Selected Papers of #AoIR2024:
The 25th Annual Conference of the
Association of Internet Researchers
Sheffield, UK / 30 Oct - 2 Nov 2024

UNPACKING EXPERTISE IN THE PRIVACY TECH INDUSTRY

Rohan Grover
University of Southern California

Introduction

Data privacy laws have been passed and implemented with increasing velocity since the European Union's General Data Protection Regulation (GDPR) passed in 2016 (Bennett, 2018; Bradford, 2020). These laws are socioculturally distinct (Grover et al., 2024), but broadly they impose restrictions on companies as the most visible actors responsible for collecting, processing, sharing, and selling personal data. In response, these companies often call upon internal and external lawyers, technologists, compliance officers, and consultants to develop compliance programs that minimize both legal risk and impact to their surveillant business models (Waldman, 2021).

In response, companies have spent billions of dollars building compliance programs, giving rise to an emergent *privacy tech industry* that consists of tech startups, consultants, investors, platforms, and domain experts that collectively help companies comply with data privacy laws. These actors play a key role in translating the law into software products that constitute the infrastructure of companies' privacy programs.

This study asks: how is expertise defined and encoded in the privacy tech industry? It is part of a broader ethnographic study about mapping the privacy tech industry while focusing specifically on how boundaries are drawn across professional jurisdictions that index conceptualizations of privacy and consent in technical, legal, economic, political, and moral terms. The study draws on multi-sited fieldwork in the privacy tech industry, including 18 days of participant-observation at industry conferences, 29 semi-structured interviews, attending industry events and following trade publications, developing my own expertise through training and certification, and examining regulatory documents and media artifacts.

Suggested Citation (APA): Grover, R. (2024, October). Unpacking Expertise in the Privacy Tech Industry. Paper presented at AoIR2024: The 25th Annual Conference of the Association of Internet Researchers. Sheffield, UK: AoIR. Retrieved from http://spir.aoir.org.

Unpacking Expertise

Expertise is a multidimensional analytic developed by sociologists and science and technology studies (STS) scholars in part to account for controversies over claims to knowledge. Analytically, it is valuable for deconstructing logics that have been naturalized and stabilized through professional boundaries. It can be defined either as an attribute found “inside” people or as an attribution defined externally, such as through certified credentials or professional memberships (Collins & Evans, 2007; Eyal, 2019).

One key dimension is how expertise contributes to how professional groups establish jurisdiction, distinguish responsibilities, and uphold legitimacy. These questions have been approached by understanding expertise as “performance” (Hilgartner, 2000) or “enactment” (Knorr Cetina, 1999) that are made visible by “boundary work” (Gieryn, 1983) that manifests in institutional stability (Abbott, 1988). Thus, expertise is a valuable meso-level analytic to evaluate a professional field.

A second key dimension of expertise is whether “lay” individuals possess expertise and what role, if any, lay expertise should play in policy and governance (e.g., Epstein, 1995). Such questions index a debate about whether expertise should be defined to facilitate technocracy—in which experts are entrusted due to their unique technical knowledge—or participatory democracy, in which citizens are empowered to contest technical authority with lived experiences (Eyal, 2019). Thus, expertise is also valuable for surfacing structural power and normative politics.

Findings

First, my findings demonstrate that the privacy tech industry constitutes a networked arena of relations structured by partitioning professional expertise across technical, legal, and operational domains. This is evident in the International Association of Privacy Professionals, the global association that organizes industry conferences, conducts trainings, and offers certifications for privacy tech professionals. This boundary work allows technologists and lawyers to maintain legitimacy despite uncertainty about what constitutes “privacy” as well as “compliance.” It also upholds the credibility of technologists who often stand in for technical systems despite lacking sufficient insight and transparency to attest to their contents, structure, activities, and levels of compliance. Thus, technical expertise, in particular, is operationalized as an *attribution* rather than an *attribute* in that it is broadly attributed to software engineers based on their software engineering skills, technical fluency, professional image, and, most importantly, proximity to technical systems.

Second, technical expertise in the privacy tech industry is often tenuous and contingent. Actors such as startups, consultants, technologists, and investors bring their own interests that shape how they interpret ambiguous factors in data privacy law, such as what constitutes due diligence, responsibility, and valid consent. However, individuals are often ill equipped to make confident assessments because privacy programs are modularized, built on networks of integrated software that undermine epistemic accountability. For example, a senior developer shared that they felt unable to certify the compliance of their products because they were “entrusting that what is supposed to

happen, does… We're sending a signal [to another system] and getting a response… What happens on their systems is completely opaque to us." This example illustrates the contingent nature of technical expertise, which could be strengthened by applying scrutiny and agonistic deliberation to evaluate the content of expertise rather than its performance.

Third, boundaries of expertise are increasingly encoded in compliance software, perpetuating performative rather than scrutinized expertise and therefore codifying splintered accountability. Compliance software refers to products such as data mapping, consent management, third-party risk management, and data rights automation offered by tech startups including OneTrust, Securiti, TrustArc, BigID, and Transcend. These products encode values that scale as thousands of companies integrate them into their privacy programs. This software often promotes efficiency over friction, especially by automating translation work between functional teams. For example, a privacy tech executive described her clients' biggest problem as "translation error" between privacy program managers and software developers—two groups that embody operational and technical expertise. She understood her goal to be minimizing friction by automating translation work across teams, substituting social interaction with software integrations. However, automating translation work upholds jurisdictional boundaries and inhibits the scrutiny needed to evaluate the content of expertise. This includes impeding contestation from individuals and communities who fall outside the technical-legal-operational expertise model. At scale, then, privacy tech software promotes managerial processes that manifests as checkbox compliance, in which individuals such as the senior developer mentioned above simply perform isolated actions that should, theoretically, add up to upholding the spirit of the law, but, in practice, may fail to achieve accountability.

Discussion

Expertise in the privacy tech industry mediates relations among professional groups, between people and technical systems, and between professional experts and the public. There are substantial stakes for understanding—and reconfiguring—expectations and standards of expertise in data privacy and technology policy more broadly. Currently, interpreting and operationalizing data privacy law is often assigned to people with technical proximity and accreditation. However, the questions at the heart of data governance concern values such as subjectivity, autonomy, and consent, which would benefit from scrutinizing the contents of expertise and inviting agonistic deliberation.

Moreover, the exclusion of lay expertise—which is concretized through privacy tech software products—perpetuates the technocratic structural relations of a surveillance economy. This is evident in how privacy is enacted as an individual value and evaluated based on individual behaviors. Privacy scholars have long advocated for recognizing privacy as a fundamentally social phenomenon (Cohen, 2012; Nissenbaum, 2009) and argued that individualizing privacy capitulates to the depoliticizing impulse of "digital resignation" (Draper & Turow, 2019). Nevertheless, these practices persist in the privacy tech industry, allowing corporate actors to define the terms and stakes of technology policy. This manifests in borders to participation such as requirements for

technical literacy, training, certification, and corporate affiliations. These dynamics characterize privacy expertise as something that cannot be found organically "within" individuals but instead as technical skills and knowledge only accessible to professionals with proximity to technical systems.

Codifying boundaries of expertise attenuates data privacy law in action. Inhibiting cross-functional deliberation and democratic participation authorizes existing practices by hegemonic institutions. Perhaps drawing from alternative sources of expertise, including embodied, subjective, affective knowledge from the intended beneficiaries of data privacy laws—individuals and communities, especially those with marginalized identities with higher stakes for digital privacy—can contribute to a more equitable and more effective data privacy paradigm.

References

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor*. University of Chicago Press.

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

Bradford, Anu. (2020). *The Brussels Effect: How the European Union rules the world*. Oxford University Press.

Cohen, J. E. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. Yale University Press.

Collins, H. & Evans, R. (2007). *Rethinking expertise*. University of Chicago Press.

Draper, N. A. & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839.

Epstein, S. (1995). The construction of lay expertise: AIDS activism and the forging of credibility in the reform of clinical trials. Science, Technology, & Human Values, 20(4), 408–437. https://doi.org/10.1177/016224399502000402

Eyal, G. (2019). *The crisis of expertise*. Polity Press.

Gieryn, T. F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review*, *48*(6), 781–795. https://doi.org/10.2307/2095325

Grover, R., Jang, K., & Su, L. W. (2024). Beyond digital protection(ism)? Comparing data governance frameworks in Asia. *Journal of Information Policy*, *14*. https://doi.org/10.5325/jinfopoli.14.2024.0005

Hilgartner, S. (2000). *Science on stage: Expert advice as public drama*. Stanford University Press.

Knorr Cetina, K. (1999). *Epistemic cultures: How the sciences make knowledge*. Harvard University Press.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Waldman, A. E. (2021). *Industry unbound: The inside story of privacy, data, and corporate power*. Cambridge University Press. https://doi.org/10.1017/9781108591386