CULHANE MEADOWS PLLC
Big Law for the New Economy®

Many Privacy Practices that are Still Surprisingly Legal in the U.S.

By Kim A. Verska
January 28, 2021

Countries all over the world are passing laws regulating the privacy and security of personal data, but thanks to a largely deadlocked Congress, the US still lacks one national law. Unlike the EU and many other countries, the US has never subscribed to the view that the right to control one's own data is at its core a "fundamental" human right. Instead, we view personal data as an asset that can be exchanged for free services (such as when you browse online content without paying a subscription), or that can be bargained away by "consent" buried in non-negotiable terms and conditions that you must agree to in order to buy products or services online. The modern-day US economy is built upon, and is dependent on, this concept of "data as value" and current legal frameworks support this foundation. While this has led to a flourishing of the Internet, it has also led to a situation for US consumers described rather well in 1999 by Scott McNealy, founder of Sun Microsystems: "you have no privacy. Get over it."

One party control of Washington, international pressure, and increasing state regulatory action may signal a new era of change. But it will likely be slow to materialize – the world of data privacy is complex and the group of well-funded actors that benefit most from the current legal framework in the U.S. is large. Nonetheless, to take stock of the current state of affairs, it's worthwhile to review where we stand in terms of data privacy law as we begin 2021.

Among the consumer data that companies have recently been found to routinely sell to third parties while staying within the letter of U.S. law include: location data from your telco provider (recently mostly curtailed); data about your health conditions both from HIPAA-regulated healthcare providers (in "anonymized" form, but still capable of being reverse-engineered to identify you) and from app providers not covered by HIPAA; and data from your profile and use of social media, such as famously revealed in the Cambridge Analytica scandal (Facebook and your profile). These practices are so normalized in U.S. companies that the only potential disruptor can sometimes be an investigative reporter bringing a disturbing story to light. This was the case in the hot-off-the-presses case by the FTC against app-provider Flo Health for selling the "intimate information" of users reflecting on their fertility and personal health tracking. In that case, a Wall Street Journal reporter brought the case to the attention of the Federal Trade Commission (FTC), and it was only because this data-sharing violated the language of the company's privacy policy that the FTC was able to take action. But given the impenetrability of many legally accurate privacy notices these days, it could have ended differently with no FTC action at all and consumers blissfully unaware of this happening.

You may be surprised by some of the above, and you might well ask "how can this be legal"? The answer lies within the patchwork that is data privacy law in the U.S. At present, meaningful protection is extended only to consumers dealing with companies in certain sectors (banking, healthcare, telecommunications, to name a few), that engage in certain regulated activities (texting/robocalling, targeting websites to children, etc.), and where the consumer's data falls within the narrow categories of highly sensitive data. Most states have laws protecting Social Security Numbers from wrongful use, and credit card companies have done a good job of ensuring that your credit card data is encrypted in processing and storage (In this article, I'm going to refer to the more regulated areas described in this paragraph above, and the specific laws mentioned below, as "Limited-Scope Privacy Laws"). However, an ocean of data identifying you and tracking your activities lies completely open for exploitation under current U.S. law.

Below is a rundown of gaps in U.S. privacy law that have led to this situation:

- No requirement to publish a privacy policy/notice to describe company practices with personal data. There is no federal law requiring companies to publish a notice to consumers of their practices regarding personal data. California's Consumer Privacy Act (CCPA) does require companies to publish a privacy policy and provides certain opt-out rights for California residents, but the CCPA only applies to companies who have over $25 million in annual revenues, who have the data of over 50,000 individuals/devices/households, or whose business is largely from the sale of data. This leaves customers of smaller companies in California, as well as all residents of other states, largely unprotected. The consequence is that smaller companies may not have a privacy policy at all, which deprives the FTC and state consumer protection agencies of their most important regulatory hook: prosecuting companies for violations of their own published privacy policies. A few other states are beginning to pass similar laws to the CCPA, and large companies are extending California rights to US consumers generally for operational simplicity, but the lack of any nationwide law applicable to all companies generally is the foundational hole that allows all the surprising practices discussed in this article.

- Many companies can do whatever they want with the data you provide them. There are two flavors of this gap: companies without privacy policies/notices, and companies with extremely permissive privacy policies. A company without a published privacy policy can collect and do whatever it wants with your data after you give it to them, unless it bumps up against a Limited-Scope Privacy Law (as defined above). Similarly, any company can publish a privacy policy carving out the right to sell your data to third parties, subject only to those same Limited-Scope Privacy Laws -- and possible consumer

backlash. Companies take advantage of these legal gaps to compile your data into a profile (e.g., "in the market for a new home") and sell the profile to advertisers, data brokers, insurers, financial institutions or others for those third parties' marketing purposes. The U.S. laws on email marketing are relatively toothless, there are none for regular postal mail, and laws relating to the reams of electronic personal data generated as you use the Internet and phone apps are in their infancy. Your gut is right: everyone, everywhere is directing targeted marketing to you all the time, and the current legal framework won't protect you well, if at all. In case you doubted Orwell, in the early 2010's, a man learned that his daughter was pregnant from the Target baby item mailers addressed to her arriving at his home.

- Many companies can do whatever they want with your data that they obtain legally from third parties. In addition to the two flavors noted above, there is one more here: hidden players in the data world who may or may not have published privacy notices. If a company hasn't agreed to restrictions on its use of data in its contract with a third party from whom it obtains personal data, and it or the third party has a permissive or no privacy notice, the only limits on the use of that data by the company are Limited-Scope Privacy Laws, plus one new but growing area of state law regarding "data brokers." In 2019, Vermont passed a law specifically applicable to these companies who have no direct relationship with consumers but whose business model consists of compiling and selling data about those consumers. This law, again protecting only Vermont residents, includes privacy notice publication requirements and opt-out rights similar to that of California's CCPA, but only two states have these laws at present. On this front, I'll relate one personal story: when I first obtained a copy of my own credit report in 2002, I was surprised to see that it contained accurate salary information. I asked someone who had been employed by a one of the large credit reporting agencies about this, and he didn't even blink, going on to explain that that information was part of the "consumer file" that anyone could purchase from the agency. As it turned out, there was nothing preventing my former employer's paycheck processing company from selling this information. A few years ago, I negotiated a data processing agreement for a client with the same large paycheck processing company, and even then, their "take it or leave it" language didn't restrict their sale of the salary data.

Data about you, obtained and sold, powers the "information economy" in the US. The degree to which federal lawmakers are willing to limit or cut off the data fuel is unclear. In the meantime, the patchwork continues, with some states, like California, marching forward in emulation of the EU by passing strong data privacy laws, but the majority of states have failed to take action like this to date. The patchwork of laws benefits neither companies, who struggle to identify and comply with what very well

could be conflicting laws, nor consumers, who are largely unaware of any rights they may have but understandably concerned about their privacy. Continuing along the present path quite likely will result in a scenario where only the biggest companies survive and thrive and only a small number of consumers – namely those who are both data-savvy and have time to spare -- achieve good protection for their data. 2021 is a new year, and here's hoping that lawmakers will be able to thread the needle and provide a good baseline of protection for all consumers' data privacy while still preserving the dynamism of the U.S. economy.

The foregoing content is for informational purposes only and should not be relied upon as legal advice. Federal, state, and local laws can change rapidly and, therefore, this content may become obsolete or outdated. Please consult with an attorney of your choice to ensure you obtain the most current and accurate counsel about your particular situation.

Kim A. Verska is the CIO at Culhane Meadows PLLC. Using the perfect balance of tenacity and refined legal analysis, she counsels business clients on data privacy/compliance and guides clients through complex domestic and cross-border technology and other commercial transactions. Ms. Verska concentrates her practice on corporate and technology transactions as well as regulatory issues, particularly in the arena of data privacy and security.
