HUFF POST TECH

THE INTERNET NEWSPAPER: NEWS BLOGS VIDEO COMMUNITY

James B. Rule
Distinguished Affiliated
Scholar, UC Berkeley Law School

A Privacy Right to Believe In

Posted: 04/10/2012

Unless you've spent the new millennium on another planet, you've noticed that details of your personal life are circulating more and more freely. Like water in those inscrutable underground rivers, data on your family circumstances -- or buying patterns, website visits or finances -- disappear at one point, only to surface in utterly different contexts. Typically these data-flows are the work of highly interested parties, bent on using your data to fine-tune their dealings with you.

These uses often bring rude surprises. Kevin Johnson of Atlanta, for example, recently received a letter from American Express informing him of a sharp reduction in the credit available on his card. "Other customers who have used their card at establishments where you recently shopped," the letter stated, "have a poor repayment history with American Express."

At least American Express drew the damning information from its own files. Companies can just as readily target customers on the basis of purchases or website visits with other organizations altogether. As law professor Lori Andrews recently noted in the *New York Times*, "If guitar players or divorcing couples are more likely to renege on their credit-card bills, then the fact that you've looked at guitar ads or sent an e-mail to a divorce lawyer may cause a data aggregator to classify you as less credit-worthy."

Practices like this offend elementary instincts of privacy. In everyday transactions, we willingly furnish information we believe needed to deliver what we're seeking -- our address, on taking out a subscription; medical history, when seeking care; or information about past credit use, to open a new credit account. When we disclose such data, we don't expect it to be captured and redirected for new and unintuitive purposes -- especially unfriendly ones.

But as more and more crucial relationships and transactions unfold over the internet, such expectations ring increasingly quaint. Big organizations troll cyberspace operating on the opposite principle: that personal information, once released for any purpose, belongs to whoever can capture it. Fabulous profits beckon to those who succeed in mobilizing just the right personal data to shape the "right" treatment for each consumer -- the right ads, the right terms for insurance or credit, or the right price for a given item, judged by what the consumer has been willing to pay in the past. In this quest, personal data are often most valuable in contexts farthest removed from where they are captured. If companies can make just the right connections, all they need to worry about is public indignation.

In nearly all the world's prosperous democracies, anticipation of such indignation has inspired adoption of privacy codes -- legislation and policy to establish personal rights in the treatment of data on one's self. These laws have achieved significant successes. But a salient disappointment has been failure to foster broad public understanding or engagement, with most citizens remaining vague on what protections the laws provide. As a result, struggles over who can do what with personal information have become the province of bureaucrats and specialists.

Now the Obama administration has weighed in with its own initiative. In February, it promulgated a Framework for a Consumer Privacy Bill of Rights, aiming at "clearer protection for consumers" against internet misuse of personal data. Privacy advocates publicly welcomed the spirit of the initiative. Off the record, they wondered whether it could succeed where other efforts have failed against pressures from industries fixated on personal information as their essential raw material.

The Framework is a wonkish document -- its more than fifty dense pages ensuring that few non-specialists will read it. Still, many of its stated goals are heartening. For example: companies should make it easy for consumers to block use of data they provide on the internet to target ads directed at them. Consumers should be able to withdraw permission for release of their personal data granted earlier. Companies aggregating and selling personal data without actually dealing directly with the public should be encouraged to disclose their policies. Worthy aims, all.

But interlarded with such statements are repeated affirmations of the value of activities supported by the very same privacy-eroding practices. The "reuse" (i.e., unauthorized capture) of personal information, the Framework states, represents "an important source of innovation." Targeted ads -- those based on data on the consumer -- "are worth significantly more than non-targeted ads." Available privacy-protecting mechanisms should be adapted to "... strike a balance with innovative uses of personal data...". Here one senses a quest for compromise between widespread public desires for control over one's own personal data, and industry appetites for precisely the opposite.

With such sharply conflicting principles in play, everything turns on the measures adopted to reconcile them. Here the Framework proposals do not inspire confidence. Rather than proclaiming broad and binding rights for consumers, they call for complex and indeterminate efforts at self-regulation -- new codes of conduct fashioned in "multistakeholder processes" bringing together industry representatives, technologists, privacy advocates, law enforcement agencies and others.

Different industry sectors are to constitute separate "stakeholder" groups, each framing its own privacy code. Individual companies, we are told, "may choose to adopt multiple codes of conduct to cover different lines of business." Once approved by the Federal Trade Commission, each code will be binding, though only on the companies explicitly adopting it. The FTC, the ultimate regulator, will be expected to look favorably on the activities of industry members who adhere to these codes.

Thus, a far-flung policy machine with countless moving parts. Taken at its word, the Framework could spawn dozens of codes -- different ones for social networking sites, presumably, or for vendors of personal data to advertisers, or for internet service providers. In each of these domains, no doubt, some players will reject the codes. Both these outliers and subscriber groups will remain subject to the oversight of the FTC. This is a vast agenda for any regulator.

Nor is it at all clear how strong the consumer options decreed by the "stakeholder" processes will be. Would companies like American Express be prevented from using data on where its customers use their cards to reduce the credit extended to them -- as in Kevin Johnson's case? Would companies remain free to supplement their own account data with personal data purchased from outside brokers to determine what treatment their customers will receive? At times the authors of the Framework imply that their aim is simply to put privacy-invading practices on record, leaving customers to assume what they call "responsibilities to protect their privacy as they engage in an increasingly networked society." In context, this suggests that companies may be free to pursue the most high-handed uses of consumers' data -- if only the latter are duly warned in advance.

Such strategies of encouraging consumers to protect their privacy piecemeal, by foregoing otherwise attractive uses of the internet, are extremely inauspicious. American consumers are indeed on record as desiring protection for their data. But few are prepared to stop each individual transaction in its tracks, research the detail of their options under the applicable privacy code, and scrap the transaction if those options appear unsatisfactory. Retailers, creditors, website operators and the like exploit this impatience by requiring customers to acquiesce to draconian warnings and "terms of service" at the last moment before transactions can go ahead. When was the last time you actually read one of these statements in detail before clicking on with your internet business?

In fact, the administration's complex and demanding regulatory project has things backwards. Instead of relying on industry self-restraint and intensive regulation from above to manage personal data once it has "escaped," we should reconsider who owns such information in the first place.

Imagine that everyone enjoyed property rights over commercial exploitation of his or her information -- as with mineral rights or water rights. Without explicit consent from the rights-holder, no party could trade in personal data, or use it to add value to their product or service -- e.g., for targeting ads on the internet. Such consent could be withheld categorically, granted indiscriminately, or predicated on payment of royalties. A right to punitive damages for unauthorized commercial use would provide ample incentive for compliance.

Here the enforcers of privacy obligations would be the rights-holders themselves, or their designated representatives. Establishment of the right would likely trigger formation of new companies dedicated to monitoring both authorized and unauthorized uses of personal data, and claiming compensation where the owner imposes this as a condition for use.

Who could fail to see the virtues of such an elegant and self-activating formula for privacy protection? Only the vast industries that now flourish by appropriating personal information without consent. For them, prospects of people's having an easy option to block commercialization of data on themselves will be about as appealing as a proposal for Steak Tartar at the Vegans' annual banquet. Creation of real, enforceable rights of this kind, industry interests will warn, will spoke the wheels of "innovation" -- crimping the cornucopia from which flow jobs, fortunes and a steady stream of contributions to electoral politics.

But establishing property in personal information would hardly have such drastic effects. What it would do would be to require all commercial users of personal data to make their activities acceptable to those whose privacy they compromise -- if those activities are to go ahead at all.

Best of all would be the effect on public consciousness. The notion that everyone owns the right to commercial exploitation of data on one's self is something that everyone could understand -- unlike the complex array of options likely to issue from the Obama Framework. Poll data suggest that the idea of ownership of one's own data would be hugely popular, rewarding any politician who seriously proposes it. The new right would make all citizens the ultimate judges of whether new uses of their data -- which now would really be "theirs" -- represented life-enhancing technological progress, or unwarranted invasion of personal space.