Hero or Villain: The Data Controller in Privacy Law and Technologies

Claudia Diaz, Omer Tene, Seda Gürses

In Europe, privacy is considered a fundamental human right. Section 8 of the European Convention of Human Rights (ECHR) limits the power of the state to interfere in citizens’ privacy, “except such as is in accordance with the law and is necessary in a democratic society”. Constitutional privacy protection also appears in the Fourth Amendment to the United States Constitution. Both the ECHR and the US Constitution establish the right to privacy at a high level of abstraction as freedom from government surveillance. Over the past 40 years, a specific framework has emerged to protect informational privacy. Unlike the constitutional documents, this framework is technologically minded. However, it provides little protection against the risk of surveillance by either government (which benefits from explicit exemptions) or private sector organizations (which are assumed to be trusted parties). This article argues that privacy enhancing technologies (PETs) should fill the gaps between these frameworks to help individuals exercise their freedom from surveillance.

Today, surveillance capabilities are no longer restricted to the realm of states. As more and more daily activities become mediated by technology, private sector organizations have gained the ability to conduct surveillance at an unprecedented scale, including of individuals’ communications data, online and offline purchases, geo-location and health. In this article, we address the role PETs play in protecting individuals from surveillance, a term we use to capture not only monitoring by government but also by private sector entities. While the term “PETs” has been used loosely to describe a broad range of privacy technologies, we use it in this article to mean technologies specifically aimed to enable individuals to engage in activities free from surveillance and interference. PETs allow individuals to determine which information they disclose and to whom, so that only information they explicitly share is available to intended recipients.

We argue that PETs are aligned with the objectives of the constitutional framework, which given its level of abstraction is not tech-oriented; while not always in tune with the goals of the tech-oriented information privacy framework. Hence, PETs are trapped in a “regulatory limbo” between a framework which recognizes their goals but not their means, and one that recognizes their means but not their goals. We claim that given the genesis of information privacy law in fears about surveillance, policymakers should recognize and expand by appropriate regulatory measures the role of technologies that enable individuals to enforce their right to privacy as freedom from surveillance.

The legal framework for protection of information privacy is organized around a set of “fair information practice principles” (FIPPs), which apply to “data controllers”, business or government organizations collecting, storing, using or disclosing personal data. While Alan Westin’s canonical conceptualization of privacy concerns individual control over information, the FIPPs provide
individuals with very little control, usually presented as a “notice and choice” mechanism. Given the weak controls on information collection, the legal framework has shifted to imposing information stewardship obligations on data controllers, who act as custodians of personal data. These obligations, increasingly grouped under the title “accountability”, include devising a privacy compliance program; appointing a chief privacy officer; conducting “privacy impact assessments”; notifying regulators and/or individuals about data security breaches; maintaining a record retention policy; and more. All of these measures assume that a data controller is a trusted party, essentially a fiduciary for individual rights. Even the concept of “privacy by design”, which some initially thought was meant to embed principles of data minimization and anonymization into product engineering, is increasingly portrayed as introducing privacy into organizational processes. In other words, privacy by design too has become an “accountability” tool.

The notion of the data controller as a trusted party is ill at ease with the anti-surveillance gist of constitutional privacy and PETs. The technological community researching PETs departs from a diametrically opposed perception of a data controller, that of an adversary. Under this approach, information disclosed to a data controller is compromised and can no longer be viewed as private. The assumption is that once a data controller collects personal information, it can use it in unforeseen ways, possibly to disadvantage the individuals concerned. Proponents of this view point-out that after disclosure, it is almost impossible to control how personal information is used, concluding that PETs should prevent (or at least limit) information disclosure.

Given that constitutional privacy protects individuals from surveillance and that privacy by design is a vehicle for integration of privacy into technology, we argue that PETs deserve a greater role in the privacy framework. Information privacy law applies mainly to data controllers; hence to examine possible ways to address PETs in law, we classify the PETs according to the degree of data controller involvement.

Certain PETs, such as private information retrieval or zero knowledge protocols, require collaboration by the data controller. They enable a data controller to provide a service that takes as input private user information without the controller becoming privy to such information. For example, a data controller can process a search query and return results without ever learning the query or the results. Other examples include protocols for pay-as-you-drive tolling systems that do not reveal the location of users; and protocols for smart metering that allow accurate periodic billing and real-time prediction of demand – while concealing from the utility the real-time energy consumption of individual households. These PETs thus permit modernization of large-scale infrastructure services without such systems becoming infrastructures of mass surveillance. To implement such PETs, active collaboration and potentially significant investment is required from the data controller.

An additional category of PETs can be deployed unilaterally by users within a service offered by a data controller. These include, for example, encryption tools
that maintain the confidentiality of the contents of emails or social networking posts, including vis-à-vis the data controller. PETs in this category do not require active intervention on the part of the data controller nor modification of its service. Yet the data controller retains the power to disable or block the use of such PETs, and such actions may be in its business interest.

A third category of PETs are stand-alone systems, typically implemented by individuals who work collaboratively to collectively achieve privacy protection. These PETs may be used to access an external service run by a data controller. The most prominent examples of such PETs are anonymous communications networks such as Tor. Here too, active participation by the data controller is not necessary to implement the PETs; yet data controllers can disrupt a PET’s operation, for example, by rejecting access coming from the Tor network.

Finally, PETs operated collaboratively can function as peer-to-peer services, where all participants concurrently act as both users and service providers. The objective of these PETs is to enable the collaborative provision of the service without a centralized party, which is in a position to conduct surveillance. For example, consider the distributed social network Safebook, which is based on a peer-to-peer architecture to avoid the creation of or engagement with a central all-knowing entity.

After classifying the PETs and providing examples of their objectives and strategies, we assess the policy considerations involved in reforming the legal framework to tolerate, facilitate, or indeed mandate their use. For the first category of PETs, which require active data controller implementation, we examine the contexts in which it would be justified to mandate inclusion of PETs in system design, as well as how the legal framework might incentivize the adoption of such PETs for a broader range of services.

For the second category of PETs, which are deployed by users within a service, we ask whether data controllers should be entitled to block the use of PETs or to deny service when a PET is detected; whether contractual terms of service that restrict PET use are fair; and whether data controllers could be incentivized to facilitate the use of the PETs.

For the third and fourth categories of PETs, which are implemented collaboratively to operate as general-purpose private communication channels or as standalone peer-to-peer services, we ask whether such PETs should be protected by law and not delegitimized.

We conclude by arguing that the current informational privacy framework fails to adequately address surveillance concerns. In particular, despite embracing the concept of privacy by design, policymakers have given short shrift to PETs protecting surveillance privacy. The informational privacy framework assumes that a data controller is a trusted party and that it is incumbent upon it to protect individuals’ privacy. This overlooks the fact that a data controller may itself subject individuals to persistent surveillance. The current framework’s treatment of PETs is not the result of regulatory oversight. It is precisely the
capacity of PETs to limit surveillance that has caused them to lose favor with powerful state interests, particularly in law enforcement and national security. At the same time, the information privacy framework should guarantee that the principles underlying constitutional privacy are not discarded with ease.