Data Is a Toxic Asset - Schneier on Security

Published by

Estimated reading time
6 min
Added on
2024-01-31
Address
https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html

Data Is a Toxic Asset - Schneier on Security

Thefts of personal information aren’t unusual. Every week, thieves break into networks and steal data about people, often tens of millions at a time. Most of the time it’s information that’s needed to commit fraud, as happened in 2015 to Experian and the IRS.

Sometimes it’s stolen for purposes of embarrassment or coercion, as in the 2015 cases of Ashley Madison and the US Office of Personnel Management. The latter exposed highly sensitive personal data that affects security of millions of government employees, probably to the Chinese. Always it’s personal information about us, information that we shared with the expectation that the recipients would keep it secret. And in every case, they did not.

The telecommunications company TalkTalk admitted that its data breach last year resulted in criminals using customer information to commit fraud. This was more bad news for a company that’s been hacked three times in the past 12 months, and has already seen some disastrous effects from losing customer data, including £60 million (about $83 million) in damages and over 100,000 customers. Its stock price took a pummeling as well.

People have been writing about 2015 as the year of data theft. I’m not sure if more personal records were stolen last year than in other recent years, but it certainly was a year for big stories about data thefts. I also think it was the year that industry started to realize that data is a toxic asset.

The phrase “big data” refers to the idea that large databases of seemingly random data about people are valuable. Retailers save our purchasing habits. Cell phone companies and app providers save our location information.

Telecommunications providers, social networks, and many other types of companies save information about who we talk to and share things with. Data brokers save everything about us they can get their hands on. This data is saved and analyzed, bought and sold, and used for marketing and other persuasive purposes.

And because the cost of saving all this data is so cheap, there’s no reason not to save as much as possible, and save it all forever. Figuring out what isn’t worth saving is hard. And because someday the companies might figure out how to turn the data into money, until recently there was absolutely no downside to saving everything. That changed this past year.

What all these data breaches are teaching us is that data is a toxic asset and saving it is dangerous.

Saving it is dangerous because it’s highly personal. Location data reveals where we live, where we work, and how we spend our time. If we all have a location tracker like a smartphone, correlating data reveals who we spend our time with—including who we spend the night with.

Our Internet search data reveals what’s important to us, including our hopes, fears, desires and secrets. Communications data reveals who our intimates are, and what we talk about with them. I could go on. Our reading habits, or purchasing data, or data from sensors as diverse as cameras and fitness trackers: All of it can be intimate.

Saving it is dangerous because many people want it. Of course companies want it; that’s why they collect it in the first place. But governments want it, too. In the United States, the National Security

Agency and FBI use secret deals, coercion, threats and legal compulsion to get at the data. Foreign governments just come in and steal it. When a company with personal data goes bankrupt, it’s one of the assets that gets sold.

Saving it is dangerous because it’s hard for companies to secure. For a lot of reasons, computer and network security is very difficult. Attackers have an inherent advantage over defenders, and a sufficiently skilled, funded and motivated attacker will always get in.

And saving it is dangerous because failing to secure it is damaging. It will reduce a company’s profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges.

All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company’s computers and networks. The data is vulnerable, and the company is vulnerable. It’s vulnerable to hackers and governments. It’s vulnerable to employee error. And when there’s a toxic data spill, millions of people can be affected. The 2015 Anthem Health data breach affected 80 million people. The 2013 Target Corp. breach affected 110 million.

This toxic data can sit in organizational databases for a long time. Some of the stolen Office of Personnel Management data was decades old. Do you have any idea which companies still have your earliest e-mails, or your earliest posts on that now-defunct social network?

If data is toxic, why do organizations save it?

There are three reasons. The first is that we’re in the middle of the hype cycle of big data. Companies and governments are still punch-drunk on data, and have believed the wildest of promises on how valuable that data is. The research showing that more data isn’t necessarily better, and that there are serious diminishing returns when adding additional data to processes like personalized advertising, is just starting to come out.

The second is that many organizations are still downplaying the risks. Some simply don’t realize just how damaging a data breach would be. Some believe they can completely protect themselves against a data breach, or at least that their legal and public relations teams can minimize the damage if they fail. And while there’s certainly a lot that companies can do technically to better secure the data they hold about all of us, there’s no better security than deleting the data.

The last reason is that some organizations understand both the first two reasons and are saving the data anyway. The culture of venture-capital-funded start-up companies is one of extreme risk taking. These are companies that are always running out of money, that always know their impending death date.

They are so far from profitability that their only hope for surviving is to get even more money, which means they need to demonstrate rapid growth or increasing value. This motivates those companies to take risks that larger, more established, companies would never take. They might take extreme chances with our data, even flout regulations, because they literally have nothing to lose. And often, the most profitable business models are the most risky and dangerous ones.

We can be smarter than this. We need to regulate what corporations can do with our data at every stage: collection, storage, use, resale and disposal. We can make corporate executives personally liable so they know there’s a downside to taking chances. We can make the business models that involve massively surveilling people the less compelling ones, simply by making certain business practices illegal.

The Ashley Madison data breach was such a disaster for the company because it saved its customers' real names and credit card numbers. It didn't have to do it this way. It could have processed the credit card information, given the user access, and then deleted all identifying information.

To be sure, it would have been a different company. It would have had less revenue, because it couldn't charge users a monthly recurring fee. Users who lost their password would have had more trouble re-accessing their account. But it would have been safer for its customers.

Similarly, the Office of Personnel Management didn't have to store everyone's information online and accessible. It could have taken older records offline, or at least onto a separate network with more secure access controls. Yes, it wouldn't be immediately available to government employees doing research, but it would have been much more secure.

Data is a toxic asset. We need to start thinking about it as such, and treat it as we would any other source of toxicity. To do anything else is to risk our security and privacy.

This essay previously appeared on CNN.com.

Tags: breaches, data retention, databases, doxing, essays, fraud, hacking, laws, risks

Produced by wallabag with tcpdf

Please open an issue if you have trouble with the display of this E-Book on your device.