Encoding Privacy: Sociotechnical Dynamics of Data Protection Compliance Work

Rohan Grover
rohan.grover@usc.edu
University of Southern California
Los Angeles, California, USA

ABSTRACT

How do developers shape data protection regulations when they are passed from the policy arena to technical teams for compliance? This study explores data protection compliance work (DPCW) as a sociotechnical process mediated by developers' attitudes and experiences. We draw on 14 semi-structured interviews with individuals responsible for GDPR and/or CCPA compliance to examine how developers approach DPCW and the resulting implications for user privacy. We highlight three key ways in which developers can shape compliance: by creatively interpreting ambiguous regulatory requirements; by exploiting expectations of technical expertise and low accountability; and by reducing DPCW to a one-time project. We conclude by discussing the implications for both researchers and practitioners and by recommending how to conceptualize and conduct DPCW otherwise. This article adds specificity to understanding why and how developers' attitudes and experiences affect data protection regulations in the field.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in collaborative and social computing**; • **Security and privacy** → **Human and societal aspects of security and privacy**; • **Social and professional topics** → *Government technology policy*; • **Software and its engineering** → Software creation and management.

KEYWORDS

data protection, personal data, user privacy, compliance, developer studies, GDPR, CCPA

ACM Reference Format:
Rohan Grover. 2024. Encoding Privacy: Sociotechnical Dynamics of Data Protection Compliance Work. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3613904.3642872

1 INTRODUCTION

In September 2019, a team of developers for a user-facing mobile app with approximately 500,000 daily active users [1] worked with a product manager to implement new data protection and opt-out features to comply with the California Consumer Privacy Act (CCPA). Initially, they were excited to shape privacy safeguards for their users. However, there were many unresolved questions: What constitutes "selling" data? Should they roll these privacy features out to all users or only in California? How discoverable should they be? Should they audit opt-outs to confirm compliance or simply expect it to work? As they pored over the legal guidance from the privacy lawyers, they grew increasingly frustrated by shifting feedback, poor communication, and insufficient resources to instrument the features that they thought were necessary.

Soon, it became clear that the paramount objective for the company was to implement something—*anything*, really—within just a few weeks, before the law would take effect in early 2020, to show that the company made a good faith effort at compliance. Under pressure and frustrated by poor communication and corporate bureaucracy, the developers revised their scope, sacrificing features and usability to meet their deadline. What they launched looked very different from what they had planned just a few weeks earlier.

On one hand, this outcome is unsurprising since prior research has found that quality software development practices may be disregarded in the face of resource constraints or market pressures [13]. However, the stakes for data protection laws are unique because they are implemented via technical features launched by liable companies–and the stakes are growing given the acceleration of regulatory action in recent years. In particular, both the CCPA and the European Union's General Data Protection Regulation (GDPR), passed in 2016 and 2018, respectively, have played outsized roles in setting global standards for data privacy laws [5, 34]. These standards have developed because both states and liable companies have adopted GDPR's and CCPA's principles as *de facto* regulatory approaches to achieve harmonization [3, 32]. It is therefore important to understand how companies–and their workers–have responded to GDPR and CCPA through compliance practices that are likely to become increasingly standardized and globally widespread.

Thus, this study asks: How have developers shaped GDPR and CCPA when they were passed from the policy arena to technical teams for compliance? It pursues this question by building on previous research that approaches developer practices in general, and privacy work in particular, as a sociotechnical process informed by developers' attitudes and experiences. We focus specifically on this process as our empirical object and call it *data protection compliance work* (DPCW): the labor of translating data protection regulations from policy into code. As we demonstrate, encoding privacy laws is not a straightforward process of conversion, but rather a sociotechnically contingent system that brings together a broad network of actors whose relations are often mediated through developers.

[1] The app has been de-identified to avoid identifying interview participants. See Section 3.2

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642872

Following a review of related literature about privacy work in software development and a description of methods, we summarize themes and representative quotes from 14 interviews with software developers and adjacent workers that we collectively label *data technicians* (see Section 3). These findings are organized around four guiding questions: How do developers approach compliance work? How is compliance work situated within organizations? How do developers make decisions about compliance work? What do developers think about the lasting effects of GDPR and CCPA?

This article expands upon prior research by describing developers' unique capacity to shape data protection compliance in three ways: by creatively interpreting ambiguous regulatory requirements; by exploiting expectations of technical expertise and low accountability; and by reducing DPCW to a one-time project. At the same time, the developers interviewed conceived of their impact and responsibility as contingent, ambivalent, and dependent upon networks of external actors. This discrepancy demonstrates the significance of these findings, which highlight the central role that developers play as mediators whose attitudes and experiences carry implications for data protection regulations in the field. More broadly, these findings demonstrate the importance of studying data protection compliance work (DPCW) as a sociotechnical phenomenon, which includes unpacking expectations of developer expertise and boundary work across fields, and imagining alternative promises for data protection and digital privacy.

2 STUDYING PRIVACY IN SOFTWARE DEVELOPMENT

2.1 Developers as Key Actors

This study builds on previous research that has investigated how developers approach privacy. This literature begins with the premise that privacy values can be embedded in technical design and development, a framework called Privacy by Design [4]. Many researchers have been inspired by this framework to explore the decisions developers make when designing and developing software, especially when implementing privacy features.

One challenge with Privacy by Design is "translating the general abstract notion and the meaning of informational privacy (or, in its European term, data protection) into concrete guidelines" [22]. This has opened up a line of research about how developers approach privacy work in software development because they are delegated responsibility to interpret and design privacy frameworks [22, 43]. In particular, Greene and Shilton [16] argued that Privacy by Design "positions developers and mobile companies as ethical agents" and then, accordingly, "platforms emerge as *de facto* regulators" (p. 1643). This effectively promotes platforms as well, such as iOS and Android, as not only sites of privacy mediation but also as privacy co-regulators themselves, especially because iOS and Android developers maintain different conceptualizations of privacy [16, 35, 47].

Given developers' role as ethical agents, several studies have explored how developers conceptualize and approach their relationship to privacy work. For example, Tahaei et al. [41] found that both computer science students and professional developers share similar attitudes toward privacy and security, including "hacker and attack mindsets", inexperience with security instrumentation, and a tendency to trust other developers' solutions while applying minimal scrutiny. In response, many developers turn to online forums for advice on approaching privacy work, which means that online forums serve as important spaces where developers deliberate ethics and values [35]. However, these spaces and the discourse and actions they cultivate are not neutral. For example, Tahaei et al. [47] analyzed privacy-related questions on Stack Overflow using both topic modeling and qualitative analysis and found that developers seeking answers to questions about privacy derived their answers from platforms (i.e., iOS and Android) or individual opinions from other individuals regardless of their expertise. In another study, Tahaei et al. [42] found that responses to questions on online forums can be biased toward particular privacy paradigms. Thus, developers are key actors in digital privacy not only through their software development practices but also by developing and sharing best practices beyond their teams and organizations.

2.2 Social and Institutional Factors

Collectively, these studies indicate that developers are often generally uncertain about how to tackle challenging privacy questions, and that they often rely on social networks and discourse to define privacy priorities and standards. But sometimes there are exceptional developers who are committed to privacy and offer to lead team decisions and culture. Tahaei et al. [40] characterized such individuals as *privacy champions*—defined as those who strongly care about advocating for privacy on their teams—and found that they play important roles in cultivating a team culture that prioritizes privacy in software development. They further found that privacy champions attempt to overcome prioritization conflicts, organizational ambiguity, and limited support through team-building practices such as informal discussions, promoting stakeholder communication, and developing documentation.

On the other hand, many developers' privacy decisions are also subject to influence from institutional sources. For example, developers tend to retain the default privacy settings on third-party services such as advertising networks [27]; meanwhile, platforms claim that developers are responsible for their own regulatory compliance—even though their configuration interfaces contain dark patterns that nudge developers toward "privacy-unfriendly defaults" [44]. However, developers are often not aware of the data collected by third-party tools due to a lack of resources, expertise, and time [2]. These findings are consequential for how and when developers think about privacy. For example, Li et al. [24] found that although developers often claim to care about privacy, they may carry a limited understanding of their own products' data collection practices, partly because of poor documentation. Instead, developers may be more likely to discuss privacy concerns in response to changing policies from platforms, app stores, or regulators rather than to develop new privacy features in their own products [24]. This may be because developers see a clear separation between their own code and third-party services, who they consider responsible for their own privacy practices [27], or because developers feel that additional privacy work is likely to incur more costs than benefits [25].

2.3 Implications for Data Protection Regulation Compliance

Understanding how developers approach privacy work is important because their decisions can carry material consequences for user privacy, especially when implementing GDPR and CCPA. Feng et al. [12] found that data protection features that meet the baseline standard for compliance often do not help users make informed decisions, and thus argued that compliance work should be enhanced by providing users with "meaningful privacy choices" that meet a higher standard of usability. Indeed, several studies have found that the types of privacy choices mandated by these regulations are placed in different locations on websites, some of which are difficult to find or use [19, 20], and that both visual and UX design choices–such as link text, colors, iconography, and choices between banners and overlays–can affect user comprehension of and decisions about privacy choices [8, 18, 28, 29, 33]. Such studies have even led to regulatory changes and standards [7, 21]. These criticisms also apply to data subject access requests, which allow users to access, modify, and delete their personal data collected by liable organizations. For example, Di Martino et al. [10] conducted audits that exposed that many large websites leaked personal information to unauthorized third parties after only minimal social engineering. Although developers are not always responsible for fulfilling requests, they are often implicated in setting up workflows to verify and execute them.

Overall, while previous studies have explored how developers make privacy decisions in general, and how their technical and design decisions shape user outcomes in particular, they have not defined the specific responsibilities assigned to developers to comply with data protection regulations or how they are situated within their organizational contexts. These dynamics are important because they shape users' experiences of privacy online—in essence, to what extent the regulations fulfill their intended goals—which is increasingly important as new data protection regulations have been passed or introduced around the world. This study addresses that gap by evaluating how communicative and team-based processes identified in the literature interact with GDPR and CCPA—and the implications of developers' decisions on what privacy regulations actually look like in practice.

3 METHODS

This study focuses primarily on developers because the literature has already demonstrated that they play a key role mediating between many stakeholders: they operationalize regulators' statutes, remain accountable to privacy lawyers, learn from and negotiate with platforms, and produce features for end-users [16]. However, this study also explores developers' experiences with data protection regulation compliance work (DPCW) as collaborative processes with diverse organizational actors, including lawyers, executives, and other technical workers. Thus, it departs from previous research, which has either focused on developers alone (and excluded adjacent functional areas) or the outputs of their work (i.e., code, features, and frameworks), by including workers from data, product, design, and operations teams.

We call this broader category of workers *data technicians*, or workers who operationalize the key processes of data collection, administration, management, design, and analysis. Software developers are key data technicians, but they also collaborate or work alongside data analysts, designers, product managers, operations specialists, and others. Thus, data technicians are collectively responsible for managing the mediating data infrastructure between organizations (e.g., "data controllers" and "processors" as defined by GDPR) and individuals (e.g., "data subjects" or "consumers" as defined by GDPR and CCPA, respectively). This expansive approach to interviewing data technicians beyond developers alone was chosen in order to account for the diverse contributions of different workers besides software developers. For example, in the course of complying with data privacy laws, data scientists recommend collecting or storing personal data with particular structures and attributes, and designers create particular iconography or design patterns to present to users. We included these roles in order to better understand how they contribute to DPCW alongside and in relation to software developers, who are often the only focus. However, in our study, participants largely described their compliance work in relation to decisions and processes led by software developers, so our findings below focus primarily on developers' attitudes and practices—but are enhanced by perspectives from the broader category of data technicians.

3.1 Recruitment

This study was conducted through semi-structured interviews with 14 data technicians who have been responsible for GDPR and/or CCPA implementation in a variety of organizational contexts. The key inclusion criterion was that participants should self-identify as having experience bearing some responsibility for an organization's compliance with GDPR or CCPA.

Participants were recruited using purposive sampling by drawing from personal and professional networks. *Purposive sampling* is a non-probability sampling technique that is most useful when researchers aim to account for specific perspectives without needing to generalize to an entire population [11]. It is appropriate in cases where the research question requires calls for specific perspectives or experiences that may not be adequately captured in probability samples. We adopted a purposive strategy in this study to account for recruitment challenges documented by previous research [45], which has led many qualitative studies about developers' privacy attitudes and practices to be based on small samples of 10–20 interviews [1, 22, 38–41, 46].

Individuals were recruited based on diverse organizational experiences, including tech giants, startups, and non-profit organizations, and in different geographic regions. This allowed us to follow a maximum variation purposive sampling strategy to discern common themes and differences across experiences [11]. We posted calls for participation on LinkedIn and Facebook, which yielded three interviews, and reached out directly to 26 individuals, which yielded 11 additional interviews. We continued reaching out to individuals approximately every two weeks until saturation was reached. Saturation, or information redundancy, is a common measure to demonstrate rigor in qualitative research, but it is often undefined [17]. In this study, we operationalized a version of saturation called *code saturation*, or the point when no new codes (which

we call *themes* to avoid confusion with computer code) emerge from additional data collection [23].

We faced the additional challenge of recruiting individuals with direct experience with DPCW, which is both uncommon and difficult to identify from the outside. In many organizations, compliance instrumentation may be a discrete project—or even a series of tasks within a sprint—rather than a full job description. Therefore, asking a potential participant if they have worked on privacy regulation compliance was open to interpretation and subject to recall from their project history from two (for CCPA) or four years (for GDPR) prior at the time of data collection. Even if a participant was eligible for the study, we found that they were sometimes reluctant to discuss sensitive privacy regulation compliance issues on the record. Participants voiced this concern for two reasons: privacy regulations are considered sensitive topics given individuals' inability to speak for an entire company while potential complaints carry high fines, and because of the context of high-profile, expensive leaks from Facebook and ongoing controversies related to companies such as Twitter and Amazon. Therefore, other potential participants may have harbored fears of retribution or may have been bound by nondisclosure agreements in an industry marked by considerable asymmetry between workers and owners.

3.2 Ethics

This study's recruitment and interview procedure was approved by the University of Southern California's Institutional Review Board as study UP-21-01100. As part of the approved process, participants were provided with a PDF copy of the approved informed consent form before the interview began. Verbal consent was requested before proceeding with the interview and, if the participant agreed, with recording the audio and/or video.

Participants were offered the option for their responses to remain de-identified to avoid scrutiny of their work or negative implications for their current or prior employers and clients. Eleven out of 14 interviewees requested for their responses to remain de-identified. We therefore decided to de-identify all examples and quotes to treat all participants equally. Individual companies and countries are not identified, precise job titles are not disclosed, and the gender-neutral "they" is used for all participants throughout this article. Additionally, since several participants asked to remain anonymous, the quotes we use to illustrate our points primarily come from a subset of participants. However, the experiences illustrated by the quotes were applicable to many participants, which we describe throughout the article.

Participants were notified in advance that they would be offered a digital gift card worth USD 25 (or the equivalent in their local currency) regardless of their willingness or ability to answer every question. Several participants declined the gift card, most often because of restrictions imposed by their employer; in one case, a participant asked for their payment to be donated to a privacy-oriented advocacy organization.

3.3 Interviews

The 14 interviews were scheduled for 60 minutes but lasted between 30 and 90 minutes. They were conducted between October 2021 and August 2022 on Zoom, except for one interview that was conducted in-person at the participant's request. Participant demographics are summarized in Table 1. In terms of geographic distribution, 9 participants primarily work in North America; 2 in Oceania; 2 in South Asia; and 1 in Europe. We aggregated by region to respect participants' confidentiality preferences and to minimize the risk that any individual participant can be identified. The over-representation of developers and of North America-based participants reflects two factors: our professional network and experiences and participants' experiences being responsible for GDPR/CCPA compliance.

Table 1: Interview Participants

Alias	Duration	Company Size	Functional Area
P01	26	Small (<100)	Engineering
P02	52	Small (<100)	Engineering
P03	54	Small (<100)	Engineering
P04	56	Small (<100)	Engineering
P05	35	Small (<100)	Design
P06	66	Medium (100–500)	Engineering
P07	69	Medium (100–500)	Operations
P08	48	Medium (100–500)	Engineering
P09	68	Large (500–10,000)	Engineering
P10	41	Large (500–10,000)	Operations
P11	44	Large (500–10,000)	Data
P12	32	Tech Giant (10,000+)	Engineering
P13	35	Tech Giant (10,000+)	Product
P14	62	Tech Giant (10,000+)	Data

Eleven of the 14 interviews were recorded and transcribed, yielding approximately 75,000 words of transcripts. The other three interviews were not recorded or transcribed as requested by the participants. Instead, we took non-identifiable notes during the interviews. The transcripts and notes were analyzed using iterative open coding to identify common themes, exceptional experiences, and representative quotes.

3.4 Interview Guide

Interviews were semi-structured in order to explore participants' experiences and perspectives in depth. This was important because this study is not simply interested in answering questions about *what* developers do, but also about *why* compliance work is experienced in a particular way and *how* they handle ambiguity and uncertainty. Thus, we drew from an interview guide and then probed further based on each participant's experience, recall, and interest.

We developed the interview guide (see Appendix A) based on exploratory research questions. We began by asking participants about their familiarity with GDPR and/or CCPA and to recall a specific organizational and temporal context in which they were responsible for data protection compliance. This helped to validate that participants met our inclusion criteria and helped participants locate specific experiences. Next, we asked questions about how DPCW was distributed and implemented. To do this, we asked how responsibility was determined and negotiated across functional teams, about risk and uncertainty, and about tools, systems, and preparation. We repeated these questions for participants who were

responsible for data protection compliance in multiple organizations (N = 2) or who recalled specific experiences with both GDPR and CCPA in the same organization (N = 3).

After that, we asked participants to reflect on their experience(s) with DPCW. We asked about how their background informed their approach, about expectations about their expertise, and about the extent to which their company's compliance work would be surprising to different actors. Finally, we asked participants to reflect on their own relationship with data protection and digital privacy. This yielded several interesting insights and, in some cases, led to new or more precise reflections about DPCW.

3.5 Analysis

The interviews were analyzed using a constructivist grounded theory approach in which data and theory are co-constructed by the researcher and participants. Grounded theory, in its original formulation by Glaser and Strauss [15], followed a positivist orientation to systematic and objective analysis, requiring the researcher to let meaning emanate from empirical data through iterative procedural rigor and with minimal interpretation or prior literature. Instead, a constructivist approach, as advocated by Charmaz [6], embraces empirical rigor while also acknowledging how analysis is inherently interpretive; thus, she calls for bringing in the subjectivity of the researcher and situating analysis in prior literature. We embraced a constructivist approach because we understand our analytic object—DPCW—as a sociotechnical process that cannot be understood without acknowledging and interpreting social context. Thus, we followed Charmaz in conducting and transcribing interviews, iteratively coding themes using prior literature to correlate excerpts with concepts such as privacy champions, expertise, and uncertainty, and updating an analytic memo throughout the data collection process, which extended over the course of 11 months. The themes can be found in Appendix B.

4 FINDINGS

This section summarizes the findings from the 14 interviews oriented around four questions: First, how do developers approach GDPR/CCPA compliance work? Second, how were developers' responsibilities situated within their organizational contexts? Third, what decisions did they make while doing compliance work? Fourth, what are the lasting effects and attitudes about data protection regulations today?

4.1 How Did Developers Approach Compliance Work?

These questions were oriented toward discerning participants' attitudes toward data protection regulations and understanding of the scope of work.

4.1.1 Feeling Unprepared to Address Vague Regulations. Participants often expressed hesitation when describing the scope of GDPR and CCPA in detail. This was even true of several participants who were individually responsible for overseeing compliance work for a particular product or application. For example, P09, working at a large technology company, described GDPR compliance work in 2018 as such:

> *We were in a mad dash to ultimately be able to say we're in compliance. That was, and is in all my experiences, the principal concern—being able to say we are compliant. I don't know that anybody I've encountered—and certainly not I—has a concrete grasp of exactly what that means.* (P09)

P06, who was solely responsible for GDPR compliance at a small company, provided a blunter response to a question about how prepared they felt to tackle GDPR: *"Zero. I felt unprepared"* (P06).

These two examples are representative of the experiences described by participants across different organizational contexts, which are also captured by the metaphors participants used to describe their experiences. For example, P06 compared data protection compliance work to fulfilling accessibility requirements but (DPCW) with *"less clear guidelines"* in which *"a lot of people and a lot of companies don't want to implement them to the point they are recommended, or at all, until it becomes a legal issue"*. Similarly, P08 described DPCW as being *"in the same bucket"* as the US Health Insurance Portability and Accountability Act (HIPAA), but *"less serious"*. The perception that data protection regulations are *"less serious"* than HIPAA was apparent in how participants reconciled their approaches to achieving compliance. Several participants used expressions such as *"the spirit of GDPR/CCPA"* to describe their aspirational level of compliance rather than trying to satisfy every component of the regulations.

4.1.2 Compliance Work as Risk Assessment Labor. The two exceptions among the participants—in that they felt well prepared for regulatory compliance work—were both working in operations roles supporting compliance efforts at very large technology companies. P07 *"fell in"* to privacy work after being pulled into a project to respond to a data breach, which provided the necessary experience to become familiar with the technical and legal nuances of compliance work: *"The best preparation happens on the job. I didn't plan to work in privacy. The breach happened, and then I got into it"*. In addition, P10 described how they drew upon their background working in content moderation to make decisions about verifying and fulfilling data subject access requests:

> *In the end, it's all about risk assessment. Is giving this person their data, or removing an account, based on the information they've given us more likely to result in the most correct outcome? Or is it more likely to result in some random person getting someone's data? It's the same as trying to trust someone to accept the rules of whatever platform they're on and not harass someone in the future. You're just basically just assessing what you have in front of you.* (P10)

In both cases, the participant identified prior experience with different types of risk assessment and management as a source of confidence in approaching DPCW. This contrasts with developers' feelings of unpreparedness and reluctance, which suggests that expertise in DPCW should perhaps be less defined by specific technical capabilities or proximity to data systems than by experience with managing risk.

4.2 How is Compliance Work Situated Within Organizations?

4.2.1 High Autonomy. Participants on developer teams described high levels of autonomy with minimal oversight over their work. In several instances, developers were the first to bring GDPR or CCPA compliance requirements to the attention of their organization's leadership. P12 recalled how their autonomy came from a combination of pressure from executive leadership and lack of product strategy:

> *We had a lot of autonomy in general, and in particular with GDPR and CCPA. So this was a particular thing that engineering took upon itself to try and handle. We were responding to middle manager engineering pressure. The underlying mechanics were fairly technical in nature… So it was a hodgepodge between direction that we were getting from senior engineering leadership in the organization, and our own judgment and instincts about what the intention of the laws were.* (P12)

This description is similar to the experiences articulated by other developers, including those in smaller organizations who received pressure from executive leadership instead of middle manager developers. In general, they described being saddled with-or perhaps entrusted with-conducting DPCW because of their technical expertise, even if they did not feel equipped to do so. For example, P06 described their experience instrumenting GDPR compliance as a contractor working for a large multinational company. They described how they were saddled with the responsibility of ensuring that the organization was prepared for the beginning of the enforcement period:

> *We were not really given clarity on what compliance was. We had a [marketing director]—she mostly just passed it off to [us] and had us kind of just figure it out… It involved Googling and seeing how to be compliant and using online resources and not necessarily getting legal interpretations of how to do it.* (P06)

Since P06 was one of two contractors who each worked on separate projects for the same client, their work was not code reviewed by another developer, nor was their work fully tested for quality assurance. Instead, they were independently responsible for both executing and checking their own work—all while acting as a contractor rather than a full-time employee. P06 ultimately ended their contract before the GDPR compliance work was complete, passing it back to the marketing director who hopefully found another contractor to pick up the remaining work.

Similarly, P04 described a state of confusion among developers who were left to determine their own standards for quality. They were consulting for about a dozen small to medium companies in different countries in 2017-18 as GDPR entered its enforcement period. They described how developers in different client organizations needed to solicit privacy lawyers for advice, and how they made solicitation decisions in part based on lawyers' different risk tolerances with little or no input from other organizational leaders since GDPR compliance was deemed a technical issue.

4.2.2 Lack of Oversight. A related theme was a lack of oversight over developers' work. This was related to high autonomy, as described in Section 4.2.1, but applies specifically to the extent to which developers' work was held accountable to actors in another functional area, such as a legal department. For example, P09 described how *"it was ultimately up to us, the implementing team, to look at what was in the application, document all the [third-party services], and identify which ones were potentially at risk [for collecting personal data]"*. In addition, they recounted how the process of determining which categories of data collection were permissible without user consent according to the organization's "legitimate interests" (under the GDPR) were not verified by executives, compliance officers, or lawyers:

> *One of the main things that I remember is a statement that basically 'information that you collect that applies directly to the operation and function of your application isn't really subject to the same restrictions... We creatively applied that in a few places where it was like, okay, I think this is operational data. You could probably argue it in a different direction, but we don't have an easy workaround here, and we don't think it's a flagrant violation. So we're going to go with it. We're just going to say this is operationally relevant data that we're collecting, it's not being used for tracking or profiling. We're just going to ignore it.* (P09)

In sum, *"we could have easily flaunted it entirely and nobody would have known; nobody was in a position to question us"* (P09). This lack of oversight was corroborated by P01, P05, P07, and P13, working in different functional areas such as design and product. Each of them described providing suggestions or minimum requirements to developers, but then allowing developers to lead in developing a compliance strategy, even if it was *"patched together and disorganized"* on the back end (P01). P07 even described one instance where they were accosted by a developer: *"There was a person who screamed at me. They were like, why are you wasting my time? I said I'm not wasting your time, I'm just telling you what you need to do"* (P07). Ultimately, P07–a non-developer working in an operational role–did not have the authority to block the developer from launching their non-compliant feature. This example, while irregular, illustrates how developers' high autonomy can be upheld through institutional immunity from oversight by other functional teams.

4.2.3 Tenuous Relationships with Lawyers. Developers' high levels of autonomy and minimal oversight extended to their relationships with lawyers. In some cases, this was attributed to developers' reluctance. For example, P09, working at a large technology conglomerate, described how their team was hesitant to consult lawyers to reconcile questions about whether a particular third-party service was compliant:

> *Nobody up or down the chain knew exactly what the answers were. But there was generally a hesitation to take things to lawyers just because it usually ended up being more work. We would often get the outcome that we might have suspected but would prefer to avoid it in terms of the effort required or the implication.* (P09)

In other cases, this tenuous relationship was attributed to lawyers' reluctance to prescribe specific instructions. For example, P08, working in a large company, had access to a lawyer and a full-time compliance officer to support GDPR and CCPA compliance, but they appeared to be more interested in upholding the *"spirit of the law"* in general simply to avoid a large penalty:

> *It's like, "just make a good faith effort and that's good enough." That's kind of our legal take on it… There's a lot of gray area on what is the right thing to do. But I think the lawyer probably wrote one paragraph about it and then stopped caring about it. Because there's very little chance we're going to get sued or anything, and that's what the lawyer cares about.* (P08)

In several other cases, participants described how legal expertise was unavailable to them, either by design or because of lack of capacity. For example, P06 described their experience working with a small organization that was reluctant to consult any lawyers throughout the process:

> *The struggle was that nobody wanted to talk to a lawyer to give us any understanding of the things we should do… It was something that, uh, felt like it was actively being avoided… So I don't know how close to compliance we were because I'm not a privacy expert and that was never what I was hired for.* (P06)

Collectively, these examples demonstrate how developers' autonomy was upheld by constructing boundaries between technical and legal decisions and expertise, although these boundaries were constructed and negotiated differently across organizational contexts, especially by developing socially and institutionally contingent distinctions.

4.3 How Did Developers Make Decisions About Compliance Work?

4.3.1 "Just a One-Time Thing". The specific regulatory features that participants focused on included implementing cookie consent notices, adding disclosures and configuration options to forms, updating privacy policies, purging data, investigating and reconfiguring third-party integrations, and updating data infrastructure. However, one of the most common themes across all interviews was that participants described a lack of auditing or follow-up to ensure high quality compliance. This was an issue for several participants because they described facing major bugs while instrumenting initial compliance. For example, P14 described how EU visitor traffic doubled immediately after deploying a page redirect for GDPR because new cookies were being created for existing users. However, the issue was not caught immediately because a separate bug affecting a third-party analytics service was introduced at the same time, effectively masking the bug that inflated their traffic metrics.

P08 also described a bug with cookie opt-outs during CCPA implementation that was caused by testing for one case (users opting *out* of personal data collection) but not for another (users opting *in*):

> *Our original code for [our third-party tracking service] wrapper was successfully turning off the cookies for people who didn't want them, but also had a bug where it was successfully turning them off for everyone else, too. We went like a week without collecting data before anyone noticed this. What happened was somebody wrote the code, somebody else ran it and opted out, and then looked at [the third-party tracking service] and confirmed that the correct data was there. That was our testing process. If that stopped working now, it would probably be months before we noticed it. We don't have any sort of regular audit.* (P08)

P08 was describing an experience at a medium-sized tech company with more than 250 staff, one-fifth of whom are developers or in similar technical roles. Further, the company also handles sensitive health data protected by the Health Insurance Portability and Accountability Act in the United States.

When asked about the current status of GDPR and CCPA compliance, participants universally admitted that they had not reviewed or audited their implementation work, including confirming that third-party cookies were caught behind a wrapper, confirming that the appropriate disclosures and configurations were available on forms, and so forth. Two participants (P06, P08) suggested that their privacy lawyers likely would not agree to a proactive compliance audit because it was not mandated; thus, in their minds, they could remain ignorant to potential bugs or violations while staying true to *"the spirit of the law"*.

The mindset that regulatory compliance work was *"just a one-time thing"* also applied to handling data subject access requests at small and medium-sized organizations. While some participants used self-service solutions such as privacy dashboards to enable users to request or delete their personal data, other participants set up manual processes that they planned to automate in the future in order to handle higher volumes of requests. However, none of those participants had streamlined those workflows when the interviews took place 2–4 years later. Both P02 and P09 attributed this to the low volume of requests:

> *We wrote a "hacky" script that an admin runs with the intention that, if we get a lot of these requests, we'll make this a self-service tool so that we don't have to spend a lot of time doing this and so that it's easier for customers. But I think we've only had three people ever ask for their data. And I want to say maybe once a month somebody asks for their data to be deleted.* (P09)

4.3.2 Limited Sense of Responsibility. In addition to expressing reservations about the status of their compliance instrumentation, several participants expressed how they inevitably relied on several third-party services to maintain their compliance mechanisms. For example, P09 described their GDPR and CCPA compliance work in a mobile app as *"flipping a series of switches"* without any visibility into what actually happens to user data stored on other companies' servers:

> *I'm responsible for making sure the switch is there, and that it calls the service somewhere when the user taps it. Beyond that, I have no idea what happens… Everybody on my team and my peers and colleagues, we are doing what we believe needs to be done, by law, by intention,*

> *by principle, but without actually concrete assurance.* (P09)

This reflection captures a sense of ambivalence expressed by several developers. In contrast with the expectations of expertise and responsibility, described in Section 4.2.1, which led to developers enjoying relatively high autonomy in conducting DPCW, many developers saw themselves as reliant on networks of actors that may be invisible to their colleagues and broader organizations.

4.4 What Do Developers Think About the Lasting Effects of GDPR and CCPA?

4.4.1 Strategic Value of Regulatory Ambiguity. Several participants described how they have been able to advance personal priorities under the ambit of data protection compliance work (DPCW). For example, P03, a senior developer with a background in the free software movement, noted that they found strategic value in drawing on GDPR to advance an anti-corporate ethos. They described how GDPR provided cover for decisions to, for example, reduce dependence on *"Big Tech"* companies such as Meta, Google, and Amazon.

> *I would never be okay with uploading emails to Facebook to create targeted lists, because I imagine that Facebook is holding the data… We didn't really use Google Analytics for the same purpose. You put their tracker on your website and you're inviting the giants to your website and to all your users… These things influenced my decisions [about privacy]. For instance, I would prioritize not giving data to huge corporations. But I wouldn't—and I didn't—prioritize creating an automatic way for people to access their data [under GDPR]. I would say, they can email us and ask to deliver their data, or change it, or delete it, and that's fine.* (P03)

In this example, the developer made decisions about their organization's technical systems, such as avoiding integrations from the largest tech companies, under the ambit of advancing privacy—even though those services were not actually disallowed by the GDPR. Instead, they described strategically interpreting the *"spirit of the law"* to advance their own privacy framework, especially their own interpretation of data minimization. Later in the interview, P03 acknowledged that their values were not shared by their company, and that once they left for another job, the organization returned to using services by Meta and Google again.

While this may seem like an extreme example, P09 described a similar appreciation for the regulations providing cover for advancing privacy as a human right:

> *[GDPR and CCPA] are not the best thing for our business, but it is important to our values to try and deliver it to users to whom it matters and for whom it's important, because privacy as a value and a principle does matter to us as a group. It's not great for the advertising business so we would prefer that users did not elect to opt out. But we do think it's the right thing to do to (A) be compliant because it's the law, and (B) because privacy is a fundamental right. So we are, in some ways, grateful that the mechanisms exist for us to be able to do that.* (P09)

To P09, advancing privacy is an important goal that is fundamentally incompatible with their business's corporate strategy, which is premised on an advertising model. Therefore, the mandates of complying with GDPR and CCPA offer permission for the developer team to exceed regulatory requirements and advance data privacy goals that may have been unfavorable for their employer's profitability.

4.4.2 "Regulations Do the Bare Minimum". Participants responded to questions about the value of GDPR and CCPA with great skepticism. In general, they were not very hopeful about advancing a broader conceptualization of privacy through data protection regulations that were neither standardized nor enforced. P01 captured this sentiment, which was shared by several participants, by describing how they realized from serving as a technical executive that *"companies will do the absolute bare minimum in terms of privacy"*. However, several participants noted the value of compliance work instigating important discussions and processes within their teams. For example, P08 highlighted how the regulations have promoted discussion and allowed developers on their team to signal their values to each other:

> *I have kind of mixed feelings about [how important the regulations are]. I think it's important that they drive conversations at companies. I appreciate hearing someone say, "let's do more than we're legally required to do for our users". I would also appreciate hearing somebody say the opposite of that because then I would think—this isn't a company I want to work at. So I think that's probably the main benefit I see of it. I don't think the regulations do much to improve user data privacy. But I think they start conversations that wouldn't happen if the regulations weren't in place.* (P08)

Similarly, P09 appreciated that data protection regulations allow them to challenge their employer's business model:

> *I think privacy is really important… In my work, I have tried to advance what I think is the spirit of the regulations in an environment even though it's sort of against the interests of the business that I'm working for. There's a conflict there.… But I've tried to do what I think the intention [of the regulations] was for our users, knowing that it's not enough. It's far from it. The regulations are ambiguous on the surface, and they're ambiguously implemented, although they're well intentioned. I don't know what the net benefit is, if any.*

5 DISCUSSION

This study has examined the empirical object of data protection compliance work (DPCW), scrutinizing neither the text of data protection regulations themselves nor their outcomes but rather the sociotechnical process of achieving compliance. This approach is valuable for shifting focus from technology policy analysis or social analysis alone to instead understanding how the social and technical are mutually constructed. Thus, a number of important

analytic themes have emerged that highlight key contributions to the subfield of *developer studies* and also topics for future research.

5.1 A Unique Responsibility to Define the "Spirit of the Law"

Developers can creatively interpret specific clauses of data protection regulations. As previously discussed, developers made substantive decisions about interpreting various parameters in strategic or instrumental ways, such as adopting a flexible understanding of data collection that is exempt from data protection regulations; shifting the boundaries of their responsibilities when assessing third-party software; and advancing additional goals through compliance work. A handful of phrases recurred across the interviews to justify or frame these decisions, including a broad commitment to *"the spirit of the law"*.

But what, exactly, is *"the spirit of the law"*? This, too, was left open to individual interpretation. This uncertainty suggests that *privacy* operates as a boundary object—a concept whose ambiguous definition enables cross-functional actors to collaborate without actually agreeing upon a single definition [37]. This ambiguity enables developers to define compliance work not only in terms of implementation decisions about specific technical features but also a more general sense of the scope of work. For example, the experiences of developers strategically interpreting the scope of GDPR and CCPA to advance goals outside the explicit scope of the regulations adds to Tahaei et al.'s [40] findings a new way that privacy champions influence their teams, and further suggests that privacy champions can bear outsize influence beyond developer teams by shaping organizational strategy, especially in smaller organizations, by, for example, defining *"the spirit of the law"*.

This opportunity is unique to developers. We discovered this in this study by, at first, recruiting participants from a variety of functional areas—developers, data managers, product managers, and designers—who, on paper, seemed to have key roles in DPCW. However, our interviews confirmed that developers are the most important category at the center of DPCW since they hold key responsibilities and expertise-even compared to legal teams. In our study, this was manifested in lofty yet often unsubstantiated *expectations of developer expertise*. Participants described how colleagues from legal departments and other functional areas delegated the *"technical"* work of compliance to developers. Our focus on this *"technical work"*—which we call DPCW—has demonstrated that it is not straightforward or clear. Instead, developers navigate a range of sociotechnical and institutional factors with material-and thus political-implications. One exemplary implication is that developers often do not meet the expectations imposed upon them about their ability to simply translate policy into code, to see into technical systems, and to sustain a state of compliance over time.

These findings extend and raise the stakes for prior research on how developers approach privacy work. Such studies have often focused on understanding developers' attitudes toward [22, 41] and discourse about [16, 25, 35, 42, 47] privacy. However, this article has demonstrated that it is also crucial to explore the sociology of expectations. For example, future studies could explore how expectations of technical expertise over data systems and privacy develop and proliferate, how widely they are held and by which actors, and how developers respond to and negotiate such expectations. This would shift the focus of research that "audits" data protection regulations [8, 10, 19, 20] from applying a binary rubric of compliance to instead unpacking sociotechnical processes as an organizational genre [49] enacted by multiple functional teams that collectively uphold the fiction that compliance is a straightforward and feasible endeavor. Thus, this article calls for new questions about how DPCW has evolved and become standardized through contestations over professional boundaries related to skills and expertise [14, 37]. There is substantial literature on objectivity, quantification and technocratic expertise in governments and institutional contexts [31], but data governance is often characterized as a values-centric project of advancing an ethic of privacy. How has DPCW come to constitute a kind of boundary work that privileges developers' presumed skills and experiences? And how does it manifest in different institutional and cultural contexts?

5.2 Developers as Street-Level Bureaucrats

At the same time, developers face remarkably little accountability in DPCW while wielding outsized influence on policy. While previous research has measured the influence of the "human factor" in software development in general, and privacy work in particular, this study adds a comparative dimension by interviewing data technicians in non-developer roles, including design, data, and compliance. Participants' experiences suggest that adjacent functional workers such as product managers and executives are capable of influencing these decisions, but that developers are nonetheless often uniquely autonomous.

This autonomy is evident in two types of decisions. First, developers enjoy autonomy by creatively defining the scope of their work, as previously discussed. Second, developers sustain limited accountability by deciding when their decisions should receive external input—and from whom. This was evident in the anecdotes about deciding when it was appropriate to put additional effort into reaching out to third-party companies and when to consult lawyers whose responses might increase their workload.

This finding brings prior literature on developers' privacy attitudes and behaviors in conversation with policy implementation. Specifically, it highlights how developers can and should be understood not only as technical workers within companies but also as "street-level bureaucrats" of public policy [26]. This complements internet governance research that has demonstrated how technology companies act as "central points of control" [9], especially through institutional forces [48], by highlighting the specific and unique role that developers play in shaping policy. While this study was focused on data protection regulations, developers may also play a substantial role in implementing, and thus shaping, other internet governance regulations, especially related to artificial intelligence (AI) governance and regulation. Thus, this study elevates the implications of studying software development practices in the context of privacy and policy implementation, as reviewed in Section 2.

This bears relevance for both practitioners and policymakers. We have demonstrated that DPCW is not a straightforward, objective task, but rather a complex, institutionally situated sociotechnical process that requires negotiation and resolution. The questions

posed in the vignette at the beginning of this article—*What constitutes "selling" data? Should they roll this out to all users or only in California? What's the discovery strategy? Should they audit opt-outs to confirm compliance or just expect it to work?*—merit attention from a collaborative group of heterogeneous actors and should not just be delegated to developers to *"make a good faith effort"* . Responsibility and accountability for compliance should be collectively held and deliberated by drawing on multiple forms of expertise.

It is tempting to conclude that data protection regulation should impose more specific software and design requirements. In some cases, this is an appropriate and even necessary approach. For example, studies have demonstrated that certain design choices can and should be standardized in order to improve clarity and use for the public [21]. However, in our findings, the line between *"specific, clear requirements"* and *"open to interpretation"* was not so easy to find—and it is not clear that such a line can exist. Instead, data protection regulations should serve as an infrastructure or baseline set of expectations for public accountability over companies that collect personal data. Just like other infrastructure, these regulations are deeply integrated into other systems in complex ways and thus require regular repair and maintenance work. However, infrastructure famously becomes most visible on breakdown [36], which, according to our findings, can be difficult to discern in the case of data protection regulations because data and data systems are not easily subject to public scrutiny–or even visible to developers themselves (see Section 4.3.1). How can we uphold responsibility for compliance for complex sociotechnical systems that don't reveal themselves when they fail? This issue suggests alternative mechanisms or systems of accountability need to be imagined in order to fulfill the promises of data protection and digital privacy.

5.3 Opportunities for Accountability?

Developing a more detailed and nuanced understanding of DPCW is even more important because developers often conceive of data protection compliance work as a one-time project. All the participants acknowledged that they have not returned to initial compliance instrumentation to ensure high quality, update temporary settings, or audit their work—even though several participants described implementing provisional configurations that they intended to return to in the future. Instead, they generally wait for bugs to emerge—which are unlikely to emerge as long as users are unlikely to exercise their privacy rights or call attention to errors.

This suggests that end users can play a key role in increasing accountability for privacy work. For example, in the case of data subject access requests, several participants stated that they intended to enhance or automate their processes, but that they did not see the need to do so because of the small number of requests submitted by users. Moreover, participants agreed that few users are likely to take advantage of features such as opting out of optional cookies. Increasing pressure from end users, and making developers aware of user interest, may increase developers' motivations to reconceptualize DPCW as a continuous priority and to return to and improve data protection features. This urgency and pressure would also contribute to persuading developers that DPCW is valuable not only to achieve regulatory compliance but also to meet users' needs and expectations. Collectively, then, these findings suggest an alternative way to understand how developers approach privacy work: by exploring how and why developers anticipate user feedback about data privacy–and how they respond.

5.4 Limitations and Future Work

This study used purposive sampling and constructive grounded theory to explore data protection compliance work (DPCW) as an object of empirical analysis. These methods have some important limitations. Our participants were skewed toward North America and we focused on common themes across a variety of organizational contexts, but future studies could pursue comparative analysis or focused study on specific geographic regions (either specific regulations or liable companies in a specific region). In addition, our interviews were conducted in 2021–22, up to 5 years after compliance work began for GDPR. Thus, our participants had different levels of recall of specific details. For all these reasons, this study is not necessarily generalizable to all companies subject to data privacy laws in all contexts. Future research could examine DPCW soon after implementation or, ideally, in action through ethnographic study with a team.

In addition, future studies can focus on specific roles within the category of data technicians that were not recruited in this study. For example, in some companies, *privacy program managers* develop company-wide operational practices and mediate between functional teams such as developers and lawyers. In fact, this work is codified in the curriculum for the Certified Information Privacy Manager (CIPM) certification that is offered by the International Association of Privacy Professionals (IAPP) [30]. This curriculum outlines standardized expectations and processes that can be analyzed to unpack how privacy program managers navigate technical, legal, and operational expertise and boundary work, as described in Section 5.1.

6 CONCLUSION

This article expanded upon prior research by adding texture to an understanding of developers' unique capacity to shape data protection compliance in three ways: by creatively interpreting specific clauses such as *"strictly necessary"* and *"personal data"*; by making such decisions in a uniquely unaccountable way; and by treating data protection work to be a one-time project with dubious, indeterminate value to users. At the same time, the developers interviewed conceived of their impact and responsibility as highly limited. This discrepancy highlights the significance of these findings for adding specificity to why and how developer attitudes and experiences affect data protection regulations in the field.

Overall, these findings validate the importance of understanding not only the behavior of developers and other technical workers when implementing privacy features, but also their attitudes toward that work—especially in the case of data protection regulations. Further research connecting attitudes to technical outcomes that materially affect users' privacy experiences online will clarify how developers play a highly impactful, yet under-studied, co-regulatory role in shaping privacy through subjective interpretation and implementation of data protection statutes.

ACKNOWLEDGMENTS

Thank you to all the research participants who shared their experiences and dedicated their time. Thanks to Professor Christina Dunbar-Hester for valuable feedback on the development and analysis stages of this project, and to the organizers and participants of the symposium on GDPR and CCPA organized by UC Berkeley's Center for Long-Term Cybersecurity. Finally, thank you to the anonymous reviewers whose comments greatly improved this article. This work was supported by the USC Center on Science, Technology, and Public Life and by the Michael Hoefges Graduate Student Research Fund hosted by AEJMC's Law & Policy Division.

REFERENCES

[1] Rebecca Balebako and Lorrie Cranor. 2014. Improving App Privacy: Nudging App Developers to Protect User Privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58. https://doi.org/10.1109/MSP.2014.70

[2] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Faith Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. In *Proceedings 2014 Workshop on Usable Security*. Internet Society, San Diego, CA, 10 pages. https://doi.org/10.14722/usec.2014.23006

[3] Colin J Bennett. 2018. The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity* 23, 2 (2018), 239–246. https://doi.org/10.3233/IP-180002

[4] Ann Cavoukian. 2009. *Privacy by design: The 7 foundational principles.* Technical Report. Information and Privacy Commissioner of Ontario, Canada.

[5] Anupam Chander, Margot E Kaminski, and William McGeveran. 2021. Catalyzing privacy law. *Minnesota Law Review* 105 (2021), 1733–1802.

[6] Kathy Charmaz. 2014. *Constructing Grounded Theory* (2 ed.). Sage, Los Angeles.

[7] Lorrie Faith Cranor. 2021. Informing California privacy regulations with evidence from research. *Commun. ACM* 64, 3 (2021), 29–32.

[8] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proceedings 2019 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA, 15 pages. https://doi.org/10.14722/ndss.2019.23378

[9] Laura DeNardis and Andrea M Hackl. 2015. Internet governance by social media platforms. *Telecommunications Policy* 39, 9 (2015), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

[10] Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax, Wim Lamotte, and Ken Andries. 2019. Personal Information Leakage by Abusing the GDPR "Right of Access". In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA). USENIX Association, USA, 371–386.

[11] Ilker Etikan, Sulaiman Abubakar Musa, and Rukayya Sunusi Alkassim. 2016. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics* 5, 1 (2016), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

[12] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Yokohama Japan, 16 pages. https://doi.org/10.1145/3411764.3445148

[13] Hadi Ghanbari, Tero Vartiainen, and Mikko Siponen. 2018. Omission of Quality Software Development Practices: A Systematic Literature Review. *Comput. Surveys* 51, 2 (2018), 27 pages. https://doi.org/10.1145/3177746

[14] Thomas F. Gieryn. 1983. Boundary-Work and the Demarcation of Science from Non-Science: Strains and Interests in Professional Ideologies of Scientists. *American Sociological Review* 48, 6 (1983), 781–795. http://www.jstor.org/stable/2095325

[15] Barney G. Glaser and Anselm L. Strauss. 1967. *Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine, Chicago.

[16] Daniel Greene and Katie Shilton. 2018. Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society* 20, 4 (2018), 1640–1657. https://doi.org/10.1177/1461444817702397

[17] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* 18, 1 (2006), 59–82. https://doi.org/10.1177/1525822X05279903

[18] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "Okay, whatever": An Evaluation of Cookie Consent Interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, 27 pages. https://doi.org/10.1145/3491102.3501985

[19] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 12 pages. https://doi.org/10.1145/3313831.3376511

[20] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 387–406.

[21] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, 25 pages. https://doi.org/10.1145/3411764.3445387

[22] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by designers: Software developers' privacy mindset. *Empirical Software Engineering* 23, 1 (Feb 2018), 259–289. https://doi.org/10.1007/s10664-017-9517-1

[23] Monique M Hennink, Bonnie N Kaiser, and Vincent C Marconi. 2017. Code saturation versus meaning saturation: how many interviews are enough? *Qualitative Health rResearch* 27, 4 (2017), 591–608. https://doi.org/10.1177/1049732316665344

[24] Tianshi Li, Yuvraj Agarwal, and Jason I. Hong. 2018. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 35 pages. https://doi.org/10.1145/3287056

[25] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 28 pages. https://doi.org/10.1145/3432919

[26] Michael Lipsky. 1980. *Street-level Bureaucracy: Dilemmas of the Individual in Public Service.* Russell Sage Foundation, New York.

[27] Abraham H. Mhaidli, Yixin Zou, and Florian Schaub. 2019. "We Can't Live without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 225–244.

[28] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 13 pages. https://doi.org/10.1145/3313831.3376321

[29] Sean O'Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. 2021. (Un)clear and (In)conspicuous: The Right to Opt-out of Sale under CCPA. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (Virtual Event, Republic of Korea) *(WPES '21)*. Association for Computing Machinery, New York, NY, USA, 59–72. https://doi.org/10.1145/3463676.3485598

[30] International Association of Privacy Professionals. 2023. IAPP CIPM Body of Knowledge. https://iapp.org/media/pdf/certification/CIPM_BoK_v4.0.0.pdf

[31] Theodore M Porter. 1996. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life.* Princeton University Press, Princeton, NJ.

[32] Michael L Rustad and Thomas H Koenig. 2019. Towards a global data privacy standard. *Florida Law Review* 71, 2 (2019), 365–453.

[33] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing effective privacy notices and controls. *IEEE Internet Computing* 21, 3 (2017), 70–77. https://doi.org/10.1109/MIC.2017.75

[34] Paul M Schwartz. 2019. Global data privacy: The EU way. *NYU Law Review* 94, 4 (2019), 771–818.

[35] Katie Shilton and Daniel Greene. 2019. Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics* 155, 1 (2019), 131–146. https://doi.org/10.1007/s10551-017-3504-8

[36] Susan Leigh Star. 1999. The ethnography of infrastructure. *American Behavioral Scientist* 43, 3 (1999), 377–391. https://doi.org/10.1177/00027649921955326

[37] Susan Leigh Star and James R Griesemer. 1989. Institutional ecology,translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science* 19, 3 (1989), 387–420. https://doi.org/10.1177/030631289019003001

[38] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, 24 pages. https://doi.org/10.1145/3544548.3581060

[39] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Deciding on personalized ads: nudging developers about user privacy. In *Proceedings of the Seventeenth*

USENIX Conference on Usable Privacy and Security (SOUPS'21). USENIX Association, USA, 23 pages.

[40] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, 15 pages. https://doi.org/10.1145/3411764.3445768

[41] Mohammad Tahaei, Adam Jenkins, Kami Vaniea, and Maria Wolters. 2019. "I Don't Know Too Much About It": On the Security Mindsets of Computer Science Students. In *Socio-Technical Aspects in Security and Trust* (Luxembourg, Luxembourg) *(STAST 2019)*. Springer Nature Switzerland, Cham, Switzerland, 27–46. https://doi.org/10.1007/978-3-030-55958-8_2

[42] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. In *Proceedings on Privacy Enhancing Technologies* (Sydney, Australia), Vol. 2022. Sciendo, Berlin, Germany, 114–131. https://doi.org/10.2478/popets-2022-0038

[43] Mohammad Tahaei and Kami Vaniea. 2019. A Survey on Developer-Centred Security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (Stockholm, Sweden). IEEE, New York, NY, USA, 129–138. https://doi.org/10.1109/EuroSPW.2019.00021

[44] Mohammad Tahaei and Kami Vaniea. 2021. "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, 11 pages. https://doi.org/10.1145/3411763.3451805

[45] Mohammad Tahaei and Kami Vaniea. 2022. Recruiting Participants With Programming Skills: A Comparison of Four Crowdsourcing Platforms and a CS Student Mailing List. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, 15 pages. https://doi.org/10.1145/3491102.3501957

[46] Mohammad Tahaei, Kami Vaniea, and Awais Rashid. 2023. Embedding Privacy Into Design Through Software Developers: Challenges and Solutions. *IEEE Security & Privacy* 21, 1 (2023), 49–57. https://doi.org/10.1109/MSEC.2022.3204364

[47] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 14 pages. https://doi.org/10.1145/3313831.3376768

[48] Ari Ezra Waldman. 2021. *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge University Press, Cambridge, UK.

[49] JoAnne Yates and Wanda J Orlikowski. 1992. Genres of organizational communication: A structurational approach to studying communication and media. *Academy of Management Review* 17, 2 (1992), 299–326. https://doi.org/10.5465/amr.1992.4279545

A INTERVIEW GUIDE

(1) Background
   (a) What is your familiarity with GDPR and/or CCPA?
   (b) Tell me about the time and place where you were involved with GDPR or CCPA compliance. What was your job and company, when was this, and which regulation(s) did you work on?
(2) Data Protection Compliance Work
   (a) What specific elements of GDPR/CCPA compliance did you work on? What were you responsible for?
   (b) Which other teams were involved in this work? Who was the point person or lead within the company?
   (c) Was there anything you were unsure about? How did you handle it? Can you provide an example?
   (d) How did you think about risk within the company?
   (e) What decisions was each team, including your own, responsible for?
   (f) How was responsibility managed across these teams? How was this decided?
   (g) How much responsibility or decision-making power do you feel like you held?
   (h) How prepared did you feel to make decisions about user privacy?
   (i) What tools or systems do you use to handle compliance, including responding to user requests for access or deletion?
   (j) What was different about CCPA compliance in 2019–20 versus GDPR in 2017–18?
(3) DPCW Reflections
   (a) How did your background inform how you approached your work on data protection compliance, such as education, previous work experience, or training?
   (b) What expectations did you feel about your ability to work on compliance? How did you feel about those expectations?
   (c) How satisfied are you with how your company has handled data protection compliance?
   (d) How committed do you think your company is in upholding user privacy through data protection?
   (e) What, if anything, do you think would surprise people if they knew how your company handles data protection compliance?
(4) Personal Reflections
   (a) How do you feel about your privacy in the applications you use on a daily basis?
   (b) To what extent has working on privacy changed your feelings about your own privacy?
   (c) Any other opinions or experiences you want to share?

B LIST OF CODES/THEMES

Table 2: Codes/Themes in Interview Data

Category	Code/Theme
Attitudes About...	California Consumer Privacy Act or California Privacy Rights Act
	Data privacy laws (current, in general)
	Data privacy laws (future, in general)
	Digital privacy (in general)
	Digital security (in general)
	General Data Protection Regulation
	Other data privacy laws
Personal Experience With...	Data breaches
	Data privacy laws
	Data privacy training and education
Work Experience With...	Data breaches
	Noncompliance
	Partial/incomplete compliance
	Regulator inquiries, charges, fines, or violations
	User complaints
Organizational Dynamics of Compliance Work	Accountability
	Ambiguity and uncertainty
	Audits
	Autonomy
	Boundaries (functional/professional)
	Code review
	Decision-making
	Expertise
	Privacy champions
	Responsibility
	Risk
Relationships Between Developers and...	Compliance officers
	Data analysts/scientists
	Designers
	Executives
	Lawyers
	Product managers
	Project managers
	Third-party actors
	Users