The New York Times https://nyti.ms/2xRVtVx

TECHNOLOGY

Seriously, Equifax? This Is a Breach No One Should Get Away With

Farhad Manjoo

STATE OF THE ART SEPT. 8, 2017

Equifax, you had one job. Your only purpose as a corporation, the reason you were created and remain a going concern, is to collect and maintain people's most private financial data.

Now you have fallen down on your only job — and spectacularly so. Hackers penetrated the spectral gauze of security surrounding your website, and over the course of nearly two months, they made away with the personal information of as many as 143 million Americans. It is the most important financial data available on any of us — our names, birth dates, Social Security numbers, home addresses and in some instances a lot more — and it was just sitting there on your site, all but wrapped up in a red bow.

So, Equifax, I have to ask: Now that you have failed at your one job, why should you be allowed to keep doing it?

If a bank lost everyone's money, regulators might try to shut down the bank. If an accounting firm kept shoddy books, its licenses to practice accounting could be revoked. (See how Texas pulled Arthur Andersen's license after the Enron debacle.)

So if a data-storage credit agency loses pretty much everyone's data, why should it be allowed to store anyone's data any longer?

Here's one troubling reason: Because even after one of the gravest breaches in history, no one is really in a position to stop Equifax from continuing to do business as usual. And the problem is bigger than Equifax: We really have no good way, in public policy, to exact some existential punishment on companies that fail to safeguard our data. There will be hacks — and afterward, there will be more.

Experts said it was highly unlikely that any regulatory body would shut Equifax down over this breach. As one of the nation's three major credit-reporting agencies, which store and analyze consumers' financial history for credit decisions, it is likely to be considered too central to the American financial system; Equifax's demise would both reduce competition in the industry and make each of the two survivors a bigger target. Raj Joshi, an analyst at Moody's, said in a note to investors that Equifax was likely to be fine, as "the impact of the security breach will only modestly erode its solid credit metrics and liquidity."

The two regulators that do have jurisdiction over Equifax, the Federal Trade Commission and the Consumer Financial Protection Bureau, declined to comment on any potential punishments over the credit agency's breach.

Consumers also have piddling rights over how Equifax may continue to use their credit data. "There's nothing in any statute or anything else that allows you to ask Equifax to remove your data or have all your data disappear if you say you no longer trust it," said John Ulzheimer, a consumer credit expert who worked at Equifax in the 1990s.

But wait, it gets worse. You also can't prevent Equifax from getting any more of your data.

"You might be able to casually say to your bank that you don't want them to give information to Equifax anymore, but I don't know that's going to have an effect on anything," Mr. Ulzheimer said. "You don't control the rules of engagement."

This isn't just about Equifax. We live in the age of Big Data. We have allowed, mostly passively, the emergence of huge and exquisitely detailed databases full of information about all of us. Financial companies, technology companies, medical organizations, advertisers, insurers, retailers and the government — thanks to technology, they can all now maintain massive warehouses of information on just about everyone alive.

Yet in many cases these data stores are only lightly regulated, and compared with the scale of the data compromised, the punishment for breaches is close to nonexistent. There is no federally sanctioned insurance or audit system for data storage, the way the Federal Deposit Insurance Corporation provides insurance and a wind-down process for banks after losses. For many types of data, there are few licensure requirements on organizations seeking to house personally identifiable information.

In many cases, terms-of-service documents indemnify companies against legal consequences for breaches. In fact, according to the Consumer Financial Protection Bureau, the credit-reporting service that Equifax is offering customers affected by this breach requires people to waive their legal rights to sign up.

"It is troubling that Equifax is forcing people to waive legal rights in order to receive fraud monitoring after the company's breach put their personal information at risk," Samuel Gilford, a bureau spokesman, said in a statement.

With all these ways of mitigating fallout from attacks, breaches keep happening — and in almost all cases, even when the data concerns tens or hundreds of millions of people, the companies that were hacked continue to operate anyway. See Yahoo, for instance, which hackers hit for 500 million accounts, and then again for one billion accounts — but which is still in business.

You might argue that not every data hack deserves a corporate death penalty. That's reasonable. Neither Target nor Home Depot, for instance, is primarily in the business of storing your data. Both were hit in hacks for millions of people's credit-card data, but after they offered some penance and promised to fix their systems, it's not unreasonable that you would continue to shop at their stores.

And you might argue that hacking is impossible to avoid no matter how many security measures companies take. Unforeseen calamities happen in complex systems — banks are robbed, airliners crash, car engines blow up.

But the Equifax case is troubling because neither of these arguments applies.

"If it fails at its one job, it really is quite hard to justify using it again," said Steven S. Rubin, a lawyer who specializes in cybersecurity law at the firm Moritt Hock & Hamroff.

And if it really is impossible to safeguard against hacking, Equifax's continued existence becomes even more untenable. On its website, Equifax boasts that it "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."

But if we are now conceding that hacks just happen and no one can stop them — well, here's a crazy thought: Maybe let's not allow any company to house all this data. I contacted Equifax to ask about this, but did not hear back.

What is likely to happen is just the opposite of a harsh punishment. The more data a company has on us, the less likely it is that a breach will put the company in any real danger, because its very size protects it.

"Smaller companies have more of an existential concern," Mr. Rubin said. "When a small law firm or accounting firm loses people's data, they're going to be in big trouble, because you can go down the street and find someone else."

But Equifax? It has more of your data than just about anyone else. So even after losing it, it will probably keep just getting more.

Email: farhad.manjoo@nytimes.com; Twitter:@fmanjoo

A version of this article appears in print on September 9, 2017, on Page B1 of the New York edition.
