Originally published in August 2018 by
Legal BlackBook
CyberInsecurity

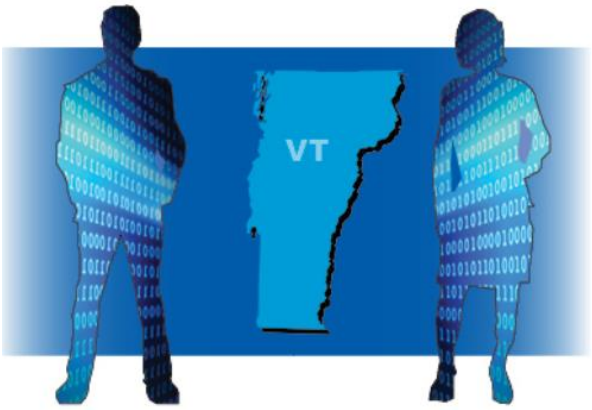
CULHANE MEADOWS PLLC
Big Law for the New Economy®

The Data Regulation You Probably Haven't Heard About

Vermont's new data broker law is one that companies elsewhere need to get to know.

*By **David Jacoby** and **Linda Priebe***

After all the attention garnered in recent weeks by the EU's General Data Protection Regulation (GDPR), there's another regulation that you may have missed. And with good reason, given that only about 0.2 percent of the United States population live in Vermont. But the state's new, first-of-its-kind law regulating data brokers is likely to have an impact far beyond what that number alone would suggest.



The statute creates significant obligations for businesses that collect or make available defined types of personal data for individuals with whom the businesses do not have a direct relationship. And the law will apply if data of any Vermont resident is included. It also imposes standards for information security safeguards and makes the failure to have them in place actionable by the state's attorney general or by individuals suing under the state's unfair and deceptive acts and practices statute.

But first let's clarify what we're talking about. Data brokerage differs from traditional online behavioral advertising. Under the Vermont law, a data broker is a business "that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." (Your favorite online store isn't a data broker because you have a direct relationship with it.)

Shadow Profiles

Though it's not universally known, the personal information that U.S. companies collect from their customers and their websites and their social media visitors is used to create "shadow" profiles of consumers. These profiles are not regulated in the United States and can be used to determine creditworthiness (provided that no actual credit score is used, since that triggers the Federal Fair Credit Reporting Act). They can also be used to determine the favorability of terms of financial services offers, and even which job notices to display to a person online.

The personal information that U.S. companies collect from their customers and their websites and their social media visitors is used to create "shadow" profiles of consumers. These profiles are not regulated in the United States.

The registration and data security provisions that the new law imposes on companies won't take effect until January 1. But the law's other provisions—for example, prohibiting credit reporting agencies from imposing a fee for implementing a credit freeze—took effect with the law's passage on May 22, three days before the GDPR and shortly before California enacted major changes to its own data privacy laws. And the three laws strike a number of common notes.

U.S. businesses routinely purchase consumer personal data from data brokers, and many U.S. companies even have a side business selling the personal data they collect to other companies, including data brokers. The shadow profiles can be used to target ads to consumers on the basis of highly sensitive personal information, such as medical conditions. And there's nothing illegal about any of this, according to World Privacy Forum director Pam Dixon. Speaking about the new Vermont law, Dixon told TechCrunch, "If you take a thousand points like shopping habits, zip code, housing status, you can create a new credit score; you can use that, and it's not discrimination."

Like the GDPR, the Vermont law is intended to help protect consumers from this kind of online profiling done without their knowledge. GDPR Article 22 grants persons located in the EU "the right not to be subject to a decision based solely on automated processing [of their personal data] including profiling which produces legal [or similar significant effects] concerning him or her." Although Vermont does not go as far as the EU, the new law does require a data broker's annual filing to disclose, among other things: whether it lets consumers opt out of its collection of brokered personal information, its databases or certain sales of data; which, if any, of these opt-outs are not permitted; how to go about opting out; and whether the data broker operates a purchaser credentialing process.

Comparing Covered Data

Nine types of data fall within brokered personal information: a person's name; address; date of birth; place of birth; mother's maiden name; unique biometric data, such as fingerprints or retinal images; the name or address of a member of a person's immediate family or household; a Social Security or other government-issued identification number; and anything else that, alone or with other information, would let a reasonable person identify the consumer with reasonable certainty. This parallels the GDPR approach in Art. 4(1). So, if your preference for chocolate ice cream is linked in the database to your name, your preference for chocolate ice cream effectively becomes part of your personally identifiable information.

Data brokers subject to the Vermont law must register with the secretary of state and pay a $100 annual fee. Similarly, the GDPR requires companies to register with a lead EU supervisory authority if the company meets any of three conditions:

• has a location in the EU, regardless of where in the world the company processes EU personal data;

• offers goods or services to persons in the EU (including online and for free); or

• monitors the behavior of persons in the EU (including through IP addresses, device IDs and/or cookie content on the internet).

Covered data brokers must also give Vermont information about their practices regarding collection, storage or sale of consumer information.

Covered data brokers must also give Vermont information about their practices regarding collection, storage or sale of consumer information. And as noted, registered brokers must indicate whether they let consumers opt out of the collection, storage or sale of their covered personal data.

Under the GDPR, companies must provide information directly to persons in the EU about all of the following things done with personal data: collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, destruction and more. Companies must also provide such information to regulators upon request. In addition, when consumer consent is relied on as the permissible legal basis for processing personal data, it generally must be in the form of explicit, affirmative opt-in consent, as opposed to the Vermont law's less strict opt-out standard.

While Vermont data brokers will have to report information on breaches annually, the general GDPR regime is much stricter. Companies must report data breaches to regulators within 72 hours of becoming aware of the breach, and affected persons must be notified by companies "without undue delay."

Finally, there's the controversial "right to be forgotten" provision. Both the GDPR and California's new law provide individuals with a right to have their data deleted. Vermont's new statute does not address this. But it does create a timetable for state officials to report on what further privacy and data security measures are warranted. The Vermont law requires data brokers to put in place a written, comprehensive data security system, including physical, technical and administrative safeguards for consumers' personal data. Additional requirements under all three laws govern the personal information of minors.

Available Remedies

The application of the statute is not limited to brokers that are located in Vermont (or, for that matter, within the United States). The critical nexus is possession of data relating to a Vermont resident, much as the GDPR applies to personal data of anyone in the EU. Vermont's law can be enforced by the Vermont attorney general or by any affected individual. The GDPR also can be enforced by the EU, member states or private

individuals, and this is also true for all of the GDPR's consumer protection provisions regarding both privacy of personal data and data security.

Prevailing under the Vermont law can yield not only compensatory damages, but a punitive award of up to triple the actual damages suffered by consumers, plus reasonable attorney fees. While the GDPR does not specifically provide for attorney fees, its stiff fines can reach a whopping 4 percent of a company's gross global sales revenue (including all of its subsidiaries worldwide that are using the personal data).

The Federal Trade Commission urged Congress to adopt federal data broker legislation in 2014, without success. Although several bills were introduced in Congress, all failed to make it out of committee. If the history of data breach disclosure laws is a guide, however, other states are likely to follow Vermont's example, probably in varying ways. Most state legislatures are not in session now, and California's law does not take effect until January 2020. So far, we have found only one other proposed statute dealing with data brokers, and that is at the municipal level in Chicago.

It would be surprising to see U.S. companies block access of Vermont residents to their websites to avoid having to deal with the new law. But it would not be surprising at all to see U.S. companies apply the Vermont data privacy/security standards to all U.S. consumers visiting their websites—at least until stricter standards are adopted elsewhere.

Authors

David Jacoby is a partner in Culhane Meadows' New York office. He is an experienced litigator who has handled client disputes in a wide range of businesses and industries. He has tried or argued cases in numerous state and federal trial and appellate courts, in private arbitrations and at the Iran-U.S. Claims Tribunal in The Hague. He has been an adjunct professor at Fordham University School of Law since 2007. He can be reached at djacoby@culhanemeadows.com.

Linda V. Priebe is a partner in Culhane Meadows' office in Washington, D.C. She is a Certified Information Privacy Professional/Europe (CIPP/E) and a U.S. data privacy and security compliance and federal relations attorney. Priebe was a deputy general counsel, ethics official, and digital and social media counsel at the White House Office of Drug Policy, 1999-2013. She also served as ethics adviser in the White House Office of the Counsel to the President and was counsel for the government in a dozen cases, including before the United States Supreme Court. At Culhane she helps global businesses, including SaaS providers, international organizations, digital advertisers, internet retailers, telecommunication companies and software developers, to avoid falling out of compliance with the flood of new international laws governing data privacy and security. She can be reached at lpriebe@culhanemeadows.com.

About Culhane Meadows – *Big Law for the New Economy®*

The largest woman-owned national full-service business law firm in the U.S., **Culhane Meadows** fields almost 60 partners in seven offices across the country. Uniquely structured, the firm's Disruptive Law® business model gives attorneys greater work-life flexibility while delivering outstanding, partner-level legal services to major corporations and emerging companies across industry sectors more efficiently and cost-effectively than conventional law firms. Clients enjoy exceptional and highly-efficient legal services provided exclusively by senior attorneys with significant experience and training from large law firms or in-house legal departments of respected corporations. *U.S. News & World Report* has named Culhane Meadows among the country's "Best Law Firms" in its 2014 through 2018 rankings and many of the firm's partners are regularly recognized in *Chambers*, *Super Lawyers*, *Best Lawyers* and *Martindale-Hubbell* Peer Reviews. *Law.com* included Culhane Meadows among the Top 7 Innovators of 2017.