Money For Your Life: Understanding Modern Privacy

Author : Michael Madison

Date : January 8, 2018

Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 **Colum. L. Rev.** 1369 (2017).

The commercial law of privacy has long occupied a relatively marginal place in modern legal scholarship, situated in gaps among doctrinal exposition, critical conceptual elaboration, and economically-motivated modeling. Much of the explanation for the omission is surely technological. Until Internet technologies came along in the mid-1990s, it was difficult to turn private information into a "thing" that was both technically and economically worth buying and selling.

Technology and markets have passed the point of no return on that score. Claude Shannon, credited as the author of the insight that all information can be converted into digits, has met Adam Smith. Yet relevant legal scholarship has not quite found its footing. *Paying for Privacy and the Personal Data Economy*, from Stacy-Ann Elvy, offers a novel way forward. Professor Elvy's article offers a nifty, highly concrete, and eminently useful framework for thinking about the commercial law of things that consist of assets derived from consumers' private information. It is not only the case that commercial law is one of the legally-relevant attributes of privacy and privacy practices. Privacy can be thought of as a mode of commercial law.

Paying for Privacy lays out its argument in a series of simple steps. It begins with a brief review of the emergence of the now-familiar Internet of Things, network-enabled everyday objects, industrial devices, and related technologies that increasingly permeate and collect data concerning numerous aspects of individuals' daily lives. That review is pertinent not merely to common claims about the urgency of privacy regulation but also and more importantly to the premise that the supply of data-collecting technologies by industry (with accompanying privacy-implicating features) is likely to lead soon to increased demand by consumers for privacy-mediating, privacy-regulating, and privacy-protecting instruments.

The supply/demand metaphor is purposeful, if somewhat speculative, for it leads to a thorough and useful description and taxonomy of instruments currently on offer. Those include "traditional" privacy models involving personal data traded for "free" services (such as Facebook) and "freemium" services (such as LinkedIn) that offer both subscription-based and "free" versions of their services, harvesting money from subscribers (and advertisers and partners) and money and data from the free users. More recent PFP or "Pay For Privacy" models include newer firms offering multiple versions of "pay for privacy" services. Those include "privacy as a luxury," in which providers offer added privacy controls for users in exchange for higher payments, and privacy discounts, by which users get cheaper versions of services if they agree to participate in data monitoring and collection. Switching perspectives from the service to the consumer yields a series of models collected as the PDE, or "Personal Data Economy." Those include the "data insights model," companies that enable individual consumers to monitor and aggregate private information about themselves, perhaps for their own use and perhaps to monetize by offering to third parties. In the related "data transfer model," companies broker markets in which consumers voluntarily collect and contribute data about themselves, making it available for transfer (typically, purchase) by third parties.

The taxonomy is only a snapshot of current practices. This field seems to be so dynamic that inevitably many of the details in the article will be superseded, no doubt sooner rather than later. But the taxonomy helpfully reveals the two-sided character of privacy commerce. Rounding out that basic insight, one might add that there are privacy sellers and privacy buyers, privacy borrowers and privacy lenders, privacy principals and privacy agents, privacy capital and privacy debt, privacy currency and privacy assets. There are secondary markets and tertiary markets. As Professor Elvy notes, the list of privacy intermediaries includes privacy ratings firms – firms that play much the same role as the

bond ratings firms that participated so enthusiastically (and eventually, so devastatingly) in the subprime mortgage market of the early 2000s.

Having laid out this framework, in the rest of the article Professor Elvy thoughtfully parses the weaknesses of the commercial law of privacy and develops a counterpart set of prescriptions and recommendations for further evaluation and possible implementation. All of this is admirably immediate and concrete.

Her critique is linked model by model to the taxonomy; the review below condenses it in the interest of space. First, not all consumers have equal or fair opportunities to collect and market their private data. To some significant degree, and for reasons that may be beyond their control or influence, those consumers either cannot participate in the wealth-creating dimensions of privacy or, because of social, economic, or cultural vulnerabilities (Professor Elvy highlights children and tenants), are effectively coerced into participating. Second, the article repeats, with helpful added doses of commercial law context, the widespread contract law critique that consumers are presented with vague, illusory, and incomplete "choices" in respect of collection, aggregation, and use of private data. Third and fourth (to combine two categories of critique offered in the article), current market and legal understandings of privacy as commercial law treat privacy primarily as what one might call an "Article 2" asset, that is, in terms of sales of things. Overlooked in this developing commercial market is privacy as what one might call an "Article 9" asset, that is, as a source of security and securitization. The potentially predatory and discriminatory implications of that second character should be obvious to anyone with a passing familiarity with the history of consumer lending, and Professor Elvy hammers on those.

Paying for Privacy concludes with a review of the fragmented legal landscape for addressing these problems and a complementary summary of recommendations for improving the prospects of consumers while preserving valuable aspects of both PFP and PDE models. Professor Elvy nods in the direction of COPPA (the Children's Online Privacy Protection Act) and the possibility of industry-specific or sector-specific regulation. Most of her energy is directed to clarifying the jurisdiction of the Federal Trade Commission with respect to PDE models to deal with unfair trade practices regarding privacy that do not fit into traditional or accepted models of harm addressable by the FTC. All of this has the air of the technical, but its broader substantive import should not be overlooked. *Paying for Privacy* serves as a helpful entrée to a newer, broader – and difficult — vision of privacy's future.

Cite as: Michael Madison, *Money For Your Life: Understanding Modern Privacy*, JOTWELL (January 8, 2018) (reviewing Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 **Colum. L. Rev.** 1369 (2017)), https://cyber.jotwell.com/money-life-understanding-modern-privacy/.