Good Fences Make Better Data Brokers

Author : Frank Pasquale

Date : April 25, 2014

Woodrow Hartzog, *Chain Link Confidentiality*, 46 **Georgia L. Rev.** 657 (2012) available at SSRN.

Since at least the early 2000s, privacy scholars have illuminated a fatal flaw at the core of many "notice and consent" privacy protections: firms that obtain data for one use may share or sell it to data brokers, who then sell it on to others, ad infinitum. If one can't easily prevent or monitor the sale of data, what sense does it make to carefully bargain for limits on its use by the original collector? The Federal Trade Commission and state authorities are now struggling with how to address the runaway data dilemma in the new digital landscape. As they do so, they should carefully consider the insights of Professor Woody Hartzog. His article, *Chain Link Confidentiality*, offers a sine qua non for the modernization of fair data practices: certain obligations should follow personal information downstream.

After 2013, it is impossible to ignore the concerns of privacy activists. The Snowden revelations portrayed untrammeled data collection by government. Jay Rockefeller's Senate Commerce Committee portrayed an out-of-control data gathering industry (whose handiwork can often be appropriated by government). America's patchwork of weak privacy laws are no match for the threats posed by this runaway data, which is used secretly to rank, rate, and evaluate persons, often to their detriment and often unfairly. Without a society-wide commitment to fair data practices, a dark era of digital discrimination is a real and present danger.

As Hartzog notes, "current privacy laws are too limited, subjective, or vague to effectively police the "downstream" use of information by third parties." This is a glaring weakness in privacy law, since a given bit of data might be redisclosed dozens or even hundreds of times in new digital data markets. Hartzog's approach would "use contracts to link recipients of personal information ," including in those contracts "(1) obligations and restrictions on the use of the disclosed information; (2) requirements to bind future recipients to the same obligations and restrictions; and (3) requirements to perpetuate the contractual chain." Like the viral licensing envisioned by Creative Commons, the "chain link confidentiality" approach is designed to effect a system of data transmission that balances the flexibility of private ordering with the stability of public law.

Hartzog's article highlights the importance of health privacy law for modeling new relationships of responsibility between data collectors, sellers, and subjects. As he observes, "The HIPAA Privacy Rules provide that, although only covered entities such as healthcare providers are bound to confidentiality, these entities may not disclose information to their business associates without executing a written contract that places the business associate under the same confidentiality requirements as the healthcare providers." These protections have been strengthened even further by HITECH (and the HIPAA Omnibus Rule of 2013), which impose statutory and regulatory duties on business associates and even their downstream contractors. The health privacy protections essentially "run with the data."

What property-like restrictions accomplish in the health data sphere, Hartzog wants to accomplish via contracts that would bind the recipients of data to terms like those imposed on the original collector. Not only would this help individuals get a handle on "runaway data;" it would also help promote the validity of research in the big data field by indicating the provenance of data. As Sharona Hoffman showed in the article "Big, Bad Data," if we can't tell the provenance of data, how can we adjust for or account for potential flaws or biases in it?

Both firms and data brokers increasingly try to integrate thousands of sources of information into profiles. The profiles are actionable, whether inside or outside the firm in which they are compiled. Runaway data can lead to cascading disadvantages. Once one piece of software has classified a person as a bad credit risk, a bad worker, or a poor

consumer, that attribute may appear with decision-making clout in other systems all over the economy. And it can dilute or distort findings that are increasingly based on promiscuous correlations within unstructured data sets. Chain link confidentiality would impose some baseline of order and attribution on the new data economy.

Runaway data poses a stark choice to data policymakers. Given the number of data breaches extant, it's only a matter of time before breachers start developing dark markets of information more sensitive than credit card numbers online. Are we going to allow datamongers to essentially act as "fences" for this stolen data? Or are we going to keep tabs on each "hop" of data from collector to broker to user and beyond—a bare predicate for keeping illicit or inaccurate data "fenced in?" Hartzog's chain links point us decisively toward the latter choice—a far better future for data practices.

Cite as: Frank Pasquale, *Good Fences Make Better Data Brokers*, JOTWELL (April 25, 2014) (reviewing Woodrow Hartzog, *Chain Link Confidentiality*, 46 **Georgia L. Rev.** 657 (2012) available at SSRN), http://cyber.jotwell.com/good-fences-make-better-data-brokers/.