The New York Times | https://nyti.ms/2xYvJZe

Opinion | OP-ED CONTRIBUTORS

The End of Privacy

By ANDREW BURT and DAN GEER OCT. 5, 2017

We learned on Tuesday that three billion Yahoo email accounts were compromised in 2013. In early September, it was Equifax's 143 million credit reports. Just a few months before that, we learned 198 million United States voter records were leaked online in June.

Given the constant stream of breaches, it can be hard to understand what's happening to our privacy over time. Two dates — one recent and one long ago — help explain this: Dec. 15, 1890, and May 23, 2017, are the two most important days in the history of privacy. The first signifies its creation as a legal concept, and the latter, while largely overlooked at the time, symbolizes something close to its end.

On Dec. 15, 1890, the future Supreme Court Justice Louis Brandeis and the attorney Samuel Warren published an article in the Harvard Law Review, "The Right to Privacy," which argued for the recognition of a new legal right to, in their words, "be let alone." The article was spurred by a new technology called the instantaneous photograph, which made it possible for anyone walking down the street to find their image in the newspaper the next day.

That argument forms the basis for the way we approach our rights to privacy to this day. The proposed right to "be let alone" made a fundamental distinction between being *observed,* which can accompany any act made in public, versus being

identified, a separate and more intrusive act. We consent to be observed constantly; we rarely consent to be identified.

Today, however, this distinction has eroded, thanks to the rapid advance of digital technologies and the accompanying rise of the field broadly called data science. What we have thought of as privacy is dying, if not already dead.

For example, in 2012, the United States Supreme Court in U.S. v. Jones evaluated the constitutionality of police investigators' placement of a GPS tracker on the Jeep of a suspected drug trafficker to monitor his movements for a month without a warrant. The court determined that this tracking of the defendant's public movements had crossed the line from public observation to private identification and had therefore violated his expectations of privacy. It held that sustained monitoring, even in public, exceeded the bounds of simple observation and that the government's surveillance was therefore unconstitutional.

Just five years later, this argument makes much less sense: "Sustained monitoring" is now a part of our digital lives. And that's why what happened on May 23, 2017, is so important.

On that day, Google announced that it would begin to tie billions of credit card transactions to the online behavior of its users, which it already tracks with data from Google-owned applications like YouTube, Gmail, Google Maps and more. Doing so allows it to show evidence to advertisers that its online ads lead users to make purchases in brick-and-mortar stores. Google's new program is now the subject of a Federal Trade Commission complaint filed by the Electronic Privacy Information Center in late July.

Google may be the first to formally make this link, but it is hardly alone. Among technology companies, the rush to create comprehensive offline profiles of online users is on, driven by the need to monetize online services offered free.

In practice, this means that we can no longer expect a meaningful difference between observability and identifiability — if we can be observed, we can be identified. In one recent study, for example, a group of researchers showed that aggregate cellular location data — the records generated by our cellphones as they

anonymously interact with nearby cell towers — can identify individuals with 73 percent to 91 percent accuracy.

And even without these advanced methods, finding out who we are and what we like and do has never been easier. Thanks to the trails created by our continuous online activities, it has become nearly impossible to remain anonymous in the digital age.

So what to do?

The answer is that we must regulate what organizations and governments can actually do with our data. Simply put, the future of our privacy lies in how our data is *used,* rather than how or when our data may be *gathered*. Excepting those who opt out of the digital world altogether, controls on data gathering is a lost cause.

This is part of the approach now being taken by European regulators. One of the cornerstones of the European Union's new regulatory framework for data, known as the General Data Protection Regulation, or G.D.P.R., is the idea of purpose-based restrictions on data. In order for an organization or public authority to use personal data gathered in the European Union, it must first specify what that data is going to be used for. The G.D.P.R. sets forth six broad categories of acceptable purposes, including when an individual has directly consented to a specific use for the data to when data processing is necessary for the public interest. If data is issued for an unauthorized purpose, legal liability ensues. The G.D.P.R. is far from perfect, but it is on to something big.

This method stands in stark contrast to the way data is protected in the United States, which might best be characterized as a "collect data first, ask questions later" approach. Sure, American technology companies disclose their privacy policies in a terms-of-service statement, but these disclosures are often comically ambiguous and widely misunderstood.

Many privacy advocates will no doubt find it hard to stomach that the way we think about protecting our data is outdated. But if we are to maintain the ability to assert control over the data we generate, we must also admit that our past ideas of what it means to be "let alone" no longer apply.

Andrew Burt is chief privacy officer and legal engineer at Immuta. Dan Geer is chief information security officer at In-Q-Tel.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTopinion), and sign up for the Opinion Today newsletter.

A version of this op-ed appears in print on October 6, 2017, on Page A27 of the New York edition with the headline: How Privacy as We Knew It Died.
