Harvard Business Review

REPRINT H04PY8
PUBLISHED ON HBR.ORG
JANUARY 03, 2019

ARTICLE
SECURITY & PRIVACY

Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies.

by Andrew Burt

Harvard Business Review

SECURITY & PRIVACY

Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies.

by Andrew Burt

JANUARY 03, 2019

COLIN ANDERSON PRODUCTIONS PTY LTD/GETTY IMAGES

2018 has been the year of privacy. News of Facebook's exposure of tens of millions of user accounts to data firm Cambridge Analytica broke in March — a scandal that was only compounded by recent news that the tech giant shared even more private data through hidden agreements with other companies. Then in May, the European Union's General Data Protection Regulation, the world's most stringent privacy law, came into effect. By the end of the year, even Apple's and Microsoft's CEOs were calling for new national privacy standards in the United States.

It's not just a coincidence that privacy issues dominated 2018. These events are symptoms of larger, profound shifts in the world of data privacy and security that have major implications for how organizations think about and manage both.

So what, exactly, is changing?

Put simply, privacy and security are converging, thanks to the rise of big data and machine learning. What was once an abstract concept designed to protect expectations about our own data is now becoming more concrete, and more critical — on par with the threat of adversaries accessing our data without authorization.

More specifically, the threat of *unauthorized access* to our data used to pose the biggest danger to our digital selves — that was a world in which we worried about intruders attempting to get at data we wanted private. And it was a world in which privacy and security were largely separate functions, where privacy took a backseat to the more tangible concerns over security. Today, however, the biggest risk to our privacy and our security has become the threat of *unintended inferences*, due to the power of increasingly widespread machine learning techniques. Once we generate data, anyone who possesses enough of it can be a threat, posing new dangers to both our privacy and our security.

These inferences may, for example, threaten our anonymity — like when a group of researchers used machine learning techniques to identify authorship of written text based simply on patterns in language. (Similar techniques have been used to identify software developers based simply on the code they've written.)

These inferences might reveal information about our political leanings — like when researchers used the prevalence of certain types of cars in Google's Street View image database to determine local political affiliations.

Or these inferences might also indicate intimate details about our health — like when researchers used online search history to detect neurodegenerative disorders such asAlzheimer's.

So what does a world look like when privacy and security are focused on preventing the same harms?

To start with, privacy will no longer be the merely immaterial or political concept it once was. Instead, privacy will begin to have substantial impacts on businesses' bottom lines — something we

began to see in 2018. Facebook, for example, lost a whopping $119 billion in market capitalization in the wake of the Cambridge Analytica scandal because of concerns over privacy. Polls show that consumers are increasingly concerned about privacy issues. And governments around the world are reacting with new privacy legislation of their own.

Within organizations, this convergence also means that the once clear line between privacy and security teams is beginning to blur — a trend that businesses in general, and security and privacy practitioners in particular, should embrace. From a practical perspective, this means that legal and privacy personnel will become more technical, and technical personnel will become more familiar with legal and compliance mandates. The idea of two distinct teams, operating independent of each other, will become a relic of the past.

And this means individuals and governments alike should no longer expect consent to play a meaningful role in protecting our privacy. Because the threat of unintended inferences reduces our ability to understand the value of our data, our expectations about our privacy — and therefore what we can meaningfully consent to — are becoming less consequential. Being *surprised* at the nature of the violation, in short, will become an inherent feature of future privacy and security harms.

This is precisely why the recent string of massive data breaches, from the Marriott breach that impacted 500 million guests to the Yahoo breach that affected 3 billion users, are so troubling. The problem isn't simply that unauthorized intruders accessed these records at a single point in time; the problem is all the unforeseen uses and all the intimate inferences that this volume of data can generate going forward. It is for this reason that legal scholars such as Oxford's Sandra Wachter are now proposing legal constraints around the ability to perform this type of pattern recognition at all.

Once described by Supreme Court Justice Louis Brandeis as "the right to be let alone," privacy is now best described as the ability to control data we cannot stop generating, giving rise to inferences we can't predict.

And because we create more and more data every day — an estimated 2.5 quintillion bytes of it — these issues will only become more pressing over time.

If we thought that 2018 was dominated by privacy concerns, just wait until 2019.

Andrew Burt is chief privacy officer and legal engineer at Immuta.