

TECHNOLOGY

A Grand Bargain to Make Tech Companies Trustworthy

Doctors and lawyers are prohibited from using clients' information for their own interests, so why aren't Google and Facebook?

JACK M. BALKIN AND JONATHAN ZITTRAIN OCT 3, 2016



Protestors at a rally for digital privacy in Berlin (THOMAS PETER / REUTERS)

We tell online services what we like, who we love, what we are doing, and where we live, work, and play. And they in turn provide us with a window to the world, shaping what we see and suggesting what we should do.

As we use these services, they learn more and more about us. They see who we are, but we are unable to see into their operations or understand how they use our data. As a result, we have to trust online services, but we have no real guarantees that they will not abuse our trust. Companies share information about us in any number of unexpected and regrettable ways, and the information and advice they provide can be inconspicuously warped by the companies' own ideologies or by their relationships with those who wish to influence us, whether people with money or governments with agendas.

To protect individual privacy rights, we've developed the idea of "information fiduciaries." In the law, a *fiduciary* is a person or business with an obligation to act in a trustworthy manner in the interest of another. Examples are professionals and managers who handle our money or our estates. An *information fiduciary* is a person or business that deals not in money but in information. Doctors, lawyers, and accountants are examples; they have to keep our secrets and they can't use the information they collect about us against our interests. Because doctors, lawyers, and accountants know so much about us, and because we have to depend on them, the law requires them to act in good faith—on pain of loss of their license to practice, and a lawsuit by their clients. The law even protects them to various degrees from being compelled to release the private information they have learned.

The information age has created new kinds of entities that have many of the trappings of fiduciaries—huge online businesses, like Facebook, Google, and Uber, that collect, analyze, and use our personal information—sometimes in our interests and sometimes not. Like older fiduciaries, these businesses have become virtually

indispensable. Like older fiduciaries, these companies collect a lot of personal information that could be used to our detriment. And like older fiduciaries, these businesses enjoy a much greater ability to monitor our activities than we have to monitor theirs. As a result, many people who need these services often shrug their shoulders and decide to trust them. But the important question is whether these businesses, like older fiduciaries, have legal obligations to *be* trustworthy. The answer is that they should.

To deal with the new problems that digital businesses create, we need to adapt old legal ideas to create a new kind of law—one that clearly states the kinds of duties that online firms owe their end users and customers. The most basic obligation is a duty to look out for the interests of the people whose data businesses regularly harvest and profit from. At the very least, digital businesses may not act like con men—inducing trust in end users and then actively working against their interests. Google Maps shouldn't recommend a drive past an IHOP as the "best route" on your way to a meeting from an airport simply because IHOP gave it \$20. And if Mark Zuckerberg supports the Democrat in a particular election, Facebook shouldn't be able to use its data analysis to remind its Democratic users that it's election day—while neglecting to remind, or actively discouraging, people it thinks will vote for Republicans.

The project of encouraging some accountability requires fairness in both directions—fairness to end users, and fairness to businesses, who shouldn't have new and unpredictable obligations dropped on them by surprise. The task also requires determining the proper scope of fiduciary duties—which may be different from those that apply to traditional fiduciaries like doctors and lawyers—and the remedies for

their violation. Finally, we have to persuade companies that these duties make sense, and give them reasons to accept that they are a new kind of fiduciary in the digital age.

A good starting point is a very different area of law: copyright. In the face of disputes about copyright and piracy that arose with the growth and spread of the internet, online intermediaries willingly took on new responsibilities in order to create a predictable business environment.

The U.S. Digital Millennium Copyright Act of 1998 created a safe harbor for businesses that followed its rules for when to take down allegedly infringing content. If an online business received notice from a copyright owner that content was infringing, it could avoid copyright liability by promptly removing the content; and if the original uploader responded by identifying him- or herself and claiming fair use, the content would be restored. The Digital Millennium Copyright Act was a political compromise: Businesses didn't have to accept the bargain that the DMCA offered them, but if they did, they were immune from copyright liability. Academics still grumble about some of the DMCA's details today, yet its basic features made it possible for online providers to welcome lots of outside content from their users without worrying that one wrong byte could spell a lawsuit. Businesses like YouTube and Facebook couldn't have developed without it.

Fast forward to today's difficult political environment. The public wants protection from potential abuses by online businesses that collect, analyze, and manipulate their personal data. But online businesses don't want to be hit with unexpected liability as privacy law takes unexpected turns. Currently there is a patchwork of state and

local laws about online privacy. Because of uncertainty, some of these laws end up being implemented nationwide. California, for example, requires companies who accidentally expose their customers' personal data to notify those customers of such potential breaches. While the California law requires such notifications to only customers in California, companies end up notifying everyone in order to avoid leaving any Californians out.

There is an opportunity for a new, grand bargain organized around the idea of fiduciary responsibility. Companies could take on the responsibilities of information fiduciaries: They would agree to a set of fair information practices, including security and privacy guarantees, and disclosure of breaches. They would promise not to leverage personal data to unfairly discriminate against or abuse the trust of end users. And they would not sell or distribute consumer information except to those who agreed to similar rules. In return, the federal government would preempt a wide range of state and local laws.

Compliance with state legislation and common law—and the threat of class-action suits and actions by state attorneys general—have become sufficiently burdensome that some companies, such as Microsoft, already have indicated that they are open to comprehensive federal privacy legislation that would preempt conflicting state regulation. Congress could respond with a “Digital Millennium Privacy Act” that offers a parallel trade-off to that of the DMCA: accept the federal government's rules of fair dealing and gain a safe harbor from uncertain legal liability, or stand pat with the status quo.

The DMPA would provide a predictable level of federal immunity for

those companies willing to subscribe to the duties of an information fiduciary and accept a corresponding process to disclose and redress privacy and security violations. As with the DMCA, those companies unwilling to take the leap would be left no worse off than they are today—subject to the tender mercies of state and local governments. But those who accept the deal would gain the consistency and calculability of a single set of nationwide rules. Even without the public giving up on any hard-fought privacy rights recognized by a single state, a company could find that becoming an information fiduciary could be far less burdensome than having to respond to multiple and conflicting state and local obligations.

Of course, the value of this trade-off to end users depends on how well Congress respects the central idea of an information fiduciary—the duty to use personal data in ways that don't betray end users and harm them. But this grand bargain offers a clear and plausible path to implementation that can benefit all sides in a digital world that is still evolving.

We want to hear what you think about this article. [Submit a letter](#) to the editor or write to letters@theatlantic.com.



