.domainSkate

*BRAND PROTECTION DONE RIGHT

CLIENT MEMO - UPDATE

New Personal Privacy Laws Take Center Stage

The commercial use of personal data has gone mostly unregulated in the United States. Lawmakers have grappled with how to balance data privacy issues against creating burdensome constraints that could hamper businesses. Although the law has been slow to catch up, recent high-profile security breaches have scared and outraged the public and spurred a call for oversight. A recently proposed federal law, based on privacy regulations implemented earlier this year in Europe, and several new state laws are likely just the tipping point for what will be major changes to the way data protection and privacy are administered in the United States. Thus, digital privacy is a critical commercial factor that businesses must consider going forward.

EU Passes Privacy Rules That Have Global Impact

The European Union implemented a set of data privacy rules, called the General Data Protection Regulations ("GDPR") in May 2018. The GDPR mandates baseline standards for companies that handle EU residents' data to safeguard the processing and movement of this data. Any company that markets goods or services to EU residents, regardless of location, is subject to the regulation, making the impact of the law global. The key provisions are the following:

- Consent of individuals for data processing/use;
- Anonymizing collected data;
- Notifications for breaches;
- Safely handling the transfer of data across borders; and
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance.

Companies all over the world have scrambled (and many still are scrambling) to fulfill the requirements of the GDPR and avoid being subject to fines or legal action. The GDPR has had an impact even beyond what was contemplated by European lawmakers.

For example, the new law hit the stock market, where Facebook's stock took a steep dive after the law went into effect. Facebook, Amazon, Apple, Google, and Nielsen Holdings, have also all been hit with GDPR-suits in the EU alleging failure to comply with the law.

The law has also impacted the WHOIS (domain registry) system which previously required registrars to provide the contact information for domain name registrants into a publicly available database. This information was used by legal and security professionals to help stop cyber-crime and provided critical transparency. Because of the GDPR many registrars have simply refused to provide any information into the WHOIS system for fear that it could subject them to fines and penalties under the law, thereby making enforcement efforts more difficult and less timely.

California and Vermont Enact Their Own Laws

Earlier this year the State of California passed A.B. 375 entitled the *California Consumer Privacy Act of 2018* ("CCPA"). The CCPA broadly legislates what companies that harvest online consumer data and information can and can't do with that data and penalties if they don't comply. The law is noteworthy because California is home to some of the largest data companies in the world, and it was vehemently opposed by Silicon Valley where tech companies threw millions of dollars at killing or watering down the law. Even so, the law passed and is scheduled to go into effect on January 1, 2020. The CCPA applies to businesses with the following traits:

- Annual gross revenues in excess of $25 million;
- Annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices; or
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

The CCPA also (like the GDPR) has provisions for fines for mishandling data, fining up to $7,500 for each violation. In 2017 alone there were an estimated 1.9 billion files leaked through security breaches, and there will be more in 2018 as just a few of the top breaches (Under Armor, Exactis, Facebook, Ticketfly and My Heritage) add up to almost a billion files. Thus, the financial impact of a large-scale breach under the CCPA would be tremendous and bankrupt most companies.

Other states have also started passing privacy laws. Vermont passed a law this past year (the first of its kind) regulating the activities of "data brokers" who are defined as:

> *"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."*

See Vermont Law H. 764

The Vermont law focuses specifically on third parties who deal in consumer data or "data brokers." Specifically, the law requires *"data brokers"* to annually register with the state of Vermont, to disclose whether and how consumers can opt-out of data collection, to notify consumers if there have been any security breaches during the year, and to adopt comprehensive data security programs with specific safeguards like those mandated under Health Insurance Portability and Accountability Act.

While all 50 states now have laws which require (in some form) companies to notify consumers about data breaches, the California and Vermont laws go beyond basic breach notifications and additionally require companies to make changes to their data processing operations. One of the reasons the EU passed the GDPR was to make sure that individual EU states did not enact their own laws creating different rules in every country - i.e., to prevent EU member countries from doing exactly what California and Vermont are doing here in the United States. Further, these new state laws may not even

be allowed under the U.S. Constitution. Courts have found that similar laws regulating online internet activity violate the Constitution under the Commerce Clause, Article 1, Section 8, Clause 3. *See American Libraries Ass'n v. Pataki,* 969 F. Supp. 160 (S.D.N.Y. 1997). All of this points to the need for some type of federal involvement to prevent a patchwork system from creating different laws/regs in different states.

New Proposed Federal Privacy Bill

A few weeks ago Senator Ron Wyden (Dem. Oregon) proposed a draft bill in Congress called the *Consumer Data Protection Act*. The bill as drafted is stricter than anything that has been enacted to this point. There are hefty fines and even jail time contemplated for senior executives who violate its terms. The bill, at its core, contemplates giving the Federal Trade Commission broader powers, and increased resources, to enforce violations of online digital privacy rights.

A summary of the bill that is posted on the Senator's website states the following as its goal and mission:

1. "Establish minimum privacy and cybersecurity standards.
2. Issue steep fines (up to 4% of annual revenue), on the first offense for companies and 10-20 year criminal penalties for senior executives.
3. Create a national Do Not Track system that lets consumers stop third-party companies from tracking them on the web by sharing data, selling data, or targeting advertisements based on their personal information. It permits companies to charge consumers who want to use their products and services, but don't want their information monetized.
4. Give consumers a way to review what personal information a company has about them, learn with whom it has been shared or sold, and to challenge inaccuracies in it.

5. Hire 175 more staff to police the largely unregulated market for private data.
6. Require companies to assess the algorithms that process consumer data to examine their impact on accuracy, fairness, bias, discrimination, privacy, and security."

See Wyden Press Release, Nov. 1, 2018.

Recommendations and Best Practices Going Forward

The proposed *Consumer Data Privacy Act* is a long way from becoming law, and will most certainly be significantly watered down if it ever does get passed. Even so, the bill itself is a harbinger of change and makes evident that the regulation of consumer data is undeniable and important for every business to understand. New laws and regulations will focus on creating the right/ability for consumers to have a say as to how their personal information and data are handled, during and after their engagement with that business. Further, consumers are getting smarter about how their data is used and companies deemed responsible and trustworthy in handling personal data will reap the rewards of this shift toward a consumer-focused privacy model.

Even with uncertainty around the status of the law, there is still a lot your business should do to insulate it from liability, protect your customers/clients, and avoid unnecessary costs later on. We recommend the following:

1. Use GDPR requirements as a road-map: Even if you don't do business in the EU the GDPR data rules are a good place to frame your strategy. While the California law may end up being significantly changed, and the proposed federal law is far from done, the GDPR is actually in effect. Further, the EU passed the GDPR after years of deliberation and input by experts. By comparison the California law passed after only a few weeks of discussion and largely to avoid political wrangling and having it end up on a statewide ballot initiative. Thus, even though the GDPR is not perfect, it is an important benchmark regardless.

2. Create accountability inside and out: Make sure your partners, third-party vendors, etc. can ensure that the chain of compliance remains unbroken, and that there is someone responsible internally for making sure that your company and vendors are meeting compliance responsibilities.
3. Create an incident response plan: If you don't already have an emergency or incident response plan to deal with an event, then you need to start putting one into effect now. The GDPR requires specific steps in the case of an incident or breach and contemplates heavy fines for failing to comply. Make sure you test your plan and that it is repeatable.
4. Analyze your data: Start to account for specific data types amongst your customers and determine how you are handling that data - is your company simply processing the data, or are you controlling their information?
5. Backup and encrypt your data: The GDPR mandates having a reliable backup and quick restore solution. It also compels data controllers to use pseudonymization, anonymization, or encryption to protect consumer data.

Going forward, data protection and privacy is a critical element for companies to consider on all levels of their business. While the laws are in flux companies can still avoid problems, embarrassment and lost revenue/fines by starting to put in basic protocols and make sure to follow through.