Paying to be the Product

Author : Lauren Scholz

Date : October 28, 2019

Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 **B.C. L. Rev.** 423 (2018).

Just after the turn of the millennium, it was common to hear the burgeoning data economy ethically justified through the following refrain: “If you’re not paying for it, you’re the product.” Consumers, wittingly or unwittingly, pay for free services by giving companies access to their personal information and data logs.

Nobody says that anymore. Stacy-Ann Elvy’s excellent article, *Commodifying Consumer Data in the Era of the Internet of Things* explains why. No matter how much you pay, under current US law you’re the product if the company’s privacy policy says so. A company’s privacy policy typically is not in the contract consumers agree to and can be changed at any time. Elvy cites a study that estimates that by 2020 companies will be able to earn more profits by transferring and disclosing consumer Internet of Things (IoT) data than by selling IoT devices to the consumers themselves. This includes cars, typically the most expensive good most consumers ever purchase.[1]

Elvy shows how the Uniform Commercial Code (UCC), the Bankruptcy Code, and other commercial law facilitates the transfer and disclosure of consumer data. Under Article 9 of the UCC (hereafter “Article 9”), a company can increase its odds of obtaining loans on favorable terms by “securing” the loan with some asset the company has. To secure a loan means, roughly, to give the creditor the right to take the asset in the case of default, even if the debtor enters bankruptcy. That right is called a security interest. Databases of consumer information are often the most valuable asset a company has, so companies frequently obtain loans secured by these databases. The vexing scholarly question of who owns data about persons ends up not being terribly significant for secured transactions. Article 9 permits the creation of a security interest in an asset the debtor does not fully own, but the security interest would extend only to the rights the debtor has in the asset.[2] Databases including consumer data can also be part of a debtor’s estate in bankruptcy, and unless the privacy policy puts limitations on the ability of the company to transfer the databases, personal information can be transferred to others who lack any of the constraints the previous company may have represented to consumers about what they would do with the data.

In this way, Article 9 and the Bankruptcy Code amplify the impact of transfer of data and encourage its transfer. Corporations borrowing money and taking risks is the lifeblood of the American economy. A company would be putting itself at a disadvantage if it did not seek to borrow against its consumer data and take advantage of secured credit. And the more control a company gives itself over consumer data in its privacy policies, the more flexible it can be in the case of bankruptcy. The shadow of what might happen if bankruptcy were to occur influences creditor and investor behavior.

Article 9 and Bankruptcy Code predated what Elvy calls “the IoT data gold rush” by several decades, and the results of their interaction were not intended by policymakers. In fact, the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA) was intended (among many other things) to address consumer privacy concerns arising from data sales following several high-profile corporate bankruptcy cases. As Elvy describes in detail in the article, however, BAPCPA has many limitations, most notably its limitation to personally identifiable information (a dinosaur of a concept in an era where anonymized data can be readily re-identified)[3] and deference to privacy policies.

Elvy proposes two principal solutions to the consumer-unfriendly landscape she describes. She notes that deferring to the concept of notice and choice does not adequately protect consumers; it gives consumers no control over their data while increasing the ability of companies to profit from that same data. Elvy also suggests bright-line rules limiting

biometric data use in secured transactions and sale during bankruptcy because unlike other personal information like credit card numbers or addresses, fingerprints and eye scans cannot be changed.

Ultimately Elvy's most valuable contribution is the bringing together of the various sources of law that govern transfer of personal information. American law is characteristically sector and subject matter specific. However, looking at the problem of personal information transfer in the IoT economy exclusively as a commercial lawyer, a consumer protection lawyer, or even a privacy lawyer is not sufficient. Policymakers, scholars, and stakeholders should periodically take a big picture approach to see how different areas of the law fit together and reinforce (or undermine) each other.

There is a deeply held American cultural tendency to hold individuals responsible for fine print in contracts. However, Elvy's piece shows that when and how personal information is transferred between companies is largely not determined by contract law at all, but rather a combination of commercial law and sector-specific privacy law. Who has access to what type of data held by a company is a creature of commercial law, determined by the internal policies of that company and contractual relationships between debtor and creditor.

1. Matt McFarland, *Your Car's Data May soon Be More Valuable than the Car itself*, **CNN-Tech** (Feb. 7, 2017).
2. U.C.C. § 9-203(b) cmt. 6, **Am. Law Inst. & Unif. Law Comm'n** (1977).
3. Paul Ohm, *Broken Promises of Privacy, Responding to the Surprising Failure of Anonymization*, 57 **UCLA L. Rev.** 1701, 1703-05 (2010).

Cite as: Lauren Scholz, *Paying to be the Product*, JOTWELL (October 28, 2019) (reviewing Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 **B.C. L. Rev.** 423 (2018)), https://contracts.jotwell.com/paying-to-be-the-product/.