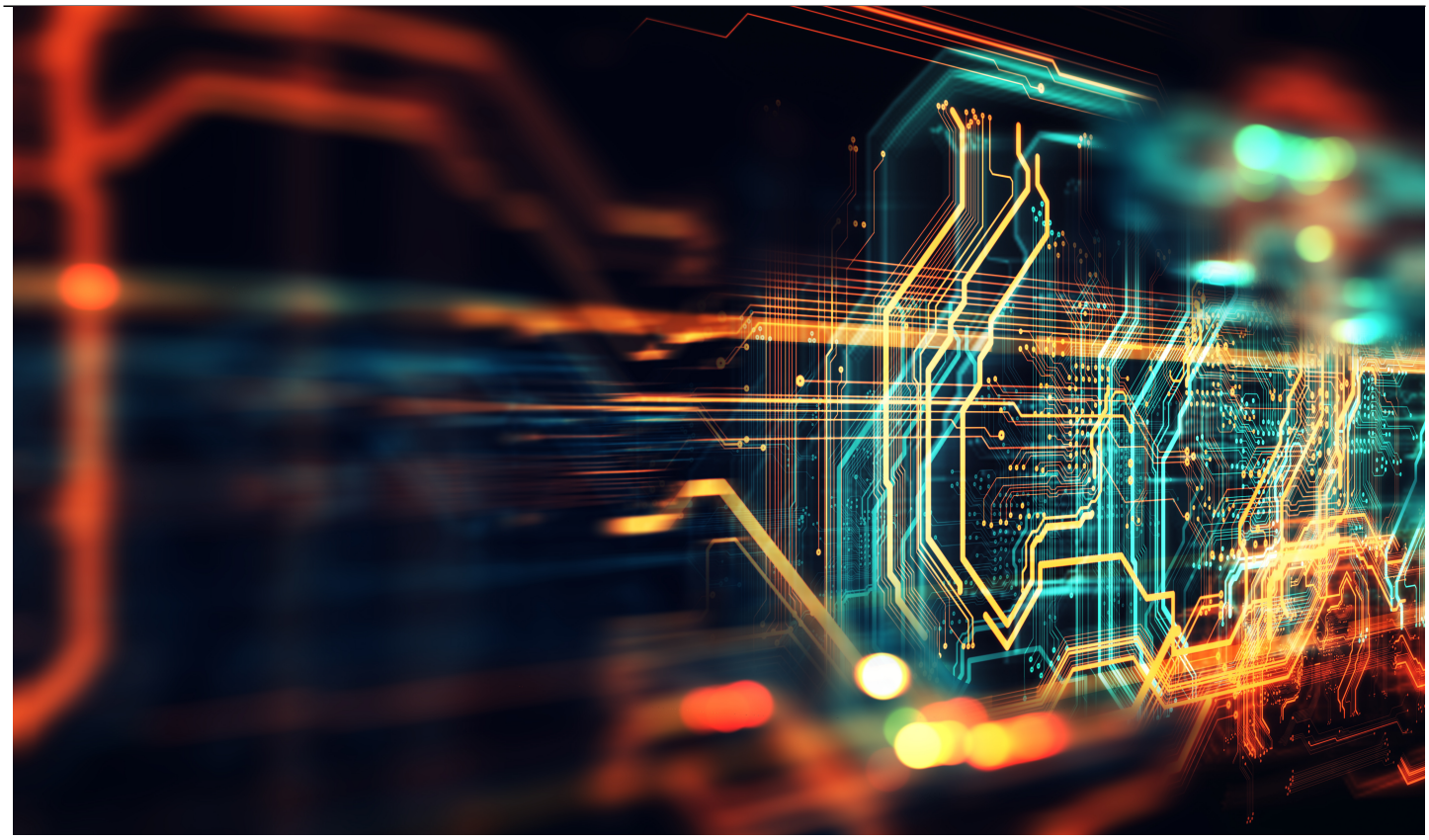
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Real Threats to Personal Privacy

Technology, Privacy, and eCommerce



At this point, it’s hard to say whether privacy should be placed on the endangered or the extinct species list. Over the past several decades, so many of us have negligently dropped or bartered away bits and bytes about ourselves or entrusted them to people who have betrayed that trust. The horses may not only have left the corral, but already stampeded over a cliff.

Many governments are trying to protect this increasingly rare commodity. But most officials don’t seem to fully understand the situation or are in denial about how bad it has become.

Let’s start with Wikipedia’s definition: “Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.” This idea of maintaining some control over what parts of your own personal information is known by others is critical. And yet, it is this very ability to choose what aspects of yourself should be known by others that is being so rapidly eroded.

The choosing part has become so difficult because when it comes to our online activities, we often don’t know enough to make an informed decision. Let’s start with the privacy policies many of us have helped our companies to draft. Has our goal in every case been to make those policies as clear and simple to understand to lay people as possible, or has it been to conservatively address liability concerns and check the right boxes to the point where only lawyers can really understand what they say?

I recently installed new operating system versions on my mobile phone, my watch, my tablets, and my computers. In each case, I was required to consent to the licensing agreement, which almost certainly included privacy terms.

“Almost certainly”? Yes, because I didn’t actually read them. Now, I am both a lawyer and a technologist. I have read so many of these darn things, and they are so boring and contain so much boilerplate, that if I think I have read such agreements by the same company before and found them acceptable, I carelessly assume the new ones will be too. Plus, I know that if they are really egregious and if push comes to shove, they will probably be found unenforceable.

On the other hand, my wife, children, siblings, and friends (and most of the people you know, too) are neither lawyers nor technologists. They never read privacy policies, licensing agreements, or anything else if it is possible to take the easier path of simply clicking a button, if that will allow them easier access to something on a device or online that they think they want. The danger of this is not that your company will use this habit to erode privacy. It is that some companies will do so.

It goes much farther than that. Most people have no idea how valuable their personal information is and therefore how carefully they should guard it. Or from whom they should be guarding it. When most people think of threats to privacy, they think of criminal hackers or governmental surveillance.

But right now, one of the biggest threat vectors is that most of the internet economy runs on advertising; advertising runs on targeted ads; and targeted ads run on what many properly informed people would conclude is information they would prefer to keep private.

Google, Facebook, and Amazon are, without question, the most powerful denizens of the world wide web.

They provide “free” services that millions of people use, while making enormous amounts of money through advertising. The reason they can demand the fees they do from advertisers is that they have collected the best information for targeting ads that the world has ever seen.

For the past several decades this has largely been done by way of cookies, and that is still the primary focus of many lawmakers. However, data miners and brokers are far more sophisticated now. As in so many other areas, the emphasis now is on using data analytics.

I know I’ve used this story before, but here is a good general-purpose illustration about how this kind of “big data” (aka data analytics) correlation works.

Like many retailers, Target collects a lot of data about customer purchasing habits. (This is one of the main reasons stores provide “loyalty” cards.) But at a certain point, Target and other retailers realized that they could use data analytics to better target (pun intended) what their customers might want. In many cases, the conclusion drawn from the data being correlated would not have seemed intuitive to humans. This was true in a well-publicized case in which Target found that certain purchases not obviously related to pregnancy nevertheless were good indicators that specific customers might be interested in pre- and post-natal merchandise coupons. Here is how Charles Duhigg described a particular incident for the New York Times:

> As [Target’s] computers crawled through the data, [Target] was able to identify about 25 products that, when analyzed together, allowed [them] to assign each shopper a “pregnancy prediction” score… About a year after [Target] created [its] pregnancy-prediction model, a man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry, according to an employee who participated in the conversation [that Target had implied his 16-year-old, unmarried daughter was pregnant].

> [On a follow up call several days later], though, the father was somewhat abashed. “I had a talk with my daughter,” he said. “It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August. I owe you an apology.”

The lesson here is that tracking our online activities provides similar data sets to advertisers and others that could be used to obtain certain insights into our private affairs.

Whenever we go on the internet, our devices provide certain data characteristics that can be identified by the websites we visit. The specifications of your personal computer or device, the browser and other software you use, the fonts you have installed, and other many clues make up a unique profile that, statistically, no other computer is likely to match. This unique profile, called a “digital fingerprint,” can be used to identify your devices and track your movement within and across websites, even without the use of cookies. Since this profile data isn’t stored on your computer, there’s no way for you to delete it. In the meantime, we are getting close to the point where the people we trust the least will have the largest and most accurate collection of personal information about us. Short of going off the grid, it is hard to see how this privacy apocalypse can be prevented. The good news is that some very smart people are working on the problem. In the meantime, one thing we can do as lawyers for our companies is to understand applicable privacy laws, how our companies collect and intend to use customer and employee information, how that information is secured, and what the risks to our companies are if the information is abused. And, we can try to write the kind of privacy policies that will help our customers and other stakeholders really understand what they are agreeing to give up.

NOTES

1 If this sounds like what has been happening in climate change, don’t be surprised. The same human tendencies toward inertia, greed, ignorance, laziness, and confirmation bias are working hard to ensure that radical change won’t happen anytime soon.

2 It sometimes seems ironic that the people being exploited by these companies are called “users” when they themselves are the ones being used.

3 How Companies Learn Your Secrets

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant