Privacy Makes a Comeback

4.12.2018

I would categorize the Cambridge Analytica incident/breach in a similar fashion to the Edward Snowden revelations in that the Snowden revelations that awakened the world—and specifically the EU—to the extent of nation-state monitoring (in the Snowden case, it was the US's monitoring activities, but don't think for a second that every other country that was outraged at our monitoring wasn't doing the very same thing to us and others) that ultimately resulted in the collapse of the US-EU Safe Harbor self-certification program, the rise of the temporary fix with the Privacy Shield and now the soon-to-be-implemented General Data Protection Regulation. All of this furor over the loss of privacy and the "theft" of personal data must be placed into context.

Privacy rights were gaining a strong foothold in the US until 911 happened. After that, the swing was toward security at the risk of losing certain rights to privacy (this was the US PATRIOT Act, signed into law within 6 weeks of the 911 attacks (remember the outrage of librarians having to turn over the titles of books people checked out from public libraries?).

With the rise of Social Media apps in the mid-2000's (My Space, Facebook, YouTube, LinkedIn), there was no real governance over what these companies could do or over what information these companies could collect. As one who had been drafting website privacy policies since the mid-1990's, I was well aware of what laws existed to protect privacy (next to none). California broke new ground in 2003 with the nation's first data breach law. Other states quickly followed, and then there were a handful of holdouts for nearly fifteen years, until just in the past 30 days, South Dakota and finally Alabama joined the rest of the country with data breach laws, requiring that state residents need to be notified when their personally identifiable information has been subjected to unauthorized access.

Related Services

Cybersecurity and Privacy Specialty Team

Emerging Technology Specialty Team

In the past four or five years, private companies have been benefiting from the great advances in both computing speeds and cheap storage that have aligned with the development of advanced algorithms, capable of determining likes, dislikes, and soon-to-be-likes from a myriad of data scraped from Social Media sites by data aggregators. In those years, I would often say that we had more to fear from private companies (because they lacked any regulation) than from the government (which at least must adhere to the Constitution). Remember Facebook's IPO when the big concern was that only its web application was monetized? At that time, Facebook's mobile app was not. That changed quickly.

So here we are today, and it's no surprise how we got here. Self-regulation is great if we are all guided by moral principles, fairness, integrity, and honesty. That's not how competitive business works, however. Unless regulations are in place to force adherence (via enforcement) on those who conduct their business in the grey zone, you will have situations such as Cambridge Analytica.

There are many moving parts in the Facebook story, and there is no simple answer. The big deal these days is to monetize the data that we all leave behind every time we touch our "connected" devices. Companies are there to earn money for their shareholders but consumers don't want to pay $5/month for ad-free apps, so we are left with a model where consumers unwittingly—but voluntarily when they consent to the privacy policy that allows it—give up their data for social media companies to use to sell ads.

Where does this lead us? I'm thinking that we in the US may swing to some sort of GDPR regulation. Apple and Amazon are clearly headed that way, Facebook, too—it's an easier model than trying to parse out whether your consumer is "in the Union" or anywhere else in the world.

Claudia Rast
734.213.3431
rast@butzel.com