The Future of Consumer Protection is Online

By Chris Curtis and Ryan Kriger

Many Vermonters still buy their produce at the local farmer’s market or put a premium on “buying local” from friends and neighbors who live in their communities. Business deals involve a handshake and relationships can span generations. Vermont’s Consumer Protection Act (CPA) is well suited to regulate these kinds of transactions. But in an era of rapid technological advancement where commerce has overwhelmingly moved online, our laws must keep pace. Now consumers seek the ease of shopping at home, comparing prices with the push of a button and expecting delivery to their doorstep. And with each online transaction, companies are learning about consumers. They amass troves of data – some of which reduce friction in the marketplace and help consumers – and some of which is packaged up and sold and re-sold in the data broker marketplace.

Vermonters place a premium on their privacy. So, Attorney General T.J. Donovan has made the security of and trade in sensitive information about them a priority. The threats in this field are rapidly evolving in both their scope and complexity and go beyond the risk of identity theft to something more fundamental. The right to privacy and anonymity; the right to freedom from a surveillance economy that seemingly tracks our every transaction and even our every move online – rights that if mortgaged today could infringe or chill our rights to speech and assembly. Vermont, like many states, is increasingly concerned about these fundamental rights and how we can square the benefits of a modern economy with protecting the freedoms, social norms and expectations enshrined in our Constitution. Navigating this new economic frontier will require balancing the immense power of the private and public sectors with the personal sphere and determining to what extent businesses or governments should be permitted to exert influence and power over our day-to-day lives.

Attorney General Donovan has tasked us with:

**CPA Enforcement in the Online Marketplace and Data Security.** We routinely work to enforce our data breach notification laws and ensure that companies with sensitive consumer data maintain reasonable data security. We have been involved in several important Vermont and multistate actions, including working with the New York Attorney General’s office to enforce the CPA in the context of serious reporting delays that left consumers exposed by a major hotel chain. We have also brought actions
against other companies that engaged in problematic privacy or security actions. Most recently, you may have read about our complaint against Clearview AI.

Clearview AI (hereafter “Clearview”) collected billions of photographs through screen-scraping, applied facial recognition to them, and markets an app that lets anyone upload a photograph and immediately identify individuals by showing them all the other photos in which that person appears, as they appear on the web. Clearview has provided this app to corporations, foreign governments, billionaires, and law-enforcement agencies.

Vermont’s interest in Clearview began when the New York Times launched a series on privacy matters and profiled the company. Significantly, we also learned that it was collecting the photographs of minors through its filing in the Vermont Data Broker Registry. This realization led us to investigate further and, having identified several problematic issues, we filed a lawsuit in early March. The complaint is three-fold: First, we allege Clearview’s actions were unfair and deceptive. Our complaint alleges that the company collected photographs of Vermonters and their children in a massive database and applied facial recognition technology to those photographs without their knowledge, consent, and in violation of the terms of service of websites where the photographs were posted. We allege the company has also made deceptive representations to consumers and the general public. Second, we allege that Clearview failed to maintain reasonable data security (its database of customers was recently hacked). Finally, we allege that Clearview violated Vermont’s data broker law that prohibits “fraudulent acquisition of data.” Given the stakes for Vermonters, we have moved for a Preliminary Injunction requiring Clearview to immediately remove all Vermonters from its database along with other injunctive relief, appropriate penalties, and costs.

Policy Reform: The Clearview case highlights the possibilities under Vermont’s first-in-the-nation data broker law. Recognizing that this was a massive, influential, and largely unknown business sector, Vermont worked with stakeholders and lawmakers to craft what we believe is a balanced solution designed to bring sunlight to an opaque industry while causing the least disruption possible. The new law has several important elements: a key definition, a requirement that third-party data brokers (those without any direct relationship with the consumers whose data they sell) register in Vermont annually, minimum data security

---

1 Recent enforcement actions and subject matter include:
   - A local software provider for Vermont municipalities (NEMRC) whose data security was so deficient, and their product so widely used by Vermont cities and towns, that we brought an action despite the lack of information related to a breach;
   - A database reporting tool provider (Entrinsik) that allowed Internet Explorer (which it used as an interface), to leave temporary text files containing Personally Identifiable Information (PII) on the client’s computer, resulting in a breach; and
   - An IT support ticketing tool provider (SAManage) that transmitted tickets through URLs but didn’t authenticate access to its tickets, resulting in a spreadsheet containing hundreds of Vermonters’ Social Security numbers being picked up by a search engine.

2 Screen scraping is the use of an automated process to download data from websites.

3 9 V.S.A § 2430.

4 “Data broker’ means a business, or unit or units of a business, separately or together, 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. Examples of a direct relationship with a business include if the consumer is a past or present: (i) customer, client, subscriber, user, or registered user of the business's goods or services; (ii) employee, contractor, or agent of the business; (iii) investor in the business; or (iv) donor to the business.” 9 V.S.A. §§ 2430 (4)(A), (B).

5 9 V.S.A. § 2446.
requirements, and a prohibition of fraudulent acquisition of brokered personal information. The data broker registry went into effect in 2019, is available to the public, and to date contains a few hundred registrations. It was the model for the California Data Broker Registry which was implemented in 2020 in order to facilitate compliance with the California Consumer Privacy Act.

More than just collecting information on data brokers, the registry has been effective in changing behavior. One data broker registered and reported that it did not sell the data of minors. After a journalist pointed out that this was not the case, the broker changed its own practices and stopped selling children’s data. Here was an example of a positive change brought about solely through sunshine, without the need for an enforcement action. Even more significantly, the registry provides us with the kind of information that ultimately led to the enforcement action against Clearview AI.

**Education and Outreach:** Our privacy and data security education efforts include meeting with Vermonters regularly, speaking at conferences and CLE programs around the state and around the country. After the Equifax data breach, hundreds of Vermonters contacted our office. We immediately initiated a series of “town hall meetings” in concert with lawmakers to let Vermonters know what happened and what they could do to protect themselves. We also meet with businesses (and their counsel) to educate them about what “reasonable data security” means from an enforcement standpoint and how to comply with Vermont laws. We recognize that in many (hopefully most) breaches, the company made its best efforts to maintain security, and a breach does not mean an enforcement action – it means helping the business get notice out and comply with the law. These efforts build relationships and understanding and protect Vermonters and the businesses that hold their data.

The future of consumer protection is online. While technology holds great promise to deliver benefits to consumers, it can also place their privacy at risk. Our job is to ensure the benefits of efficiency and choice inure to our citizenry without turning people into the product. Through enforcement, effective policy, and education and outreach, we aim to ensure Vermont does its part to help build an information economy based on principles of consent and respect for privacy.

*Chris Curtis is Chief of the Public Protection Division in the Vermont Attorney General’s Office. Ryan Kriger is an Assistant Attorney General in the Public Protection Division of the Vermont Attorney General’s Office.*

---

6 9 V.S.A. § 2447.
7 9 V.S.A. § 2431.
8 Available at: https://www.vtsosonline.com/online/BusinessInquire/.
9 AB-375. Available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.