193-220.
[20] Alan, W. (1967). Privacy and freedom.
[21] Solove, D. J. (2008). Understanding privacy.
[22] Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life.
[23] Allen, A. L. (2016). Protecting one's own privacy in a big data economy. *Harv. L. Rev. F.*, 130, 71.
[24] Allen, A. L. (2016). Protecting one's own privacy in a big data economy. *Harv. L. Rev. F.*, 130, 71.

- What are the biggest privacy challenges in your role?
- Why do those challenges related to privacy matter to your organization?
- What are the drivers or incentives that make your organization care?
- Based on your definition of privacy, how important is privacy to you?
- What do you think the biggest privacy challenges are?
- What is the role of the individual, the government, and organizations in protecting privacy?

Our choice to speak with people representing different industries was purposive. Traditionally, academic and industry research faces several limitations. First, many participant samples are based on convenience. For university researchers, this may mean using students; for industry researchers, this may mean using whomever applies to participate. Such sampling techniques limit the kinds and diversity of experiences represented in the qualitative data. Sampling is also affected by budgets and resources. Researchers may not be able to provide incentives for participation, thereby limiting the ability to recruit from different communities and professions. Other constraints include logistical difficulties, including travel and scheduling. Further, researchers may lack the skills and experience in interviewing and recruiting.

These limitations and constraints can significantly impact a study like this in which our major goal was to understand the attitudes and behaviors of individuals from various professions and experiences to, then, create policies that protect a diverse range of interests. We also outline these limitations because if policymakers or practitioners adopt some of these practices, they should be aware of some of the drawbacks of these methods. Because privacy is contextual, to enable the creation of privacy-protecting tools and policies, it is important to understand the different contextual environments and norms for data and data use. To do this, we have highlighted the language, concepts, framings, and themes that arose during our interviews with hopes that this will allow a deeper understanding of how privacy is understood and operates across networked systems, and the identification of possible harms, tensions, and other important factors.

6.1.2. Commonalities

In spite of the differences in kinds of positions our interviewees held, we found commonalities across all sectors in their concepts of privacy. These conceptualizations fall into categories broadly called control, risks vs. benefits, and fairness. The quotes attributed below come from interview participants and were approved by them for publication.

a. **Control:** Control is a common formulation of privacy even outside of this project, so it comes as no surprise that many interviewees understand privacy as “the ability to control an individuals’ personal information,” including the ability to regulate when personal data is shared and who can access it. This definition, for the most part, came from an individual’s perspective – the person using the platform is the data source, and platforms and organizations are the places where data can be shared. Interviewees

discussed data control across cases: legal, healthcare, online social media, etc. Devin Gladden, Manager of Federal Affairs at American Automobile Association (AAA), highlighted the nuance of balancing more access and control with the ability to manage data.

"*We're now at a point where consumers want greater access and control and uptake of managing their data. But the real challenge is [that they] still don't know [data is] different […] and how it can be leveraged or how it shouldn't be leveraged to make appropriate decisions.*" - *A Let's Talk Privacy project interviewee*

b. **Risk vs. Benefits:** In considering these cases, interviewees discussed the risks and tradeoffs of legislation protecting privacy and regulating information disclosure, as well as the motivations for both. A paramount concern for many, for example, was that protecting privacy by limiting data collection may reduce organizational profits, as well as affecting the efficiency and efficacy of the work in which an organization engages. These tradeoffs appeared in different ways in the different industries represented. For interviewees in policy or law related industries, the tradeoff was in focusing on the aggregate impact of the bill against whether provisions like enforcement, civil rights, consent, etc would be weakened. Designers and user research practitioners considered the tradeoffs between individual empowerment over personal data and ease of platform use. Interviewees working in the civil society sector identified two tradeoffs: between data collection and client safety, and between having enough and lacking information. Lastly, both academics and interviewees working outside of privacy and data governance saw tradeoffs in authority and choice versus automatic sharing.

"*…if you look at some of the fines that have been laid upon Facebook and Google- they're such a small slap on the wrist, that [the risk is] worth taking for these companies, given how much profit they're making. […] Things will be enforced, and there will be consequences that would be detrimental to the businesses, to the point where their risk calculations will be such that they would have no choice to follow to follow these things.*" - *A Let's Talk Privacy project interviewee*

c. **Fairness:** In addition to the formulation of privacy as control, interviewees conceptualized privacy as leading to fairness. By fairness, interviewees identified "leveling the playing field" between people and organizations, particularly large tech organizations. Many also identified ideas related to equity and value. One important theme was finding a better system to distribute power and benefits of data collection and usage to those who the data was originally derived from. Relatedly, interviewees connected privacy to trust with the organizations that collect and use data, although this creates a relationship built on information asymmetry.[25]

[25] For a discussion of information asymmetry see: Wittkower, D. E. (2016). Lurkers, creepers, and virtuous interactivity: from property rights to consent to care as a conceptual basis for privacy concerns

"I think it has to do with … choice and like transparency, [..] being able to see the answers, right, like, and having an understanding of like, what the rules are and like what the constraints are. And then ideally having some way of changing them if you see the need to." - A Let's Talk Privacy project interviewee

6.1.3. Themes

At a higher level, we consider the major thematic points of interest that arose and were unique to particular positions. These themes include single vs. multi-dimensional definitions of privacy, privacy as compliance with regulations vs. human rights, and the need to shift the norms surrounding privacy in various industries. To craft policies that take different perspectives about privacy into consideration, policymakers should consult with practitioners that may work across different sectors and with both people who use data-collecting products and services as well as non-users. We note some of the insights from direct quotes from our interviews below.

a. **Single vs. multi-dimensional definitions:** Many of the academic, legal, and policy interviewees explained privacy as a multi-faceted concept, while others – designers and non-privacy professionals – explained privacy with more context specific meaning. These differences can be reflected within the context of their professional roles. Academics and policymakers, for example, may oversee a variety of projects or cases that attempt to generalize findings for recommendations or policy. Devin Gladden, Manager of Federal Affairs at AAA, expressed this variable nature of privacy in considering how government and industry should think about data categories:

   "I think it would be very useful for the government to think about the different data categories, and how people want that data protected. For example, consumers may view financial information much different than trip information and that could result in different protection expectations. This could also lead to different obligations on a company, which would be differentiated by data category."

   In contrast, the product director of a major academic hospital may see privacy through the lens of patient privacy, recognizing the need to avoid harm to the patient, while accessing the benefits of healthcare data.This may represent differences in how directly professionals interact with privacy legislation. At the same time, data can be used for more than one purpose, reinforcing the need for multi-dimensional definitions.

b. **Privacy as compliance with regulations vs. human rights:** The interactions with privacy include considering how data moves through systems. Interviewees in roles directly connected to law and policy associated privacy with data leakage and its consequences, considering not only that data may be leaked, but that it then spreads. Both design and

---

and information ethics. First Monday, 21(10), available at: https://firstmonday.org/article/view/6948/5628.

civil society professionals were also concerned with this kind of systems thinking, albeit for different reasons. Interviewees expressed interest in creating and designing systems that allowed them to have agency over their personal information. Non-profit participants, as well as academics expressed concern with creating systems/revising current systems of data collection and aggregation to protect personal privacy as well as safety. According to Najarian Peters, an assistant professor and Faculty Fellow at Seton Hall Law School's Institute for Privacy Protection, compliance is a way for organizations to manage risk:

"*If I am talking to finance people I am focused on the bottom line and how privacy protection can actually enhance it–privacy can be a point of comparative advantage. If I am talking to healthcare people I am focused on the bottom line as well but also focusing on the importance of what privacy means to patients. Convincing different stakeholders of the value of privacy protection requires different pitches and you have to know what matters to those people right where they sit/see the world. Once you link into that you can open them up to seeing things broader beyond their immediate objective. There are best practices, I think, that often dovetail across all industries. But how we interact with privacy and privacy protection is shaped by the industry which is the entry point.*"

c. **Need to shift the norms surrounding privacy in various industries:** Across several fields interviewees were interested in changing the privacy norms. Lawyers, for example, expressed interest in changing the volume of industry data collection. Many of the designers interviewed noted the desire to implement "friction" and break design habits and privacy policies leading to click fatigue. One way to enable friction is to confirm actions that may have severe consequences, such as exporting all data or deleting an account from one's social media profile. There must be a balance between a need for friction and avoiding click fatigue in order to shift power norms in the individual's favor. Civil society professionals expressed a wish to shift industry incentives to avoid harm to their clients using, for example, "name and shame" techniques to express displeasure and direct attention at organizations using harmful practices.

Often, inhibiting shifting of norms was a conflict between mere compliance with regulations versus considerations of human rights. Compliance was defined as meeting the specified provisions of a law in the easiest way possible. Many interviewees in law and design saw privacy as compliance or a business decision.

"*At the end of the day, a business decision is the decision of the organization's leadership. The compliance people will tell you, especially GCs will remind the compliance folks of that but hopefully the reporting structure is such that it also allows for the business decision to be positively influenced by compliance and ethics. Although,*

that is not always the case.” - Najarian Peters, Faculty Fellow and Assistant Professor in the Institute for Privacy Protection at Seton Hall Law School

In addition, in compliance-heavy sectors like health, interviewees reported that compliance with health data policies would prevent them from using patients data for valuable research. This suggests that in addition to providing privacy to individuals, it is important to facilitate data collection, which would eventually benefit them. Limits on collection and use of data may in fact yield a trade-off where we lose some commercial value. Often, privacy discourse may highlight the idea that data limits may create economic value, and that may well be true, but it may also curtail some economic value (e.g., complete personalization of some services, loan or insurance underwriting algorithms).

In contrast, some civil society professionals and academics viewed privacy as a human rights consideration, often focusing on the possible harms of organizational failure to protect privacy.

“*I think the people that get screwed by this of course are the most vulnerable folks, [who] are already getting screwed by all these other things, and they're the ones that this matters for.*” - Maggie Hughes, a masters student at MIT

6.1.4. Key Insights

In general, although interviewees expressed similarities in their definitions of privacy, the contexts in which these ideas exist shape how privacy works in practice. This is important for considering what adequate privacy should include. The creation of a common language, or a set of phrases that can be understood across all sectors may prove useful. Such a lexicon could assist in identifying overlapping processes, concern, interests, and harms, as well as enable better collaborations between individuals from different sectors and professions. A shared vocabulary may also help in the creation of more effective or widely adopted policy. Current and proposed laws related to privacy are written without examining the perspectives of a variety of sectors, and fail to preempt existing federal sectoral privacy laws. Conflicting definitions and frameworks for privacy make many laws problematic and impractical from inception. Therefore, to assist with the creation of more adequate privacy regulations, it is mandatory that policymakers consult with practitioners across various sectors, as well as with the people who use these systems and may experience benefits (and harms) of the platforms first-hand.

To take a preliminary attempt at further exploring a shared vocabulary related to privacy and data protection, we used text analysis to parse each of the interviews by sector. The output (tree diagram data visualizations) illustrates the most common words both across each sector and across all interviews. We collected hundreds of pages of qualitative data from interview transcriptions that can be analyzed by sector. Each interview followed a similar series of questions based on the semi-structured interview guide we used for consistency.

For 39 of the interviews, we used Otter.ai, a 3rd party tool to record and generate transcripts of the interviews. We had 41 total interviews, but two of the interviews were conducted before we had access to the full transcription service, so we omitted those interviews. We processed the transcripts through custom scripts, programmatically removing the English stop words (e.g. her, he, to, was) listed in the Natural Language Toolkit, and visualized the 50 most frequently mentioned words across all sectors (e.g. academic, everyday, government) using D3, see **Figure 10** below. By visualizing the results by sector, we see certain words are shared across sectors, as can be seen in **Figure 11** below.

In order to explore how sectors uniquely speak about privacy, we further processed the transcripts through custom scripts. Again, we programmatically removed the stop words, further refined the results by programmatically removing the aforementioned 50 most frequently mentioned words across all sectors (e.g. know, think, data, people, right) to generate a distinct (but not unique) list of frequently mentioned words by sector. These distinct words are shown in figure 3 below.

We use a tree visualization of interviewee sectors and commonly used words (see **Figure 10, 11, and 12** below). In these tree visualizations, nodes (represented as circles) connect via branches (represented as lines) to other nodes. Reading from left to right, the root node begins with Sector. Branches then connect to individual sectors and, finally, to frequently used words. Both line thickness and color (see the Color key) of the branch correspond to frequency.

Color key

I. Heatmap corresponding to the **number of interviews** from
Fewer # interviews (left, light purple) to more # interviews (right, dark purple)

II. Heatmap corresponding to the **number of times a word was used**
Least mentioned (left, light orange) to most mentioned (right, dark red)

III. Visualization of the **50 most mentioned words across all sectors**.

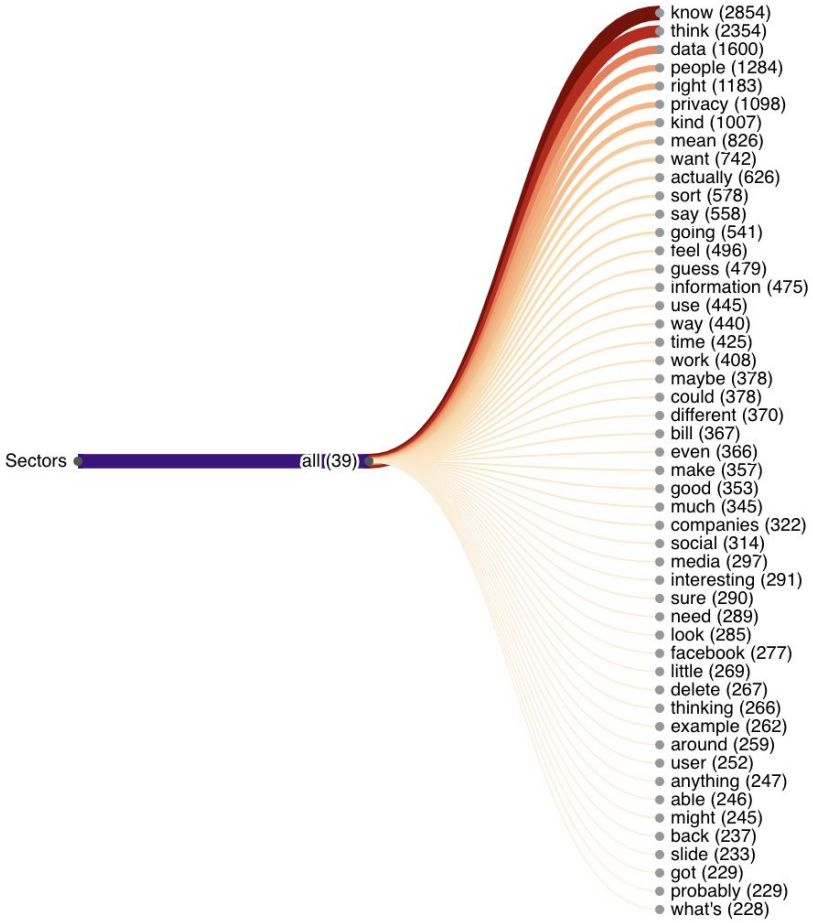


Figure 10: Top commonly used words in the interviews across all industries, standard words still included. *This was the aggregated tree visualization, showing the most common words used across all 39 interviews. These words indicate what terms may be common to conversation around data privacy and technology related topics. As a limitation, some words in this list may be common to general english language conversations in a low key professional setting (what's, got, might, sure, much, make, way, etc.)*

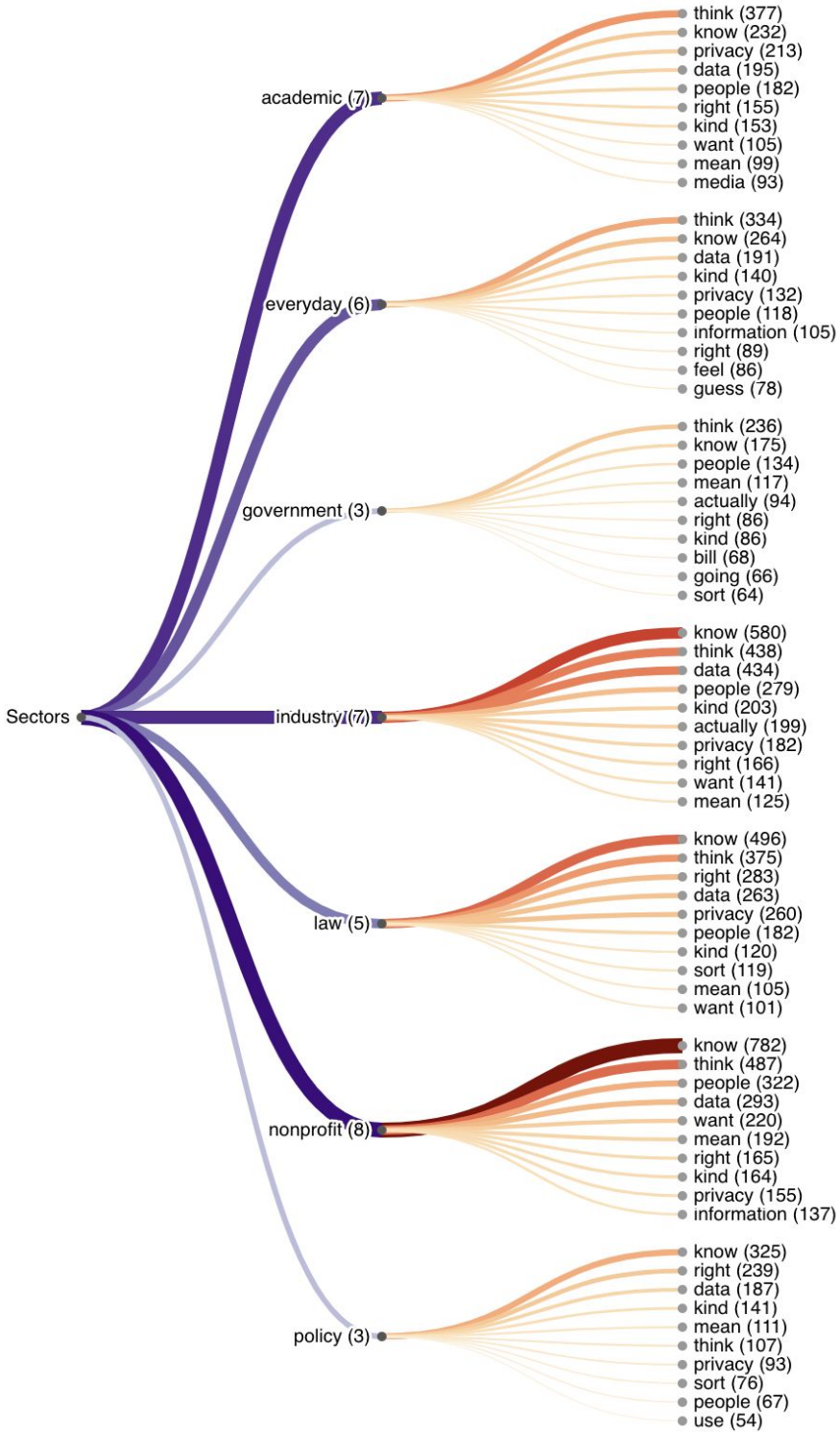


Figure 11: Top 10 most mentioned words by sector, standard words still included. *When looking at frequently used words by sector, we see that many words from Figure 1 and Figure 2 are shared between sectors (e.g. know, think, data, information, privacy). This shared vocabulary is helpful to understand what common words may exist and how this shared language could serve as the basis to better understand what concepts are valued and resonate across industries.*

I. For example in **Figure 12**, the word “delete” was mentioned 267 times, indicating the possible importance of improving individual empowerment to delete data, adding policy language around the “right to delete” information, and strengthening the capacity to clearly delete user data through both frontend and backend components. Reflecting on how a person may view how data deletion can be negative, one interviewee explained, *“For Spotify [...] I wouldn't want to delete my data because I want it to continue to show me (based on their algorithms) what kind of stuff I would be into based on the stuff that I've already liked.*” In response to a question about how a person manages their data, they shared, *“I've never downloaded my data. I have done things like deleting certain things like removing access to LinkedIn accounts and deleting [accounts] entirely.*”

II. “Facebook” was mentioned 277 times, clearly showing the influence of the social media platforms in policy, law, and privacy design and technical implementation. Many participants mentioned different ways they have managed their data through social media platforms and Facebook in particular: *“I've been slowly throughout the years deleting platforms, and I've thought about deleting my Facebook.*” A security engineer explained how there is complexity in data sharing rules, especially through the platform. For example, “*What should happen when my friend uploads a picture to Facebook to me, and who gets to choose if that gets deleted?*”

III. “Companies” was mentioned 322 times, potentially signifying how individuals across sectors recognized how data-collecting companies and platform services have a large responsibility to play to ensure data protections. One interviewee mentioned how companies would be most impacted by these laws and expressed skepticism of their efficacy: “*So depends on how these [laws] are enacted, but as soon as there's loopholes for other companies or the companies that currently do the practices to do things in a different way, they'll still exploit those and I think you'll be back to square one.*” Another interviewee worried about the usefulness of the laws if “*they're [...] a small slap on the wrist, that [...] is a risk that's worth taking for these companies, given how much profit they're making so I think you really need to establish that [...] things will be enforced, and there will be consequences that would be detrimental to the businesses, to the point where their risk calculations will be such that they would have no choice to follow to follow these things.*” While much of the study focused around data-related bills and the impact on industry, we also highlight in other areas how other stakeholders (researchers, advocacy groups, individuals) have a significant part to play to ensure that policies are useful for their communities.

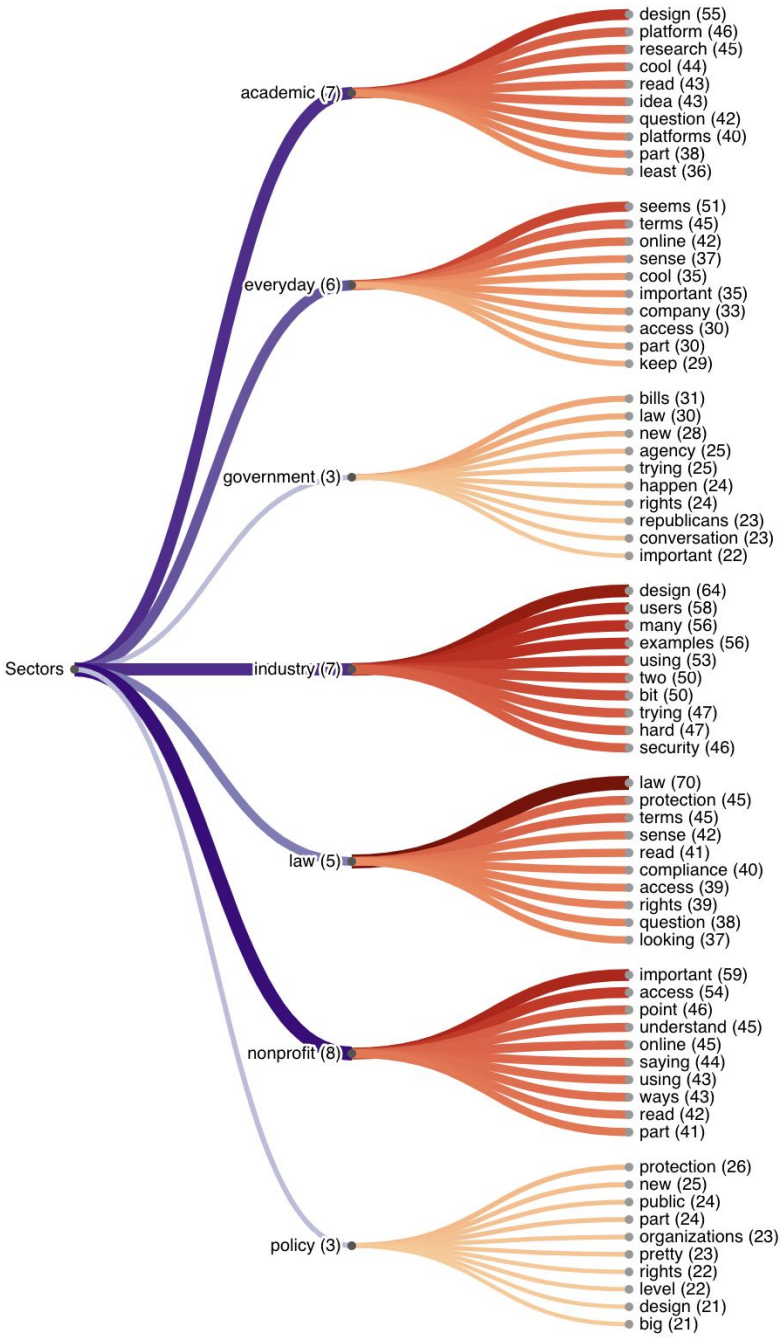


Figure 12: 10 most mentioned words per sector with top 50 commonly used words removed. *This visualization highlights terms used within specific sectors that are not necessarily common throughout all sectors. These words may have particular meaning with a sector and/or highlight aspects that particular sectors care about in regards to privacy and policy. For example, "users" is frequently used within the industry sector indicating the impact on the individual is top of mind. This is not unique to only the industry sector. With policy and law, the word "protection" is common while in government "rights" is often used. The implication is that many sectors are thinking of people who use the technology in some capacity. They use different terminology to highlight what they are working on (design, rights, protections) on behalf of those who both benefit and are harmed by using data-collecting technology.*

It is important to note there are limitations with this approach:

I. **Text inaccuracy:** The automatic Otter.ai transcripts are not perfectly accurate: some words are incorrectly transcribed (e.g. “two” instead of “too”) or certain words spoken may have accidentally been left out of the transcript entirely. After reviewing the transcriptions with the audio, we deemed the transcriptions to be accurate enough to capture the core terms of the interview.
II. **Grammar-free:** In our analysis, we count the number of times a term is used without considering the semantic grouping. How is the term used in a sentence? For example, “users never know” has a very different meaning from “users know.” In our visualization, both “users” and “known” would be counted twice. We consider this to be an acceptable limitation, since our analysis hones in on the commonalities and differences in terms used between sectors.
III. **Interviewee text included:** The interviewer’s questions are included in the transcriptions. Upon review, we deemed that to be acceptable since the interviewer overall spoke very little.
IV. **Representative sample bias:** It is important to note that the interviewees we spoke with are not a comprehensive representation of the entire ecosystem of perspectives (including law, policy, academia, etc.). The commonly parsed words we derived that correspond by industry are based on a reflection of this sample we gathered. The interviewees self selected their “sector” based on their role. The “everyday” category represents people who did not squarely fall into one of the categories and did not have self reported “expertise” in privacy or data related areas.

6.2. Research question 2: What are the strengths, challenges of select privacy bills + prototypes?

6.2.1. Overview

Privacy policies are often expected to change reflecting how technology impacts people through instantaneous data capture, production and sharing. One example of how laws have changed as a result of the introduction of a new information-collecting device is demonstrated in the story of the camera.

In the 1890’s, fourteen-year old Abigail Roberson arranged to have professional studio photos taken of herself. A few months later, she stumbled on a poster advertisement for Franklin Mills’ flour—featuring her face. This poster ad was one of 25,000 displayed in public stores. This story is just one of many.[26] At the time, women’s faces and bodies, more often than men, were “the subject of surreptitious photographs” used for commercial efforts, explained Sarah Igo in

[26] Roberson v. Rochester Folding Box Co. 171 N.Y. 538, 171 N.E. 538, 171 N.Y.S. 538 (NY 1902), available at http://faculty.uml.edu/sgallagher/roberson.htm. Accessed March 30, 2020.

her book, *The Known Citizen*[27]. The result from this litigation was the 1888 *Federal Bill to Protect Ladies* to remedy unauthorized circulation of these photos.[28]

More than a century later, in 2020, data collection from facial recognition emerges as pervasive surveillance in our cities, compromising our privacy and digital rights. Capturing one's face for advertising and other purposes is an invasive, exploitative, and one-sided transaction but the digital storage and processing of your likeness can lead to even more nefarious outcomes. With advances in technology, data privacy related policies have changed over time. In response, cities like San Francisco, Somerville, and Oakland have passed a facial recognition ban in government use of technology in 2019.

For our research, we focused on data privacy policies that involve or relate to "dark patterns" and human interface design, launched between 2018-2019. This time frame was notably a few years after the Cambridge Analytica scandal, a cornerstone moment in more recent privacy history where a company used millions of people's Facebook profiles without their consent for political purposes to influence the 2016 presidential election.

6.2.2. Policy selection

From the bills that arose during this time period, we focused on 3 bills that relate to design and data in some capacity. We chose these bills based based on the following criteria:

I. **Represent voices from Congressional teams that have been engaged in privacy and data related legislation.** We wanted to choose bills that were produced by policymakers who had a strong track record of data privacy related legislative efforts. This decision was informed by both speaking with people in Congress to get an understanding of who was seen as a leader in the space of strengthening privacy rights and doing landscape research to study the bill options.

II. **Show a variety of different policy approaches** in terms of legal, advocacy, technical and design perspectives. Legal choices in bill drafts can yield policies that have divergent implementations. We selected bills that included efforts to strengthen enforcement, directly trigger changes in platform design, establish a watchdog specific agency, and highlight no preemption of stronger state laws. We believe that an exploration of many avenues into strengthening privacy measures would be important to better understanding the different levers of change possible.

III. **Able to be prototyped visually in some way** from abstract to concrete elements specifically mentioned in the bill. We recognize that this criteria is obscure to measure. Since there are endless bill options, we wanted to focus our efforts on the ability to prototype some visual way that the bill provisions could look through a generic social media platform. We specifically chose to prototype the impact of the bills on an

[27] Igo, S. E. (2018). The known citizen: A history of privacy in modern America.
[28] Lake, J. (2014). Privacy, Property or Propriety: The Case of "Pretty Portraits" in Late Nineteenth-century America. Law, Culture and the Humanities, 10(1), 111–129.

individual's experience with a social media platform, as opposed to a prototype using a website browser, with privacy policies specifically (this scope would be too narrow) or data-collecting subject specific app (used for dating, healthcare management, fertility apps, etc.). Additionally, the language in many of the bills seemed to target large data-collecting platforms like Facebook, Google, Instagram, etc. In the future, bills could be prototyped with other types of online data collecting platforms.

The bills we chose to analyze and interview participants about include a variety of perspectives about data-collection and user experience with a technology.

I. ***The Social Media Addiction Reduction Act*** **(SMART Act) introduced on July 30, 2019 by Senator Josh Hawley (R-MO).** This Act bans infinite scroll, autoplay, and other addictive features on social media. It also requires clear choice to consent and strengthens the powers of the U.S. Federal Trade Commission and the U.S. Health and Human Services to ban similar practices. The goal of this bill is to give people more power to monitor and control their use time on social media. **Note:** While this bill incorporated less of a "privacy" related framing and more on platform "addiction" and improving the quality time spent on platforms perspective, we included it because it provided a different legislative approach focused on particular features (autoplay, badges, etc.) with online platforms.

II. **The *Online Privacy Act (OPA)* was introduced November 5, 2019 by Congresswomen Anna G. Eshoo (CA-18) and Zoe Lofgren (CA-19).** This Act focuses on creating individual rights (right to access, correct, or delete data), places clear obligations on companies, establishes a Digital Privacy Agency (DPA) and strengthens enforcement through state attorneys general.

III. **The *Consumer Online Privacy Rights Act (COPRA)* introduced on November 18, 2019 by U.S. Senate Commerce Committee Ranking Member Maria Cantwell (D-WA) and fellow senior committee members Senators Brian Schatz (D-HI), Amy Klobuchar (D-MN), and Ed Markey (D-MA).** This Act focuses on three major categories of efforts. First, it establishes foundational privacy rights to empower consumers. Second, it improves data security, protects sensitive personal data and supports civil rights in the digital economy. Third, the Act focuses on "real enforcement and accountability measures."

To understand a bit more about how we aggregated the insights below, we share a few excerpts from the questions in our interview brief. We asked all participants several questions to understand what their perceptions were of the bill summaries and the prototypes. Specifically:

- As we showed them the bill proposal text highlights and visual concept definitions we told interviewees, "Please speak aloud and narrate any thoughts, questions, or immediate reactions that come to mind. You might see a word, phrase or image that

might provoke a thought or something related to your lived experiences. You are welcome to talk about that as well."

- As we showed them the prototype interface, we asked, "As you are viewing this, please speak aloud and narrate what is happening. How does the interface and the features you see here work in practice? Feel free to mention if certain features are confusing to you or stand out."
- From [YOUR INDUSTRY] standpoint, what is the feasibility of executing this policy? Feel free to comment on what stands out, what is frustrating, what works, what seems weird.
- What are the strengths of this design?
- What are the challenges of this design?
- Does anything here remind you of what you've seen before?

6.2.3. Commonalities among all the bills

In this section, we explore similarities present among the 3 bills we analyzed and got feedback from our interviewees.

a. **The policies balance power through a variety of levers and mechanisms.** Policymakers have different perspectives through different pieces of legislation. One bill would not be a comprehensive solution to ensure privacy protections. "What we really need in privacy is an immune system," says John Wilbanks, Chief Commons Officer at Sage Bionetworks. "The assumption is that everything gets through at least one part of the immune system—what you really want is enough interconnected layers so that it's really hard to get through all of them." Maria Filippellli, Public Interest Technology Census Fellow at New America also asserts a similar approach. "I would take a multi-pronged and interdisciplinary approach, requiring the education of the public, oversight from elected officials and stronger legal protections for individuals," she says. What we need is to create new forms of power through an interwoven structure of laws that work symbiotically rather than competitively with one another.

b. **The policies provoke questions about how to improve existing privacy policy consent mechanisms.** The challenge of requiring "actual informed consent" has been a longstanding debate across industries like healthcare, research and law. Under much scrutiny are the classic text-heavy pop-up windows that individuals often do not read, as cited by investigative reporters, academics and researchers. Many of these bills we examined from the period of 2018-2019 mention some attribute of making terms of service and data policies more readable.

   "Privacy [involves] implicit areas of consent," Soraya Okuda, Education and Design Lead at the Electronic Frontier Foundation explains. "People are choosing to share what is in their comfort range [but] if data is sent elsewhere, does it align with them?" Beyond the initial privacy policy agreement window, will people be informed about ways in which their expected understanding of the platform data use is different than the actual

platform data use? To explore possible answers, the design practitioners we interviewed noted a few methods: just-in-time features to notify individuals of changes, improving "general settings" modifications and focusing on "plain-language" with straightforward wording so people understand what they're agreeing to. One designer suggested a "global design pattern for accept and decline consent features" in order to create more shared language. In the context of data-collecting vehicles and smart cars, Devin Gladden, Manager of Federal Affairs of Energy and Technology at AAA National highlighted an ongoing threat to consumers. "Cities and states around the country are trying to figure out how they can get access to the data and I think consumers have been left out of that conversation," he said. Beyond improving consent on a design level, consumers must be incorporated into the decisions of data-collectors who are using their information for potentially nefarious purposes.

c. **Another common attribute of all of the bills was the need for further clarification and definition of key terms.** Many of the people we spoke with highlighted some confusion about specific terms or how they would play out in practice. It is important to note that in some bills, the regulatory agency is given rulemaking powers to implement and interpret the law. This means that anything that is unclear under the language of the statue can be interpreted and defined through a regulatory rulemaking process by that agency. Laws would ideally be accessible and understandable. We want to avoid laws that are overly vague and only understood by people who are not necessarily legal, academic or technical experts. The SMART Act, for instance bans the use of "addictive" features like autoplay and infinite scroll on social media, while at the same time failing to adequately define "addiction." "...It seems odd to ban very specific interaction behavior," Peter Dolanjski, former Director of Privacy & Security products at Mozilla told us. "I think this is hard to define and there are just so many corner cases including ways to work around these types of constraints, so specifically banning what currently are perceived to be the addictive aspects of social media would not be easily enforceable." Interviewees noted a lack of adequate definitions for the Online Privacy Act (OPA) and COPRA as well, particularly with the "duty of loyalty." When discussing OPA, Najarian Peters asked, "What does impermanence mean?"

6.2.4. Unique aspects for each bill

In this section, we will explore higher level themes that were unique to each bill we analyzed with the interviewees we spoke with from varying backgrounds.

The *Social Media Addiction Reduction Technology (SMART) Act*

Just to reiterate, this bill incorporates less of a "privacy" specific related framing and more on platform "addiction" and improving the quality time spent on platforms. We chose bills based on a variety of perspectives about data collection and user experience features in a technology. The SMART Act in particular highlighted a number of design and feature specific recommendations.

a. **Notice & Control:** In the full bill, this suggests provisions that allow "a user to set a time limit that blocks the individual's own access to those platforms across all devices" and "provides users with regular disclosures", and around time spent on a platform. "Transparency with time limits makes sense to me," reflects a product management leader at a major healthcare institution after reading more details about the SMART Act. Depending on the design, "it may come off as more heavy handed than just transparency [...] especially if they come off as forcing functions [or] reduce the quality of the app experience." "People don't like being told what to do, even if they've imposed their own caps." a product director at a tech company explains. "People just generally have a bad reaction to technology that tries to force a change in their behavior." Additionally, limits to screen time may invoke a sense of "protestant work ethic" – based in a desire to have people working instead of using social media. There are tensions for industry practitioners to balance the best interests of the individual with coming off as paternalistic and controlling. A few social media firms have already designed controls allowing users to limit their time spent in an app. Other companies have design parental controls for limiting screen-time.

b. **Specificity:** Some of these sentiments also stem from another strong theme: specificity. For example, the bill suggests that platforms "[display] a conspicuous pop-up to a person not less than once every 30 minutes." Many of the people we interviewed asked about the significance of 30 minutes. What research provoked that particular number? Who in power gets to decide these potential time limits? The bill also distinguished specific features to be banned including infinite scroll, auto refill, autoplay and badges and other awards linked to engagement with the platform. Policymakers and lawyers highlighted that specificity may help to more easily define, identify and regulate. However, practitioners and researchers we interviewed made the point that there can be both positive and negative aspects of those features.

The *Online Privacy Act (OPA)*:

a. **Individual rights vs. Enforcement:** The Online Privacy Act highlights a list of individual rights to access, correct, port or delete their data. It also creates new rights such as data impermanence. Many of the interviewees responded positively about these rights and some reflected on how they have seen these provisions in the EU's GDPR or even in their own online experiences. On the other hand, people questioned how these rights would be enforced or what would happen to marginalized populations that are often left out in some way. Najarian Peters, Faculty Fellow and Assistant Professor in the Institute for Privacy Protection at Seton Hall Law School points out that "the bill grants every American the right to access, correct or delete [...] but impermanence is a tricky concept because we should be thinking about status when we think about impermanence." Peters further explains, "The 1974 Privacy Act grants every American the right to access, correct, or delete...but what about people who are not considered American

right now? It is important to note that the "individual" is defined in the bill as a "natural person residing in the United States for that reason. Especially as we think about some of the things that are happening under this administration where rights once recognized are now being taken away or blocked de facto." One of the biggest challenges of any of these bills is how to implement them into practice. As we continue to explore different ways to push legislation to meet the needs of individuals, we must integrate disciplines to ensure we have perspectives of the variety of challenges and use cases.

b. **New ways to advocate for rights:** This bill placed a strong emphasis on avoiding burden on the individual to navigate privacy protections on their own. Most notably, the Digital Privacy Agency (DPA) would enforce rights and could "issue regulations to implement this bill and issue fines for violations." Interviewees had mixed reviews on this approach. Some supported the effort saying that we need institutionalized regulatory power in order to incentivize industry to change and better protect consumer data. Several other bill approaches, along with a few participants suggest that the FTC could just expand their capabilities instead of starting up an entire agency from scratch. The Online Privacy Act also highlights that harmed individuals may delegate nonprofits (e.g. the Electronic Privacy Information Center) to bring collective, private civil actions for damages. Mason Kortz, Clinical Instructor at the Harvard Law School Cyberlaw Clinic, highlights the important legal implications of this work. "If we take privacy seriously, then yes we're going to create a private right of action. It is going to create new lawsuits. It's not going to completely overrun the courts, but even if it did, that would show there are a lot of people whose privacy is being invaded."

The *Consumer Online Privacy Rights Act (COPRA)*:

a. **Privacy as a fundamental human right.** According to WIRED reporters, this bill "set up a sort of privacy bill of rights for Americans while providing some stronger mechanisms of enforcement." It followed Senator Cantwell, Feinstein, Brown and Murray's set of privacy principles which aims to lay the foundation for federal privacy legislation. In response to the COPRA bill language we previewed, one interviewee mentioned that if privacy were a right, "it should be socially unacceptable to charge more for basic privacy or security functionality." Access to tools and resources should not be attainable through cost barriers. This would require an industry shift in culture and norms around privacy and security. Another interviewee mentioned, "These rights are so broadly defined, it's not clear what I should be expecting from a browser, platform, or device level to actually see and expect." This comment brought up questions about how a bill impacted the physical design of the platform versus the management and business operations of a platform. In other words, how will a bill impact what people *see* versus what they can expect is happening *behind the scenes*?

b. **Duty of loyalty.** Many interviewees were confused by the term "Duty of Loyalty," a concept that stems from privacy scholar Jack Balkin[29], and wondered if a term like this would be actionable. A product manager we interviewed interpreted the term as the "duty to look out for the users' perspective of their data" but caveated that "in some organizations that culture of conservatism is baked in while in others, not so much." This bill sparked conversations around how to define and maintain culture change to uphold values created through policy proposals. Alex Gaynor, Security Engineer and Chief Information Security Officer at Alloy, mentioned that "user research is necessary to understand what a term like duty of loyalty means in relation to individuals' expectations" of some of the bill tenets. In this legislation, there are many missing key definitions to help understand actual rights of humans and responsibilities of organizations. For example, giving people the right to delete data brings up questions when it involves multi-party conversation or photos tagged with multiple people's names, with intellectual property rights clashing with the right of deletion. If my friend posts a photo of a group of people and tags them, do the people in the photo have the right to ask for that photo to be deleted? What happens to the comments or captions associated with that photo? Data portability is key to this point, Gaynor explains, "I don't have a position here on 'what's correct', just that I think all the answers are non-obvious. Exposing too much of your friends' data to a third party (as in an export or API use case) is how you end up with Cambridge Analytica. Exposing none at all and there's no way to take your data and leave a platform." More research and cross-industry collaboration is needed to experiment with ways to solve these questions.

6.2.5. Recommendations for policymakers: Integrate individuals and communities, determine ways to improve process and policy language structure

We developed the following recommendations based on insights from interviews and from our own process of engaging various stakeholders in policy feedback. Prototyping may be one relevant way to test draft data privacy related policies before they are piloted and implemented for a broad audience. Some of these processes and practices below are already in existence with policymaking teams. We recognize these recommendations may not be as easily applicable for every policy, especially given the endless complexities and edge cases that may exist. However, this is especially a fitting method when the draft policy may impact the design and development of products and services. What we describe in this section is a high level process that may help clarify ambiguities, mitigate risk of unintended consequences for individuals by bringing challenges that may occur earlier in the implementation process. We reflect on some of the strategies we employed and the learnings we gathered from this research experience.

6.2.5.1. People recommendations: Talking to stakeholders on the ground who may experience the harm first-hand.

[29]Balkin, J. M. (2015). Information fiduciaries and the First Amendment. UCDL Rev., 49, 1183.

- **Gather research and insights directly from *individuals and/or data stewards* who understand and have some level of lived-experience of marginalized communities who may be most adversely impacted by these policies. In policymaking, there is a current lack of engaging individuals in policymaking today. The voice of the consumer is often heard second or third hand from reports or through advocacy organizations.** From pediatricians to social workers and librarians, we spoke with data stewards, or people who handle and manage sensitive data for marginalized and vulnerable populations everyday. Rather than asking for *solutions*, we mainly focused on understanding the nature of their work with regard to data privacy and how policies have impacted people. They were able to provide concrete use cases where policies have and continue to negatively impact their communities. There is no substitute for speaking with these communities who are often left out of decision-making processes that strongly impact their lives. Advocacy organizations and human rights and civil rights related groups are closely aligned to protect human and consumer rights and would be helpful to gather their perspectives and feedback as well. Policymakers and industry practitioners could also "create easy channels for advocacy and [human] rights groups to provide feedback and publicly respond to such feedback," explains Sage Cheng, Design Lead at Access Now.

- **Continue to collaborate directly with individuals and privacy minded experts in advocacy organizations, industry, academia, and government *throughout your iterative policy process*.** We note that some level of this is already done with many teams today, but we recommend getting as close as possible to the individual who is actually using and is harmed by these technologies. This is to ensure that technical standards, policies and processes are clear and actionable for people to manage and protect personal privacy. From our research, these experts can help provide knowledge of use cases that span a variety of sectors and also point to frameworks, studies, and stories of trial and error to help advance policy work. We spoke to a policymaker who mentioned their team regularly reached out to tech industry contacts such as designers and engineers at Google or Facebook. These industry practitioners were able to respond to and share case studies and research with policymakers while the bill was still being drafted. We want to recognize that there is a big opportunity to collaborate closely with individuals or groups who facilitate direct interactions to get their perspectives and expertise on similar technical and design problems.

- **Recognize the need for precision and evidence: Major findings from our interviews related to the three privacy law proposals highlight a strong desire to link policy action to research and evidence.** First, policymakers need to articulate the specific problems and associated harms they are trying to solve. Second, it should be clear from both the bill language and public discussion that policymakers have consulted with the research investigating the outcomes of certain restrictions or modifications to ensure that the regulations that they are attempting to create are viable. The bill language does not always cite the problem, but when it does, say in a "Findings" section, it has almost

no legal impact. Speeches, press releases, and, more importantly, committee hearings can be better tools to highlight the research to help create the case for more viable policy recommendations. This is related to the issue we identified in the previous section with Research Question #1 (6.1.3.c). There, we noted the necessity of consulting with individuals from various sectors. In this case, it will be advantageous to consult with the research from various sectors to create laws that are well directed.

Note for recommendations I & II above:

- Policymakers can facilitate a "premortem" with both experts and individuals to imagine how the policy may impact others as both a failure and a success. They can list the elements that contribute to each scenario, possibly clarifying ways to improve draft language.
- We also want to acknowledge that there are many existing efforts to bridge the divide between technology practice and policy. Congressional teams are hiring staffers with strong technical expertise and institutions and organizations are facilitating some of these conversations: TechCongress, The Aspen Tech Policy Hub, AAAS Fellows, Code for America, Mozilla Fellowships, New America's Public Interest Technology team, and many more.
- We want to highlight the Design Justice Network Principles as a resource that focuses design processes on "people who are often marginalized by design and use collaborative, creative practices to address the deepest challenges [their] communities face." It is important that Congressional staffers integrate constituents into their process. With these principles in mind, we suggest policymakers reach out beyond technology companies to organizations with technical and design expertise, such as research groups like Citizen Lab, along with people who have lived-experience having used or been affected by these platforms. Some examples include: Design Justice Network, Detroit Digital Justice Coalition, Civilla, Voto Latino, Contratados, Library Freedom Project and Coworker.org.

6.2.5.2. Process recommendations: Making alterations in the policy research, prototyping, and drafting process in order to better align the needs with outcomes.

- **Simplify the bill as a one-pager (similar to the press release), aiming the messaging at industry practitioners who make product or design decisions with policy in mind.** Already, policymakers create press releases, one-page summaries, and section-by-section breakdowns as well as offer full text of their bills. What we are suggesting is a document that may be written specifically for practitioners in mind using appropriate language, guiding points, etc. The goal would be to translate bill text so that designers and engineers can understand the key points, solicit reactions and understand challenges of implementation in advance. Doing this would force policymakers to think about practitioners as they are drafting language that may have implications on technical processes.

Note: Condensing policy text into a "one-pager" means that nuance and details will be left out and could create unintended complications. In this case, it would be helpful to create a set of guidelines or processes for text approval in order to reduce the risk of oversimplification across policy teams.

- **Solicit help from industry practitioners and community advocates (or similar) to design and test policies with low fidelity versions of prototypes — when relevant and possible.** These prototypes can be of generic, bare bones websites, mobile applications, social media applications, and other related formats that specifically apply to key attributes of the bill text. Showing key stakeholders draft bill text for comprehension is one helpful aspect, but being able to present a visual that highlights certain bill features may invoke different insights that may be helpful to reflect when drafting policy. Direct feedback about what may and may not work may produce better bill related text. Perhaps an existing organization that could build the capacity, such as Congressional Research Service or a revived Office of Technology Assessment should house these individuals as a shared resource.

  Note: We acknowledge there are a number of programs, initiatives, and government teams that exist to work on tech policy and implementation. We suggest to either reach out and integrate these resources into your process or embed this process and approach appropriately onto your team. These programs, while in existence, are not all comprehensive for any policymaking body and may not be as widespread as they should be. Additional questions to ask include: are there federal administrative laws applicable that require periods of public hearing and comment, and notice in the Federal Register? If so, what formats and time frame would be required? Of course, there are often meetings, forums, conversations, and hearings with stakeholders during the legislative process. Targeting audiences while legislation is drafted should be a critical factor in soliciting comments while drafting legislation or regulations. Policymakers should consider: who are the people who may be left out of this legislation? Whose perspectives might we not have that would be important to understand for this topic? In terms of threats and risks — how will this legislation be abused? How will various actors take advantage of it?

- **Before launching policies publicly, is it possible to test the policies in small, low-risk, time-boxed environments that relate to the bill's intended audience in a way that best fits the existing structures of the team?** These efforts do require more work up front, but may mitigate risks by understanding in a time sensitive, low budget way. For a step-by-step guide, we have created a Policy Prototyping Guide, available to download at https://letstalkprivacy.media.mit.edu/research. This also includes information on the structure of the roles needed to execute this work.

  Note: We understand there are restrictions from policymakers in disclosing bill language before it is live and possibly engaging specific organizations (over others) which may

appear preferential. However, consider where there is a possible and appropriate structure, approach, and implementation of these pre-pilot engagements.

6.2.5.3. Language recommendations: Consider the language and text related feedback we received upon testing 3 draft bill policies

While the details of this section may seem small, these details will help impact how courts will translate violations into law. Janet Linder, a lawyer and legal writer, editor, and a children's librarian in the Boston area mentioned:

"In drafting legislation and regulations, the crux of the matter is that language needs to be as specific as necessary but at the same time, as broad as needed. Litigation is so often about the meaning of an ambiguous law. Courts have to address what does the plain language of the text state or mean; if not easily apparent, then what is the legislative history, or what other sources can inform how the court should decide what the law means? Legislation that is not carefully but comprehensively drawn can lead to drawn-out litigation and years of confusion."

- **Strike a balance of granularity in policy language. When policymakers use general language such as "Duty of Loyalty" or the "Right to Impermanence," include examples in the legislative history and common use cases of what this may mean or look like in practice when possible.** This is helpful to better understand more obscure topics without anchoring policymakers to information that is too specific. Based on the interviews we conducted with individuals both with and without privacy and/or legal expertise, bill language came off as vague and confusing or read as a sweeping overpromise which may cause individuals to become immediately skeptical or dismissive.

- **Avoid being overly specific. Additionally, the level of specificity in bill language, if too granular, can be seen as arbitrary.** For example, the SMART Act suggested that platforms "[display] a conspicuous pop-up to an individual not less than once every 30 minutes." Respondents asked about power ("Who made the decision?"), about the rationale ("Why 30 minutes?"), and about the origin of the 30 minutes ("Where did the research from this come from?").

- **Future-proof language. Definitions of key terms are incredibly helpful, but some terms, if defined, may quickly become outdated due to evolving technologies.** One policymaker we spoke with commented favorably on a term like "sensitive data", which is difficult to define. A decade ago, people may not have considered geolocation data sensitive because it was not as pervasive and easily aggregated with other data points from platforms as it is now. This issue is further exacerbated in that many of the bills focus on one, major, aspect of data collection and privacy, usually the social, and neglect environmental data collection. It is important, then, for policymakers to use terms that

may evolve with different data-related concerns.

6.2.6. Insights for industry practitioners: User research findings and how to keep privacy UX and UI in mind on an individual and societal level

For this section, we aim to give recommendations to industry practitioners about the interviewee feedback we received relating to privacy design and design elements. We present both insights and raw quotes to support the findings.

- **Individuals want a balance of both control and empowerment over what they can do with their data, but not in a way that would overburden or diminish the platform experience.**
    - *"Platforms are constantly changing, and I feel like if you were to limit infinite scroll that it would create some new sort of populating device. So I think it makes more sense to create rights on the side of the user engagement." - A Let's Talk Privacy project interviewee*
    - *"I think it's odd that people don't know the algorithm. I think that stuff should be publicized." - A Let's Talk Privacy project interviewee*

- **Consider the individual and community impacts when oscillating individual control between passive and active.**
    - Participants had more positive reactions to design proposals, which gave them controls and choices about their information. For example, participants liked being able to delete their data. However, when the design was more passive, participants presented negative reactions. For instance, respondents didn't like the concept of having a timer on a webpage to control how much time they are spending online. They found passive designs to be "restrictive." The design features that received the most positive feedback from participants were the ones which provided participants with information about their data (informative features) and gave them choices to control their personal information (active features).

- **Explore people's context and intuition about how they collect, use, and share personal information.**
    - Some individuals may want to invest all personal data in one platform to easily track and manage information. There is also an assumption that if one platform has some information (emails, messages), they know everything anyway.
        i. *"Rather than give my data to like a bunch of companies out there, I just like to use everything by Google because I know they already have everything from my phone, camera, smart speaker, photos, drive, etc. I'm just going to put it in one basket and hope to god like that one company is not going to turn evil." - A Let's Talk Privacy project interviewee*

- Some individuals have periodic 'data maintenance' habits where they check and purge information or accounts and others have a "set it and forget it" approach.
    i. *"Every couple of months when I log in, I'll go through and delete things. I delete my Twitter archive and I delete [tweets on] a rolling 90 day basis." - A Let's Talk Privacy project interviewee*
    ii. *"I've been slowly deleting platforms throughout the years and I've thought about deleting my Facebook." - A Let's Talk Privacy project interviewee*
- How much control or power over data is reasonable to assume individuals can manage? How much flexibility do people want? More insight into these questions may show what type of features the industry can better implement.

6.3. Research question 3: How do different stakeholders perceive proposed legislation aimed at modifying social media design?

6.3.1. Overview

A 2019 Pew Research Center study on American attitudes toward privacy and their personal information reported that 63%of survey respondents did not understand current data protection regulations. At the same time, 70% of Americans favored more laws aimed at protecting personal data. The wish for more regulation has not been ignored. Over the past decade, legislators have proposed a number of bills for protecting privacy, including the California Consumer Privacy Act, Maine's An Act to Protect the Privacy of Online Consumer Information, and Illinois' Data Transparency and Privacy Act. These laws require transparency about data practices and aim to empower consumers by giving individuals the right to access and delete personal information and opt out of data sharing.

In spite of these laws, or perhaps because of them, companies continue to fail to be transparent about their data practices. This lack of transparency has resulted in a number of recent incidents —or example, when Google failed to mention that its Nest Secure Hub has a microphone or when reporters discovered that Amazon employees can listen to conversations from people who use Alexa. These privacy violations, and others like them, indicate that legislation may not be achieving the outcomes desired, and/or that the laws allow too much flexibility in compliance and interpretation. Therefore, it is critical to explore the solutions various stakeholders recommend for mitigating these privacy and data governance issues.

As part of the interview brief protocol, we asked participants the following questions:

- Looking back on the bills and design prototypes:
    - What do you believe is the biggest privacy issue?
    - If you had a magic wand, what would you do to fix that issue?

    - What are you thinking about now that you weren't thinking of before? What resonates?
- Have you done anything to protect your own privacy (changed settings, changed public actions)? What resources did you use to guide your thinking in that?

Based on those responses, we synthesized the commonly mentioned privacy issues and how each of the different participants emphasized possible angles to mitigate privacy harms. This part of the discussion highlights the numerous disciplines and possible ways to intervene. We illustrate in more detail below. Participants' responses identified the particular privacy issues deemed most pressing, as well as a number of solution-based recommendations.

Almost all of our participants noted the need for a holistic and interdisciplinary approach, taking into account the multi-faceted nature of privacy and the needs of individuals and organizations. This interdisciplinary campaign would integrate privacy education and public privacy-related awareness as well as diversify companies' leadership, among other things. The preference for a holistic approach to protecting privacy highlights the necessity of collaboration from the stakeholders to provide solutions to increasing privacy challenges.

6.3.2. A holistic and multi-faceted solution to online privacy

Our participants mentioned a number of solutions to tackle the privacy challenges related to their expertise and experiences.

Offer privacy education: A commonly mentioned approach to enhance privacy protection was the creation of privacy education targeting the public, companies, and legislators.

Participants identified various ways to educate the public about digital privacy, including mandating privacy training in primary education. Many participants noted that K-12 students do not learn about digital privacy in school, potentially leaving them at risk for privacy-related harms as more technologies enter their lives. Observing the necessity of including privacy in education system Vanessa Barone, Research Scientist at Sage Bionetworks, said:

> *"It almost feels like it needs to be incorporated into our educational system so people understand. Obviously the curriculum changes as this field moves, but at least we have some information on what is data, how is data collected from you, and what are some of the uses of your data. [This way] they have some resources to fall back on because right now there's no curriculum for this unless you go into a specialized field, or you work in the tech sector."*

Additionally, Janet Linder, a lawyer and legal writer, editor, and a children's librarian in the Boston area, expressed that "*educational components are so important. Just as children must be literate and numerate, they need to be educated about these digital privacy issues throughout their years of education, at the level appropriate for their ages.*"

More than just providing information about privacy, some interviewees discussed the importance of tailoring lessons toward different populations.

> *"There are studies that show that different generations hold different definitions of privacy," explains Becca Ricks, Researcher at Mozilla. "Young people tend to define it as having control over what other people see and now, whereas older generations tend to associate privacy with corporate and government surveillance. Education needs to address these varying attitudes."*

For example, one of our interviewees reported that it is important to consider age range when providing privacy education to people and communities:

> *"For young people, [education] could be in a classroom, but older people, maybe adults, it would be a short little video they watch on social media that [...] educates you about the possible ramifications of you unknowingly sharing your data. [...] Education would have to be formed [by] bringing in the perspectives of who you're targeting to designing education."*

Along with students, interviewees identified organizations and legislators which would benefit from privacy-related topics. An interviewee identified educating legislators as the magic wand to solving privacy challenges:

> *I would require anybody who is working in this area, particularly legislators, who are creating these bills [to go to a] boot camp to understand the history of privacy protection in this country and start with all of not just the legislation and [...] legislative history [...] why did they want to create post Watergate, the 1974 Privacy Act? What does that mean?*

Increase public awareness related to privacy through transparency and choice: Relatedly, some interviewees identified public-facing campaigns to increase people's awareness of privacy violations. Rubez Chong, Graduate Student at MIT Media Lab noted the role of the media to be especially important to report data breach incidents and increase awareness:

> *"People are growing in consciousness of these issues. [...] I'm super hopeful I think that will change [...] people are slowly becoming conscious. And over time, once that reaches the masses, we have leverage from a consumer perspective."*

A number of our participants acknowledged tensions between having the option of choice and how that may conflict with the convenience of using a product. Practitioners must gather insights from continual usability testing and human feedback in order to uncover patterns of both positive and negative impacts of UI design changes. They must also have a process in place for evaluating and weighing those tensions and possible tradeoffs around usability and

individual rights. New features that are meant to improve a person's experience, even with the best intentions, may have unintended impacts with other parts of the product or service. Chong compared messaging platforms in terms of their convenience and safety:

> *"I think because Signal doesn't have the functionalities that you would get from Telegram or WhatsApp, I think it comes back down to the designers as well. Can we design very secure platforms that have fantastic user experience?"*

Although transparency around organizational data practices was a critical solution for our participants, several discussed the importance of organizations informing people about their rights and offering them data protection choices including control over data sharing, data selling, and data deletion. In terms of empowerment, some participants placed an emphasis on making it it easier for individuals to pursue remedies for privacy violations. "CCPA only provides a limited private right of action in case of data breach, while many breach notification laws do not create a private right of action," shares Mason Kortz, clinical instructor at the Harvard Law School Cyberlaw Clinic. "For state consumer protection laws, almost all create some private right of action, but some are pretty narrow and exclude financial or real estate transactions." Many current privacy and consumer protection laws do not permit individuals to bring claims in court. Reversing this trend and providing a private right of action for privacy violations could increase pressure on platforms to provide meaningful privacy controls.

Advocate for platform decentralization: Several participants associated privacy challenges to capitalism and power imbalances. They discussed the role of culture and the economy to attract individuals to specific platforms and companies and how capitalism would harm people's privacy. Current uses in support of decentralization include the exposure notification and contact tracing systems being developed due to COVID-19. Alternative data governance structures have been proposed, such as data trusts & data cooperatives as the most prominent examples. Another approach to managing data differently is a data commons, open source data that is collectively managed by a community of users. One example is Mozilla's project Common Voice. Sam Mendez, a graduate student in Comparative Media Studies at MIT suggested using decentralized and open source platforms:

> *There are open source alternatives to things like Google Docs [...] but that also requires your own money to be able to run your server [...] I feel like the magic wand would be a more equitable income distribution. I think a lot of the open source alternatives to these things require a certain amount of technical expertise that like you have to have the time and resources to learn or require you to be able to pay someone to do it or to host things yourself. [...]If people in general, had more time to learn, and had more resources to use on their own, they would open up the doors for some of these things like wider use of open source platforms and more decentralized stuff. Yeah, my magic wand I guess, would be anti-capitalism.*

Enable social media data portability: Another recommendation related to decentralizing platforms was to make their data portable from one platform or company to another. Valerie Michel, Systems Engineering PhD Candidate at University of Virginia shared:

> *These platforms are also linked [...] I was trying to set up something with my Bitmoji and I had Snapchat in order to set it up, and I know that Bitmoji and Snapchat are owned by the same people, but it's kind of annoying that you have to log into another app to log into to get an app to work [...] I think I would change that.*

Increase organizational data use transparency: Equipping individuals with privacy-related decision making was a common topic in the interviews. They reported that in order to help consumers make more informed privacy decisions, companies should enhance their transparency about their data practices. Our participants particularly urged companies to provide people with information on:

- The type of data is being collected about them.
- For what purpose(s) users' data are being collected.
- To whom users' data will be shared with.
- To whom users' data will be sold to.

Tianyuan Cai, a research analyst, discussed the importance of transparency:

> *"Make sure everyone understands how their information is stored and being used. [...] websites help them make their choice better [...] but make sure they're making an informed choice."*

Some participants mentioned that providing transparency to consumers could benefit the companies by increasing consumers' trust. If more powerful companies provide more transparency around their data practices, this could lead to market competition and that may incentivize other companies to be more transparent and improve their data practices to survive in the market.

A number of participants discussed how important it is for companies to provide accessible and understandable information to consumers to more effectively inform their privacy-related behaviors. Charyti Reiter, Director of Programs at On the Rise talked about providing knowledge in a more accessible way:

> *"I think a terms and conditions icon that you click on might be shorter and more straightforward and it should use simple terms so that people can understand."*

Diversify leadership in data-collecting companies: One major theme was to incorporate voices of marginalized populations in top level decision-making. To accomplish this, one

recommended idea was to increase diversity in corporate leadership. Maggie Hughes, Graduate Student at MIT Media Lab discussed why this matters by saying:

> *"I don't know if companies had the capacity to care for the individuals and understand what privacy means to them and understand the nuances of that for different communities."*

Instill accountability, corporate penalties, and clarity of legislation: Interviewees commonly mentioned to make stronger legislation to make companies accountable for their data practices. To facilitate accountability, some participants discussed the critical role of auditing companies' privacy practices. Some believed that current legal penalties for privacy violations are less than the potential gains for the companies to commit the data collecting violation. Therefore, they suggested revising the penalties to better fit the harm caused by privacy violations. Maria Filippelli, Public Interest Technology Census Fellow at New America mentioned:

> *"It's important to make sure that things are enforced properly, because [...] we don't want these to be kind of like token laws [where] it's out there, but we're not holding people accountable. We should really make it hurt for [companies] when things are violated [...] there needs to be [...] penalties that fit the damage [properly]."*

Sage Cheng, Design and UX Lead at Access Now explains another way to look at this recommendation is to create *"positive encouraging mechanism[s] in addition to penalties to hold companies accountable."* For example, Access Now encourages companies to release transparency reports to disclose original stats on government and third-party requests for user data, content, and account restrictions.

Participants had recommendations on the wording of the laws to make them more accessible to people to understand and reference when needed. The suggestions hovered around being broadly accessible and written in plain-language, and providing specific guidelines. An attorney we interviewed with discussed the importance of having clear and detailed laws as a way to address privacy challenges:

> *"I would want very clear regulations and laws and very broad laws that touch on all of the details. And [...] to make the laws as broad as possible and as clear as possible and then leaving nothing left to interpretation."*

6.3.4. Recommendations & Insights

Based on the solutions mentioned by our participants, we distilled a number of recommendations to various stakeholders on how to better protect individuals' privacy. Any promising solution must take an multi-faceted approach, requiring teachers, parents, students, school administration and privacy advocates to work together toward a common goal – enhancing individual safety and well-being through privacy protecting measures in the technologies.

I. **Offer age and context-appropriate privacy-focused education opportunities:** Such an interdisciplinary approach can start early on by incorporating privacy-related courses in the K-12 education system. As technology evolves on a daily basis, people's information could be collected and used in more complex ways which were not possible in the past. It would be helpful to have an education system that teaches students about privacy protection and risks through continuously updated materials. We recognize that simply adding mandatory content to school system curricula is not easy and requires many conversations, approvals, and agreement from school officials. However these topics can potentially be integrated into existing core competencies such as contemporary civics or comparative history lessons. These lessons must be age-appropriately designed. For example, talking to a 5-year-old about information asymmetry, power dynamics and two-factor authentication is not appropriately framed or relevant to them.

Additionally, this education does not need to be restricted to schools. For example, companies can provide privacy lessons in employee onboarding practices. One of our interviewees recommended social media companies could provide privacy-related training directly on their platforms, teaching people on how to better protect themselves when using such platforms. One thing to note here is that this places a high degree of the responsibility onto the individual when often the harms are taking place at a level of abstraction where individual actions cannot account for the harms. Chris Gilliard, Professor of English at Macomb Community College, explains, "It's tantamount to expecting each person who eats beef to inspect the meatpacking plant."

We do not intend to say that the burden should be on children and individuals to learn about the technology, but more about empowerment to better understand how technology works, and if interested, explore how to be conscientious consumers (and perhaps future designers or engineers) of these systems. For example, a group of us worked with Girl Scouts of Eastern Massachusetts on Cybersecurity Badge Day workshops that integrated concepts around:

- Building intuition about the opportunities and limitations of YouTube recommendations
- Offering a creative workshop to teach students about the challenges of designing advertisements with transparency
- Exploring designing online consent in social media platforms with a focus on the Children's Online Privacy Protections Rule (COPPA).

We would like to note there are many existing efforts to improve youth data literacy from Blakeley Payne, Erica Deahl, Berkman Klein Center's Youth and Media, LSE's Media and Communications team, and existing Girl Scouts curricula. Advocacy groups like the Common Sense Media and Campaign for a Commercial-Free Childhood are engaging with parents to provide helpful materials and information to decide what topics of data

collection, privacy and security to share with their children. This could be useful context for work in this field.

II. **Enhance organizational transparency practices:** Referring to any data-collecting organization and across sectors, organizations must disclose their data collection and use practices in a timely, consistent, and comprehensible manner. Researchers have uncovered that people do care[30] and would want to know more information about data sharing. However, there can be diminishing returns. With endless privacy and security disclosures and warnings, humans may ignore them. Studies[31] have suggested people need to be re-sensitized with fewer warnings — companies need to be deliberate about the frequency and method of approach. Well designed and tested disclosures will allow individuals the ability to make better informed choices about data protection. Non-users and policy-makers will also benefit from understanding the data ecosystem. Policymakers can use this information in an attempt to better regulate. It is important, too, for non-users to understand organizational data practices as well. Though not directly used by an individual, a service or product may have widespread implications for individual privacy and security. It is important, then, for everyone to have the ability to learn about these data use practices, and be able to advocate for regulation and/or make data protection choices.

III. **Codify choice:** To codify choice would mean to enshrine individual decisions into the design of the system. True privacy, data protection, and security require individuals to be able to make decisions about the collection, use, and deletion of personal data. It is important to note that the word “delete” may be operationalized differently, depending on the platform. For example, people may be able to request data deletion for future use, but some of the data that was gathered during use may remain in the system. Though organizations have business and service related targets, it is important that individuals be able to maintain autonomy and make the choices they deem best. This may, then, require that organizations provide granular controls for what information an individual would like to choose to share, practice data minimization, or not collect data at all without allowing individuals to decide whether or not they wish to participate in the data use scheme. To codify choice in practice, many platform organizations standardize data collection and processing to facilitate individual choice to move data between systems and/or use of other purposes. Additionally, similar to our previous recommendations in Section 6.1.4 around offering a shared vocabulary across disciplines, it may be helpful to create a shared structural approach,[32] along with

[30]Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013, July). " Little brothers watching you" raising awareness of data leaks on smartphones. In Proceedings of the Ninth Symposium on Usable Privacy and Security (pp. 1-11).

[31] Krol, K., Moroz, M., & Sasse, M. A. (2012, October). Don't work. Can't work? Why it's time to rethink security warnings. In 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS) (pp. 1-8). IEEE.

[32] Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*(pp. 1-17).

vocabulary to discuss and compare different privacy notice designs. Many studies have found that privacy policies are often ignored.[33] Creating a universally comprehensible design that is both targeted, relevant and actionable would better help improve human choice.

[33] Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, *10*, 273.

7. Conclusion & next steps

Privacy has and will continue to be evaluated as new forms of data collecting technologies continue to evolve. Both qualitative and quantitative research will be helpful to understand the social values that shape how we both define and prioritize how people legislate, build, design and advocate for privacy in the products and services we use every day.

7.1. Summary

A core motivation of Project Let's Talk Privacy was to incorporate and amplify diverse voices in our investigation. We embraced this perspective through each of our research questions. Research question 1 (Section 6.1) focused on how various roles use and think about privacy in their relative fields. Our findings illustrate how different roles emphasize protections, harms, and word choice when communicating levers of change like civil rights protections in law to privacy design elements. In research question 2 (Section 6.2), we analyzed how these 41 participants responded to the strengths and challenges of each of these bills and prototypes. This solidified the opportunities to better bridge policy and practice by outlining common and distinct bill themes. We used these insights to create recommendations for policymakers: talk to individuals who experience privacy-related harm first hand, integrate prototyping and drafting process changes where possible, and consider language related feedback to improve clarity across audiences. We also created insights for industry practitioners by aggregating some human insights that could influence UX and UI design in data collecting systems. Lastly with research question 3 (Section 6.3), we illustrated how different stakeholders explored solutions in their work or experience to mitigate privacy and data governance issues. Based on these insights, we recommended that companies and organizations offer education opportunities, enhance organization transparency practices, and codify choice into the design of their products and systems.

7.2. Limitations of the research

The findings of this project are subject to limitations. The first limitation relates to our pool of interviewees. Although we interviewed a diverse set of participants in terms of background and professional roles, the demographic make-up of our group of participants was not representative of the United States population in terms of socioeconomic status, ethnicity, geographic region and level of technical exposure and understanding. Additionally, our research is reflective of US specific bills, processes, and participant responses. There are opportunities to do a cross-country or more global study. Many of the people we interviewed were in our direct circles, had technical experience, and had secondary degrees. This does not make our findings invalid but requires that we consider how the make-up of our participant pool may have implications for the answers we received during interviews.

Second, we conducted most of our interviews remotely by video chat or by phone. It would have been beneficial to observe some of the concepts and processes that the interviewers explained in practice. In addition, the answers to questions we asked (e.g. about their privacy

habits online) were self reported, creating a natural limitation of qualitative research. Future research, then, would benefit from direct observation and/or participant observation.

Additionally, as members of academic institutions, our immediate networks reflected our immediate circles, although we made an effort to reach beyond these networks. Specifically, it would be helpful to recruit individuals with no degrees (or less than advanced college degrees), more people of color, and more people who self reported little to no technical or data related expertise.

Lastly, the bills we selected were a subset of many that we could have chosen affiliated with data collection in some capacity. During the two-year period between 2018 and 2019, members of Congress proposed several privacy and/or data protection bills. Any of these bills could have been fodder for privacy research. Future research, then, could examine the similarities and differences in foci of the many bills to understand the major privacy-related concerns of legislators during this period.

7.3. Future design + research opportunities

There were many topics that we did not have time to investigate within the scope of this research. This includes but is not limited to the following:

a. **Human perception, intuition and comfort with various privacy bill concepts.** What do these actually mean in practice for the applications and services they use?
    i. Data portability: "*I think data portability is a really important element, like your friend graph and your contact graph. If we're going to have movement out of Facebook and Twitter toward decentralized privacy [and] enabling networks, […] that stuff is really important as a form of anti-competitive, so soft power.*" - *A Let's Talk Privacy project interviewee*
    ii. Right to correct data
    iii. Right to impermanence

b. **Data deletion:** When people request to be removed from mailing lists or to delete accounts, how do they actually confirm their data is deleted? In what capacity? What risks may still apply? Is it possible to still delete data if the app has used predictive technologies using your previous data?
    i. "*They've still got all the stuff they learned about you already. Which isn't data, right? These are sort of predictive features that let them make predictions about [people], […] they may have forgotten some very specific things about me, but they still know a shit ton about me.*" - *A Let's Talk Privacy project interviewee*

c. **Shared data and notions of ownership vs. human rights:** Especially in the context of photos, comments, or posts in social media platforms, where do we draw the line with who owns what data? Is a property framework relevant? If not, what is more fitting?

i. *"It's not even clear to me anyone writing legislation has thought about the question of like, what should happen when my friend uploads a picture to Facebook to me, and who gets to choose if that gets deleted? […] There is going to be some weird unintended behaviors."* - *A Let's Talk Privacy project interviewee*

ii. *"What prompted organizations, corporations to say, 'Oh no, the consumer owns their data,' right? But I don't know if any of this is possible. How do you edit how long a platform can keep your data?"* - *A Let's Talk Privacy project interviewee*

d. **Testing the policy and prototyping process on a larger scale:** We conducted a very small investigation by taking draft policies, creating wireframes, and testing them with end users, policymakers, researchers and practitioners. We recognize there are many constraints when designing and building policies including but not limited to: time, resources, existing habits and structures, and "buy-in" from many political stakeholders. In general, we believe it would be helpful to do this process alongside policy making teams in some capacity. The research gathered from the interviews could be a direct line of feedback back to the policy staffers so they are able to integrate and modify the text. In addition, there is an opportunity to test the policies in a small, closed environment before rolling out the policies nationwide.

7.4. Next steps

We will distribute this report, recommendations one-pager, prototyping guide, and website to academics, government employees, industry practitioners, lawyers, nonprofit and advocacy, and policymakers who would find value in these insights in some capacity. This will be done through the interviewees and Advisory Board that we have been working with and distributing information through our collective networks.

8. Team: Who are we?

We are a multidisciplinary academic team with experience across sectors including: policy, design, engineering, law, human-computer interaction, and research. Our brief backgrounds are below.

Anna Chung

- Designer, MIT Center for Civic Media
- Anna is a UX designer and researcher at MIT's Center for Civic Media. She has designed tools and visualizations for several social impact organizations, including the Design Studio for Social Intervention, Anti-Eviction Mapping Project, and 1001 Stories. She is passionate about using technology and design for public good.

Dennis Jen

- Lead Developer, MIT Media Lab / Center for Civic Media
- Dennis is a software developer at MIT's Center for Civic Media. He has an extensive background in building web application and visualization tools across a variety of industries, including genetics, oncology, neuroscience, and education technology. At the Center for Civic Media, he applies this background to developing technology for social good. When not hunched over a keyboard, he's often hunched over a pottery wheel or piano.

Jasmine McNealy

- Research Lead | Associate Professor, University of Florida
- Jasmine is an Associate Professor of Telecommunication at the University of Florida, where she teaches courses on regulation. She researches media, technology, and law with an emphasis on privacy, surveillance and data governance. She is also the Associate Director of the Marion B. Brechner First Amendment Project at UF, and a Faculty Associate at Harvard University's Berkman Klein Center for Internet & Society.

Pardis Emami Naeni

- Research Contributor | PhD candidate, Carnegie Mellon University
- Pardis is a final year PhD candidate of computer science at Carnegie Mellon University, where she is advised by Lorrie Cranor and Yuvraj Agarwal. Pardis is passionate about building usable tools to help people protect their privacy and security when interacting with Internet of Things (IoT) devices. During her PhD, Pardis developed a usable privacy and security label for smart devices to inform consumers' IoT related purchase decisions.

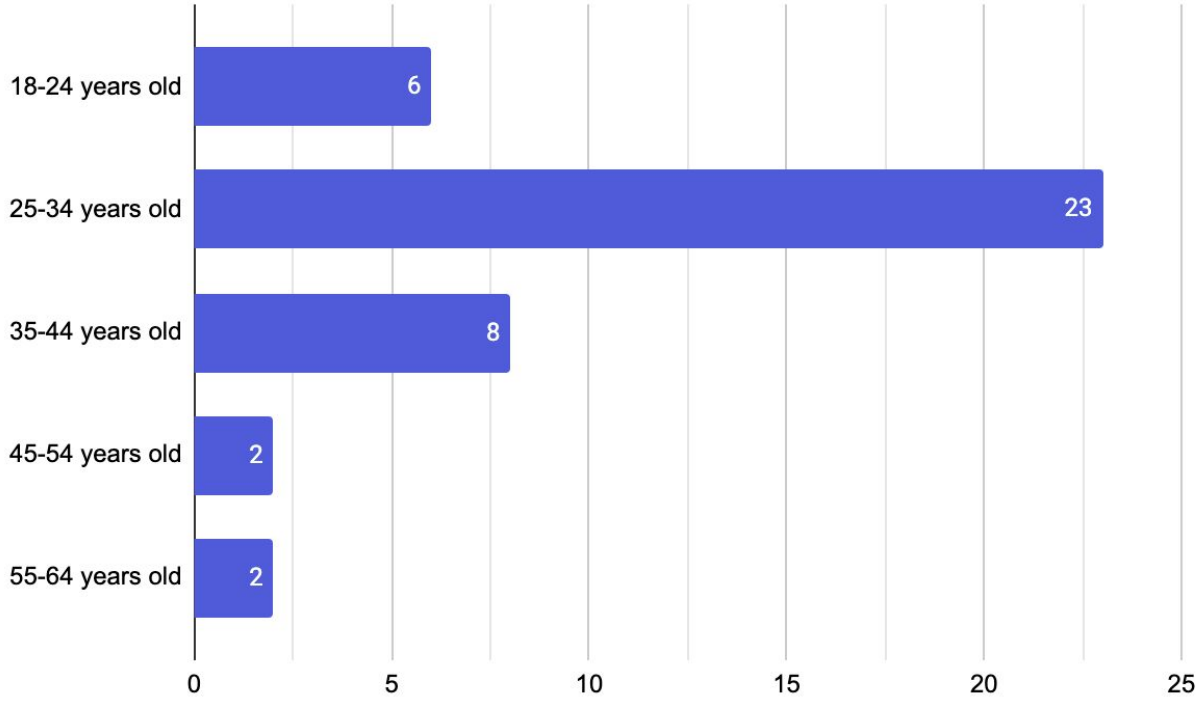
Stephanie Nguyen

- Project Lead | Research Scientist, MIT Media Lab / Center for Civic Media
- Stephanie is a research scientist and human-computer interaction designer focused on understanding data privacy perceptions and improving individual rights and experiences

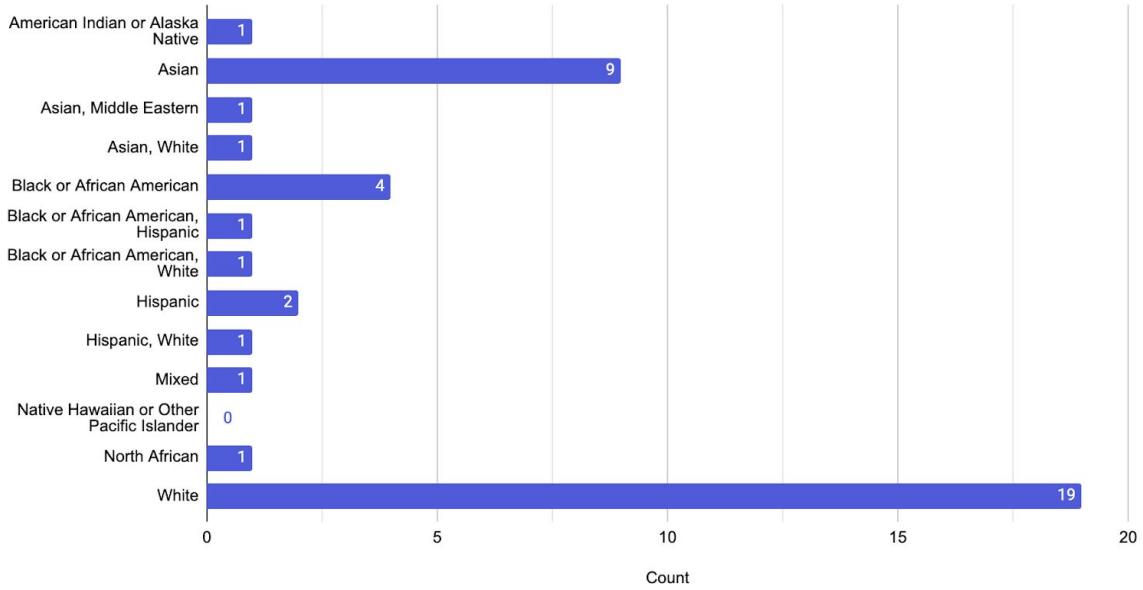
through design and policy for youth and vulnerable populations. She is an Advisory Member for IEEE's Advisory on Children's and Youth Experiences Ecosystem Committee and her research focuses on translating policy to practice by collaborating across policy, industry, and advocacy to reimagine meaningful choice and control in sharing personal data. She previously led design for government agencies at U.S. Digital Service at the Obama White House.

Appendix

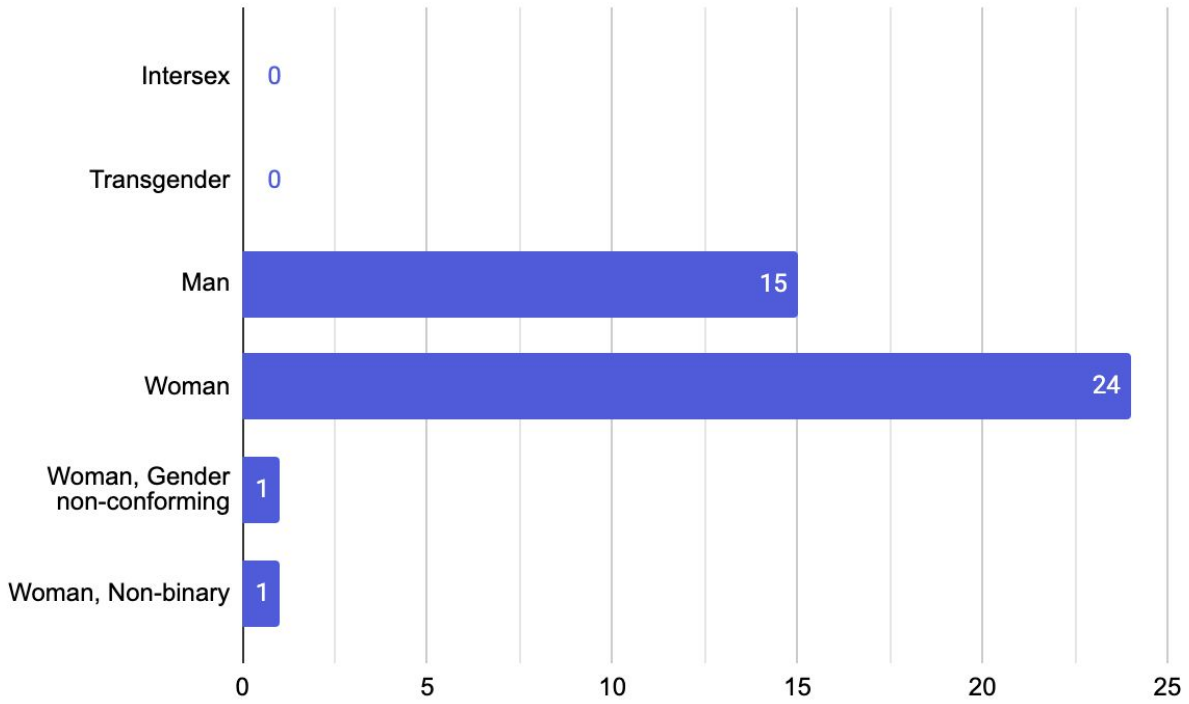
Appendix A: Demographic information of interviewees



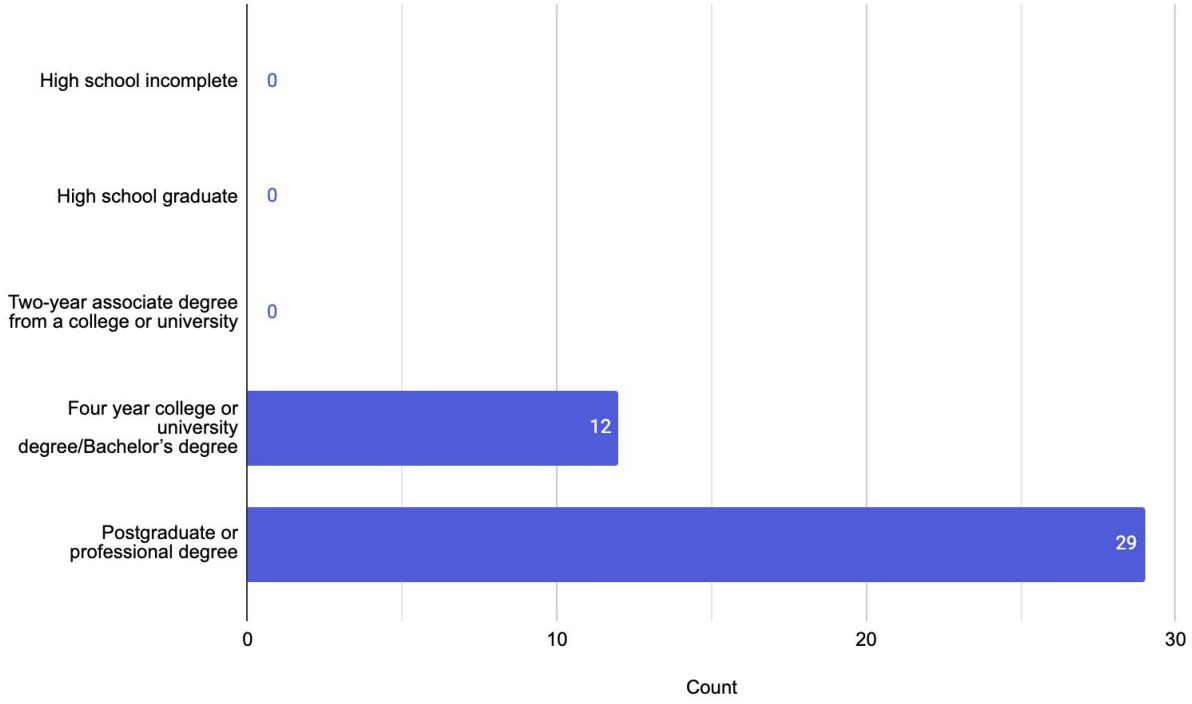
Q1 - What is your age?	Count
18-24 years old	6
25-34 years old	23
35-44 years old	8
45-54 years old	2
55-64 years old	2



Q2 - What is your race / ethnicity?	Count
American Indian or Alaska Native	1
Asian	9
Asian, Middle Eastern	1
Asian, White	1
Black or African American	4
Black or African American, Hispanic	1
Black or African American, White	1
Hispanic	2
Hispanic, White	1
Mixed	1
Native Hawaiian or Other Pacific Islander	0
North African	1
White	19



Q3 - Which gender(s) do you identify with?	Count
Intersex	0
Transgender	0
Man	15
Woman	24
Woman, Gender non-conforming	1
Woman, Non-binary	1



Q4 - What's your highest level of education completed?	Count
High school incomplete	0
High school graduate	0
Two-year associate degree from a college or university	0
Four year college or university degree/Bachelor's degree	12
Postgraduate or professional degree	29

Appendix B: Bill summaries

The following bill summaries were shown to participants during our interviews.

SMART Act (Social Media Addiction Reduction Technology)
July 30, 2019
Senator Josh Hawley (R-Mo.)

1. **Bans infinite scroll, autoplay, and other addictive features on social media**
    - Infinite scroll, autoplay, and "achievements" such as "Snapstreak" exploit the science of addiction to make it difficult to leave a social media platform
    - Exceptions include music playlists, social media predominantly designed to stream music, and "achievement" badges that substantially increase access to new services or functionality
    - Social media platforms would have to include natural stopping points
2. **Requires choice parity for consent**
    - Companies would no longer be allowed to manipulate people into consenting by making it difficult to decline consent
    - Companies would have to design "accept" and "decline" boxes using the same formats, fonts, and sizes
3. **Gives the FTC and HHS authority to ban other similar practices**
    - Rules would expire after 3 years unless ratified by Congress
4. **Gives users power to monitor and control their use time on social media**
    - Social media companies must provide an in-app tool that enables users to track the time they spend on social media across all devices and allows users to impose caps on the amount of time they spend

The Online Privacy Act
November 5, 2019
Congresswoman Anna G. Eshoo (CA-18) and Zoe Lofgren (CA-19)

1. **Creating User Rights** – The bill grants every American the right to access, correct, or delete their data. It also creates new rights, like the right to impermanence, which lets users decide how long companies can keep their data.
2. **Placing Clear Obligations on Companies** – The bill minimizes the amount of data companies collect, process, disclose, and maintain, and bars companies from using data in discriminatory ways. Additionally, companies must receive consent from users in plain, simple language.
3. **Establishing a Digital Privacy Agency (DPA)** – The bill establishes an independent agency led by a Director that's appointed by the President and confirmed by the Senate for a five-year term. The DPA will enforce privacy protections and investigate abuses.

4. **Strengthening Enforcement** – The bill empowers state attorneys general to enforce violations of the bill and allows individuals to appoint nonprofits to represent them in private class action lawsuits.

COPRA (Consumer Online Privacy Rights Act)
November 18, 2019
U.S. Senate Committee on Commerce, Science, and Transportation Ranking Member Maria Cantwell (D-WA) and fellow senior members Senators Brian Schatz (D-HI), Amy Klobuchar (D-MN), and Ed Markey (D-MA)

–

TITLE I—DATA PRIVACY RIGHTS

TITLE II—OVERSIGHT AND RESPONSIBILITY

TITLE III—MISCELLANEOUS

Appendix C: Policy Prototyping Guide

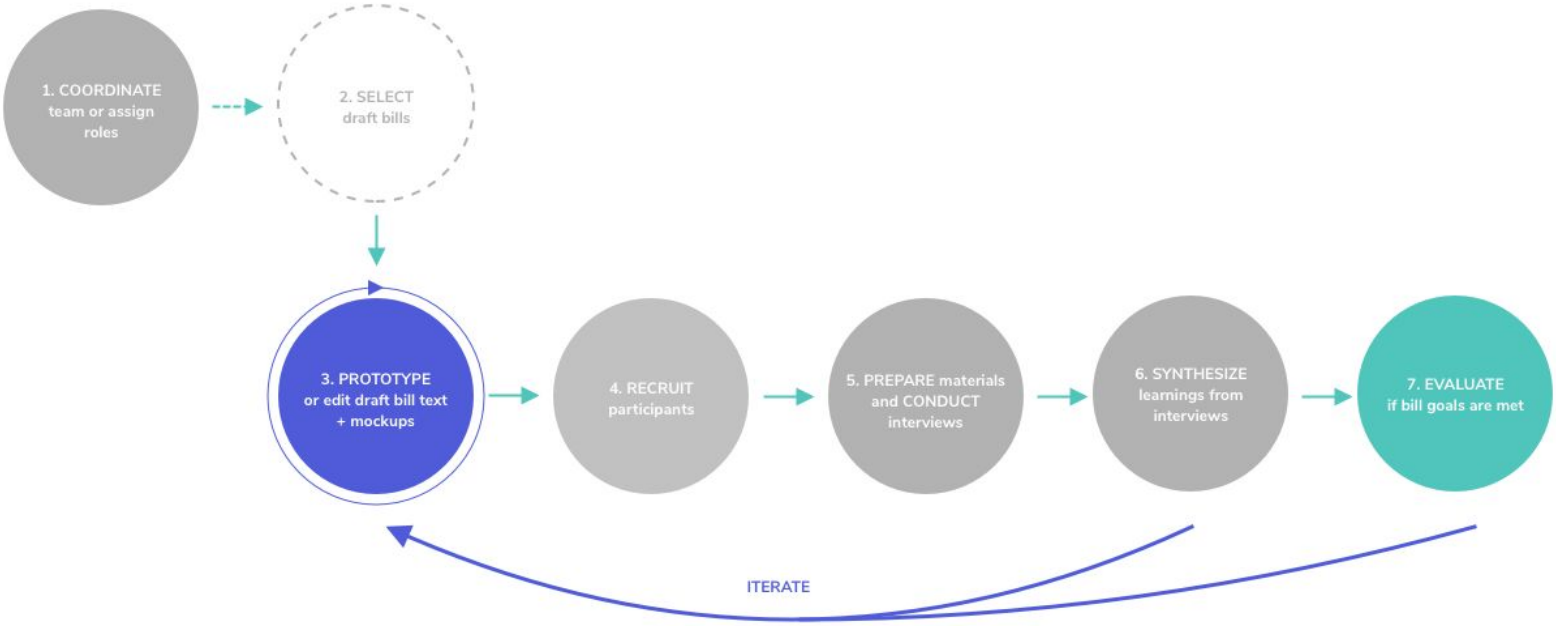
Part A: Purpose

Through our research, we advocate for a human-centered approach to policymaking. We have outlined the process we used to prototype bills and give policymakers a template procedure that explores how they may garner feedback on draft policy before publishing.

The process below was inspired by bills that referenced design and visual components of a data-collecting product or service. This version should be used as a starting point and should continue to incorporate feedback to improve the process and codify any patterns that emerge for particular domains. It is important to note that the context and content of the bill may change how the process can work. For example, policy centered around data privacy with accompanying UI components (e.g. increased transparency of terms of service or option for data portability) might follow a slightly different path from those policies that specifically focus on company policies and legal protections around data security. We see this process itself as iterative. This guide includes a high level diagram, role outlines, and a step-by-step framework.

Part B: High level diagram

1. Coordinate team or assign roles
2. Select draft bills
3. Prototype or edit draft bill text and mockups
4. Recruit participants
5. Prepare materials and conduct interviews
6. Synthesize learnings from the interviews
7. Evaluate if bill goals are met



Part C: Role outlines

1. Design and user research

Role and responsibilities *What hat does this person wear?*	This person will be in charge of doing research on existing interfaces and sketching “low-fidelity prototypes” based on the policies, which can be pen and paper or powerpoint. They will also be the person reaching out with individuals or communities to get feedback on prototypes.
Key questions *What questions might someone in this role be asking?*	• What are different ways we can sketch out the bill features we want to highlight? • What existing design patterns are available that people may be familiar with that we might want to use in our prototypes for inspiration? • Who should we interview and how do we try to enable more diversity of responses from potential constituents who would be impacted by these bill tenets? • What are an individual's expectations and needs with a system like we are proposing (based on interviews and conversations with them or from online feedback forums)? • What is confusing to them and how can we make the low-fidelity prototypes more intuitive?
Alternatives / stopgap *If you don’t have someone that neatly fits into this role, you can still bring this perspective to the table. What are some tips?*	The key is that this person is the lead on advocating for the end user’s needs and perspectives. They articulate the findings and transfer user needs into a low-fidelity prototype. This person might be a project manager, or a team member who regularly interfaces and coordinates communications with constituents (via phone, in person, etc.). They will be in charge of crafting the interview questions and brief the policy & product manager. As always, the teams can and should reach out to external design expertise as well for guidance if the option is available.

2. Technical

Role and responsibilities *What hat does this person wear?*	This person will be in charge of understanding technical components and providing feedback on prototypes. They highlight possible technical complexities and considerations with the interface. They provide feedback on how feasible an interface is to build and suggest alternatives.
Key questions *What questions might someone in this role be asking?*	• Generally, how feasible would the prototype be to implement and are there simple alternatives? • Is there existing evidence of possible side effects (e.g. security, poor mobile experience, data leakage) of putting this functionality into practice?
Alternatives / stopgap *If you don't have someone that neatly fits into this role, you can still bring this perspective to the table. What are some tips?*	This person can take the role of focusing on technical feasibility, possible alternatives, and tradeoffs of different solutions. Even experienced technologists encounter proposals that they have very little experience with. Leaning into the experiences of others (especially by honing in on the art of internet search queries) can unearth just enough insight to determine if the prototype is technically feasible. For example, searching Stack Overflow (a popular forum for technical questions and solutions) for "how to secure data packages" yields many results with links to external sources. This indicates that at the very least, solutions exist for this kind of work. Another popular resource is Github, which amongst other things, acts as a repository for software projects and enables developers to "star" these projects. Searching on Github for "photo gallery" results in thousands of projects, some with hundreds or thousands of stars. Like any field, experience matters and the jargon can be intimidating. Online sources, like Github and Stack Overflow, can be invaluable in demystifying software development. As always, the teams can and should reach out to external technical expertise as well for guidance if the option is available.

3. Product management, policy, strategy, operations

Role and responsibilities *What hat does this person wear?*	This person will be in charge of coordinating the overall process of policy prototyping, including staffing and resources. This role also focuses on formulating the strategy of the bill to prototype, managing deadlines, prioritizing goals and unblocking barriers throughout the process. Overall, this person will help ensure the insights are recycled back into the editing process and determine what the "minimum viable" is to proceed.
Key questions *What questions might someone in this role be asking?*	• What are the key questions we should focus on to test whether our bill tenets translate from policy to practice? • Based on our resources, how might we use our team to create prototypes and better understand potential technical feasibility? • How do we create a tight feedback loop between interview insights and iterating on our bills to improve comprehension and achieve the ideal impact? • What are our project success metrics, and how do we ensure we have done enough "prototyping" before we can share our policy?
Alternatives / stopgap *If you don't have someone that neatly fits into this role, you can still bring this perspective to the table. What are some tips?*	We understand there are many roles on the team, but there should be one "lead" of the team to wear the hat of project management and be accountable for driving the project forward and delivering prioritized proposed revision(s) to the bill.

Part D: Step-by-step framework

1. Coordinate team or assign roles based on existing team resources.

We recommend having design, technical, and policy/product management perspectives. We understand there may not be those exact roles on your team. So, if there is not a way to work with partners or resources in your organization or nearest neighbors (e.g. Congressional Research Service, TechCongress, etc.), then we have outlined the roles existing team members can play. See Part C: Role outlines. These guidelines are flexible based on your existing capacity. For example, if needed, team members can also assume multiple roles.

2. Select draft bill to prototype.

- If this hasn't been decided already, select a bill to prototype (or use the draft your team wrote) in order to test and get feedback.
- Establish bill goals. As a team, decide what you would like your minimum viable prototype to include. For example:
    - After reading the bill summary, the participant is able to understand key concepts of the text portion of the bill without major confusion. This may entail defining terms in parentheses, rewording to simplify language, etc. It is ok to provoke some questioning with unfamiliar features or words to get a sense of how someone may react to a new concept, but it is not a good sign for a user to not be able to comprehend the general context with a prototype.
    - While navigating the bill prototype, the participant is able to understand the general context of design elements without much assistance. If the person cannot roughly interpret what is happening without your narration it may be helpful to add more context clues or set the conversation by saying, "This is a profile page on a sample social media platform, can you explain what you see and what is happening? What stands out?"
    - While navigating the bill prototype, participants share feedback on various design elements, which can shed insights on how to improve the bill. Note: If a word is confusing or the design feature is completely indiscernible to a participant, you may want to consider re-sketching that part.
- Establish research questions. (e.g. exploring a concept like "duty of loyalty" in action, better understanding ways "data portability" can be effectively understood and used in platforms, etc.)
- Establish a timeline with team milestones. In order to scope bills goals and ensure they can be met, we recommend establishing a timeline for completing the following steps.

3. Prototype or edit draft bill text and mockups.

- Select 3-5 key features to prototype based on what you would like feedback on. This can be done through reading the full bill or looking at press releases to see what the bill aims to focus on (as framed for the general public).
- Sketch 2-3 prototypes based on the key tenets or features selected. Drawings can be intimidating and in the interest of getting feedback on functionality, low fidelity prototypes are, in fact, recommended. This can be done through pen and paper sketching or simple software that most people on your team (who need to be collaborating on this) have, such as Microsoft PowerPoint or even Microsoft Paint.
- Collect preliminary feedback and iterate on prototypes. The goal of the preliminary feedback is to ensure that the prototype is understandable and decipherable enough to get quick feedback on. This part will help you iron out key comprehension issues such as readability, misunderstanding features, etc. The team will do quick "interviews" to ask some preliminary questions to improve prototype sketches by building on constant feedback from people, generating new prototypes, combining ideas, etc.
- Select one "winner" prototype per bill.

4. Recruit participants.

- Map out the potential audience(s) that may be impacted by the bill. Note: qualitative research will not be "statistically representative" of the population. The value of this is to ensure you have diverse feedback from the group of people you speak with and to consider what questions or concerns people may have about the technology that you might not have thought of. These may include but are not limited to:
    - End users or individuals who may use the technology or service (to find various people, check out related forums, community groups and centers in the neighborhood, Facebook groups, organizations, or other affiliations that may know individuals)
    - Advocacy organizations who may have more insight on the topic
    - Industry practitioners or consultancies who might be building or designing the technology you may be focused on
    - Students, researchers or academics studying this specific issue
- Reach out to people for interviews.
    - Write an email script that your team can collectively use to standardize outreach. This should include things like:
        - Who you are, purpose of the project, what you're interviewing people for, how interviews will work, and potential date(s) and time(s).
    - Note: Use your team's strengths to reach out to networks, email lists, and communities you may be a part of or know about. This list may start out with people your team personally knows, cold-calls or emails. For each person you reach out to, ask if they have 1-2 people in mind you could reach out to follow up for another interview. This is a way to broaden your network and diversify interview participants.

- Schedule interviews based on the availability of the interviewee and your team. Consider the working schedules of those you are hoping to meet with. If location, time or limited resources is a barrier and you cannot meet in person, think of alternative ways of speaking with the candidate based on the resources they have.
    - In-person
    - Phone
    - Video chat
    - Email (This is not advised, but if there are any quick, well scoped questions you'd like to ask someone that is easier for them to respond to via email, consider this an option.)
- Space out the interviews. Have at least an hour to unpack interview insights and make sure you have enough time to prepare for the next interview, potentially tweaking questions to improve responses for the next one.
- Schedule an interviewer and a notetaker from your team to attend the interview (if possible). Ideally there is one person taking notes and one person focused on working through the interview protocol, modifying questions as needed, and probing the interviewee if there are interesting insights that appear throughout.
- Note: There is no "perfect" number of how many people to interview for this work. This is dependent on the resources of the team and whether your team has been able to capture insights, or if there are existing uncertainties that could be improved with more conversations with people.

5. Prepare materials & conduct interviews.

- Create and show a text summary of the bill. This can be done by reviewing the public press release of the bill that highlights specific aspects of the bill for a general audience. There also might be 1-pagers or summaries of the bill written by the Congressional team. If these do not exist, one way to create a quick sample of the bill is to show the table of contents. Teams can also write the summaries on their own.
- Create and show visual examples of some of the bill concepts. If there are bill concepts that may be foreign to people (e.g. infinite scroll), it might be helpful to show some relatable examples or aggregate definitions to the interviewee so they understand what the word might mean in context.

Create and show the "winner" design prototype(s). At this stage, it will be important to create a generic interface that might mimic experiences interviewees are aware of (e.g. Facebook or Twitter) but do not contain branding. This is to reduce the amount of bias toward a brand as much as possible but also to maintain some relevance to the interviewee so they understand the context of the feature and how it may work in practice (e.g. posting a photo, liking a comment, etc.).

- Create and follow an interview protocol. Here's an example structure you can follow:
    - Part 1: Introduction
        i. Explain project purposes, goals
        ii. Gain participant consent to collect information from the interview

    - Part 2: About + role
        i. What is your title/role
        ii. Introductory questions around the general topic
    - Part 3: Show bill text & prototypes, get feedback. What are the strengths, challenges of these privacy bills + prototypes?
        i. Show bill text. “Here is a bill proposal’s text highlights - let me know once you’ve finished skimming. Please speak aloud and narrate any thoughts, questions, or immediate reactions that come to mind.”
        ii. Show prototype. “Here is one way this bill might look in practice. As you are viewing this, please speak aloud and narrate what is happening. How does the interface and the features you see here work in practice?”
    - Part 4: Broader perceptions
        i. In this section, have the interview participant reflect on the bill(s) they’ve seen.
        ii. If you had a magic wand, what would you do to fix that issue?
        iii. What are you thinking about now that you weren’t thinking of? What resonates?
- Follow the interview protocol (roughly, as these are semi-structured interviews). Make any necessary adjustments to the interview protocol based on responses after each interview.
- Seek consent for taking notes during the interview, reminding candidates of the purpose of the research, who the interviewee notes will be shared with and the team’s policy on sharing any information outside of this conversation.

6. Synthesize learnings from the interviews.

- Review the interviews to identify perceived strengths and weaknesses in the bill. This requires going over notes to better understand key quotes, repeated patterns or bill text/design features that stand out to users (positively or negatively).
- Prioritize insights using methods like the KJ technique, MoSCoW Prioritization or Three Feature Buckets.
- Once priorities for bill and/or prototype changes have been addressed, loop back to one of the following:
    - If the team has decided to make changes to the bill text itself, go back to Step 3 to edit the bill text. Repeat until the team has reached their minimum viable bill prototype.
      --OR--
    - If the team has decided to make changes to the prototypes in order to improve comprehension and usability in the interviews, go back to Step 3 and repeat until the team has reached their minimum viable bill prototype.

7. Evaluate if bill goals are met.

- Review goals (or research questions) established in Step 2. As a team, assess updated bill prototypes and interview feedback against these goals.
- How do you know if you're done? We wish there was a clear formula for this, but the truth is that it depends on what resources you have available, from the capacity of team members to project timelines. We recommend outlining goals and timelines before beginning the prototyping process in order to establish a viable end point. Along the way, goals and timelines should be regularly reviewed and assessed by the team.
- If goals are satisfied, you have met your minimum viable bill prototype! We recommend sharing updated bill prototypes and feedback with other stakeholders and the general public (if applicable).