
PART I

PRIVACY

In the 1970s, Western countries began to grapple with the social implications of new information technologies. Mainframe computers enabled a very few large institutions to collect vast amounts of data about individuals. Many began to worry that these databases would inexorably erode our privacy and subject us to increasingly totalitarian methods of social control. As a corrective, American legal scholar Alan Westin articulated a set of fair information practices to give individuals some level of procedural control over their personal information.

Almost forty years later, these fair information practices have become the standard for privacy protection around the world. And yet, over that same time period, we have seen an exponential growth in the use of surveillance technologies, and our daily interactions are now routinely captured, recorded, and manipulated by small and large institutions alike.

This section begins with a critical examination of the crux of the fair information practices paradigm, the notion that individuals will be able to protect their privacy if their information can only be collected, used, and disclosed with their consent. Ian Kerr, Jennifer Barrigar, Jacquelyn Burkell, and Katie Black examine the ways in which the consent-gathering process is often engineered to skew individual decision-making, in effect creating an illusion of free choice that helps to legitimize surveillance practices. Drawing on interdisciplinary work in psychology and decision theory, these contributors argue that the current threshold for consent with respect to the collection, use, and disclosure of personal information is not high enough to protect us from corporate initiatives that invade our privacy.

Philippa Lawson and Mary O'Donoghue examine the same question from a legal perspective, by canvassing the use of consent in Canadian privacy laws in both public sector and private sector contexts. Although private sector legislation provides more scope for negotiation between collectors and individuals, the authors caution that our current reliance on consent as the gold standard for privacy protection may be misplaced because the exercise of that consent is often more notional than real.

Alex Cameron looks at the unintended consequences of fair information practices in the context of digital rights management (DRM) software. He begins with the hypothesis that DRM impedes the individual's right to enjoy creative works in private. He then concludes that the consent provisions in data protection laws may be ineffective in constraining the surveillance capacities of DRM-protected works, in effect making it harder to create an appropriate balance between property rights and privacy rights in digitized spaces.

Rob Carey and Jacquelyn Burkell approach the consent question from a different perspective. They examine the privacy paradox: although people maintain that they are concerned about lack of privacy in digital social networks, they nevertheless reveal information about themselves to relative strangers. Through a heuristics-based analysis, they demonstrate that people are more likely to protect their privacy in the context of their personal relationships and less likely to

protect it when they interact with unknown others, because their assessment of risk in the latter scenario is stripped of the social markers upon which we rely in personal interactions. Accordingly, a heuristics approach helps to explain both aspects of the paradox and suggests that we should be cautious about assuming that the online disclosure of personal information serves as a proxy for consent to its collection, use, and disclosure.

Anne Uteck takes a similar look at the assumptions that are embedded in our enjoyment of spatial privacy. As we move to an age of ubiquitous computing, the signposts we use to negotiate our sense of space, visibility, subjectivity, and privacy are subtly reconstructed. She suggests that we need to develop a more nuanced understanding that can account for our everyday experience of privacy and the expectation that the spaces in which we interact will be protected from unwarranted intrusion.

In like vein, Jason Millar posits that we should revisit our assumptions about knowledge creation in the context of predictive data mining. He argues that the network society has given rise to new forms of knowledge about persons because it enables others to extract data about us from disparate sources and to use that data to create a representation of our beliefs, intentions, and desires even when we did not mean to disclose that information. Millar concludes that policymakers must go beyond mere procedural protections or fair information practices because the context of the original disclosure of the information is lost when it is matched for predictive purposes.

Jennifer Chandler also suggests that our notions of privacy must be reframed in the context of national security. She argues that the traditional juxtaposition of privacy versus security in a zero sum game closes down debate in favor of security before we can fully examine the impact that a given reduction of privacy will have. By accounting for the ways in which privacy enhances our security, she concludes, we will be better able to articulate an appropriate balance that will advance both security and privacy interests.

Daphne Gilbert suggests that part of the problem may be the narrow legal treatment of privacy in constitutional law as part of the legal right to be free of unreasonable search and seizure. She argues that seeking to protect privacy rights through substantive equality guarantees instead of through due process protections may create a foundation for the protection of privacy as an inherent element of human dignity. In doing so, she sets out a useful framework for addressing the original concerns of the 1970s and reconnecting the privacy debate to human rights discourses that seek to protect private life.

Jena McGill advances a similar approach through her examination of the experience of a specific equality-seeking community, abused women. Like Gilbert, she seeks to broaden the scope of the privacy debate by interrogating the feminist rejection of privacy as a means of shielding abusive men from legal sanctions. Grounding her analysis in a deep concern for the lived realities of abused women, she argues that women who are able to establish and defend

4 PRIVACY

boundaries that reflect their needs and desires will be better able to achieve the privacy they require to protect themselves from a battering partner.

Marsha Hanen and Valerie Steeves apply a different lens to the privacy discourse by examining the relationship between privacy and identity. Hanen provides an overview of the ways in which new genetic technologies challenge our traditional understanding of these key concepts. She argues that genomics has the potential to redefine our sense of who we are. We accordingly need to think through the implications of new technologies from a more holistic perspective that accounts for the interaction between people's genomes, the environment, and human dignity.

Steeves returns to the starting point of fair information practices and revisits Westin's theory of privacy as informational control. Incorporating the insights of social theorists, she proposes a new model that defines privacy as a dynamic process of negotiating personal boundaries in intersubjective relations. This may potentially move the policy debate beyond the current impasse of fair information practices, by placing privacy at the heart of the social experience of identity. That experience of identity is the subject of the next section of the book.