FOREWORD

Information privacy has changed quite a bit over the past thirty years. Even if you haven't been following the news, you've probably felt it as part of your daily interaction with information technologies. More of our personal information is converted into data, collected, used, and shared than ever before. The law of information privacy has changed as well. What started with a reckoning around the printing press and handheld cameras became formalized with the advent of the database and has turned into something bigger and more complex than I would have ever imagined.

The idea for this symposium began with my mentor and longtime collaborator Daniel Solove, reflecting upon the start of the modern information privacy law project in the 1990s, and how privacy law and scholarship have developed in the 30-odd years since the widespread adoption of the Internet. When I first started studying privacy, there was only a smattering of information privacy laws scattered here and there. The first privacy texts, many written by contributors to this symposium, were comparatively thin. It was plausible to make yourself aware of most of the privacy scholarship out there because the field was still relatively new and niche.

Some things have stayed the same. We still don't have a national privacy law and Prosser's four torts (disclosure, intrusion, misappropriation, false light) are still the entry point for understanding the common law's approach to privacy. But so much else has changed. The Federal Trade Commission took the baton that Congress refused and built out a body of consumer privacy law. The European Union decided to take the fair information practices seriously and California (in a sense) followed. Meanwhile social media arrived, turned into platforms, and ate the rest of the Internet. What was once the Internet of Things is now just "Things" because it's all connected. Big data came and then turned into artificial intelligence.

Society changed too. Our wild technological optimism got tampered when we were reminded that power asymmetries are getting worse and profit motives are far older than the information superhighway. A long overdue social reckoning on race, sexual identity, gender, and ability better highlighted that while privacy might not be dead yet, it is not distributed equally or justly. Jobs became "gigs" as platforms devoured business models and markets moved to turn virtually every social interaction into an opportunity to extract our information, attention, and labor. Meanwhile, our public discourse and mediated interactions became more poisoned than ever, with every screen threating us with misinformation, deep fakes, manipulative user interfaces, and hidden surveillance.

For these reasons, we brought a group of exceptional and pioneering scholars together to explore how far privacy has come, where it is now, and where it's going. Some of the articles in this special symposium issue asses the theory and effectiveness of information privacy law. Daniel Solove and I kick things off by drawing upon the work of Franz Kafka to argue that empowering the individual

isn't the answer to protecting privacy, especially in the age of artificial intelligence. Instead, the law should focus on ensuring a societal structure that brings the collection, use, and disclosure of personal data under control. Danielle Citron revisits the Congressional debates surrounding regulation of the FBI's National Crime Information Center's computerized system to fight against the fatalism old by industry that nothing can (or should) be done to improve our privacy status quo. She argues that previous Congressional leaders of the past would have rejected modern data grabs as "unconstitutional and un-American." Citron notes that our history of legislating privacy is a reminder that "totalizing surveillance is neither acceptable nor desirable. Privacy can and should be ours." Salome Viljoen takes a meta-critical approach to the field of information privacy law and concludes that the field is selling itself a bit short. She explores how privacy (and privacy law) became an overloaded concept, weighing the tradeoffs inherent in its "big tent" approach. Viljoen argues that when insights about information's role in connecting, empowering, and endangering people get relegated solely within the domain of "privacy law," this labeling undersells the broader value these insights might have in or other legal areas for understanding legal relations in an informational society.

Other essays in this collection target the socially unjust accumulation, distribution, and use of power that comes with personal data. Scott Skinner-Thompson encourages privacy scholars to critically reflect upon what impact, if any, their privacy work is having on mitigating harm and anti-subordination goals, particularly for minoritized communities. In addition, Skinner-Thompson argues that there has been an over reliance on state-centric solutions leveraging the carceral state and surveillance tools that risk exacerbating privacy harms and subordination. Ari Waldman takes on the trap of legibility for gender-nonconforming populations, arguing that while becoming legible in government data systems might seem to be beneficial, it is actually a "damned-if-you do, damned-if-you-don't" double bind. If you remain illegible to these government systems, they can be more easily marginalized because they are effectively erased. But once you become legible, then you can be marginalized through the harassment and discrimination that inevitably follow challenges to traditional gender norms. He argues more attention must be paid to the design of choice architectures that facilitate the self-subjectification of the surveilled citizen.

Some essays focused on new avenues for privacy regulation, or new ways to think about traditional regulatory levers. Zahra Takhshid explores the underappreciated role that transaction costs, also known as "friction," can play in a privacy-by-design regulatory agenda for wearable AI tools. She argues that lawmakers should mandate bystander notice and consent for the use of wearable AI tools through the introductions of privacy frictions, which are "noticeable and tangible steps that would alert the third party exposed to the device of its presence and allow the bystander to make an informed choice." Meg Jones and Paul Ohm propose a new way of looking at the frequently critiqued concept of "consent" in privacy law—as voting. The authors argue that we should not abandon the "I agree" checkboxes we know and revile, but instead approach

them as an opportunity to meaningfully participate in the design of technology by "voting" for structures and practices. By recasting "consent" as "elections" for consumer voice, lawmakers and industry can increase the legitimacy of privacy efforts, give better voice to people regarding how technology is designed, and help build trust in systems leveraging these tools. Finally, Neil Richards and I close the issue by focusing on a key dimension of commercial surveillance that is too often treated as a supporting cast member: the concept of engagement. Measuring people's time, attention, and other interactions with a service is a lucrative digital business model, but it is costly to our privacy, our democracy, and our culture. We make the argument for a wrongful engagement doctrine as part of privacy and consumer protection law to limit the societal cost of "free" engagement-based business models.

I'd like to thank Editor-in-Chief Keenan Hunt-Stone, Senior Managing Editor Caroline Grady, faculty advisor Professor Jim Fleming, and every member of the *Boston University Law Review* for all their work on this symposium. Privacy is at the crossroads. We hope this issue will help serve as a waypoint and a guide.

Woodrow Hartzog
May 28, 2024