Notable Privacy Law Developments in the Past Year

By Douglas G. Verge

It's a simple fact – individuals value their privacy. At its core privacy means being free from outside intrusions and keeping our personal information to ourselves. Over the past several years, due in part to pressures from privacy advocates, comprehensive laws designed to protect individuals' personal information have been enacted both in the United States and abroad. One of the most comprehensive and far reaching is the General Data Protection Regulation (GDPR) in the European Union (EU), and extended to the European Economic Area (EEA). Our neighbor, Canada, has among other laws, the Personal Information Protection and Electronic Documents Act (PIPEDA).

> "The United States does not have a comprehensive general privacy law. Consequently, many states have taken it upon themselves to introduce such legislation, with California being the first with its California Consumer Privacy Act (CCPA)."

The United States does not have a comprehensive general privacy law. Consequently, many states have taken it upon themselves to introduce such legislation, with California being the first with its California Consumer Privacy Act (CCPA). Virginia recently has followed suit, enacting the Virginia Consumer Data Protection Act (VCDPA) this year. Perhaps the most significant operational impact of these privacy laws for businesses, where applicable, is that they require certain notices to individuals about an organization's/business's personal information collection, use and sharing practices, as well as notifying the individuals about rights they have, which may include the right to know/access, correction, deletion, and opting out of sale or sharing of personal information. Furthermore, failure to comply with the privacy law requirements can lead to substantial monetary and other penalties.

During the past year, there have been three particularly notable developments in the privacy law area. First, with regard to transfers of personal information about persons located in the EEA, the Court of Justice of the European Union (CJEU) (C- 311/18, *Data Protection Commission vs. Facebook Ireland Ltd. and Maximilian Schrems*) (*Schrems II*) invalidated the EU-US Privacy Shield, and called into question the continued viability of other mechanisms for transferring personal information such as Standard Contractual Clauses. Second, through ballot initiative, California enacted a number of significant amendments to the CCPA via the California Privacy Rights Act ("CPRA"), nearly all of which go into effect on January 1, 2023. Third, Virginia became the second state in the US to enact a comprehensive personal information privacy law. This article briefly discusses each of these developments in the law of privacy – the intent is to raise awareness rather than to provide a detailed analysis.

Schrems II

Under the GDPR, transfer of personal information of an individual located in the EEA (a "data subject") to locations/organizations outside the EEA by anyone other than the data subject is prohibited unless at least one of the lawful bases for such transfer under the GDPR is satisfied. One such basis is what is known as an "adequacy decision," which means that the appropriate EEA authorities have made a determination that a country or organization within that country ensure an adequate level of protection. Prior to being struck down by the court in *Schrems II*, the United States was the beneficiary of an adequacy decision pursuant to the EU-US Privacy Shield. Under that regime, organizations located in the US could self-certify that they were complying with the standards and practices required under the Privacy Shield. Absent an adequacy decision, most businesses rely on what are known as the Standard Contractual Clauses promulgated by the European Commission, in order to effectuate such transfers. Those clauses set out standard contractual terms, compliance with which satisfy the adequate level of protection requirement. The court in *Schrems II*, however, said that while those clauses are not per se invalid, they might not be available in certain situations, including in particular for transfers to the United States.

The CJEU based its conclusions upon two key findings. First, it concluded that the Privacy Shield did not adequately prevent federal government authorities from accessing the personal information of data subjects. Second, the CJEU concluded that the Privacy Shield, even with its Ombudsperson framework, did not provide adequate remedies for data subjects to enforce their rights. While the court did not outright strike down the Standard Contractual Clauses, it did indicate that by their inherently contractual nature, those Clauses

PRIVACY *continued on page 29*

Copyright from page 24

ative expression (Android's implementing code)," and "its value lies in its efforts to encourage programmers to learn and to use that system so that they will use (and continue to use) Sun-related implementing programs that Google did not copy." The Court concluded that "the declaring code is, if copyrightable at all, further than are most computer programs (such as the implementing code) from the core of copyright," and that finding fair use would be "unlikely to undermine the general copyright protection that Congress provided for computer programs."

As for the third factor, the amount and substantiality of the portion used, the Court noted that the 11,500 lines that were copied constituted only 0.4 percent of the entire Java API and found that the use was fair where the amount used was "tethered to a valid, and transformative, purpose."

Under the final factor, the effect on the market, the majority did not consider the market effect of Google's copying by looking at Oracle's lost revenue. Instead, the majority cited to evidence that Sun itself "was poorly positioned to succeed in the mobile phone market" and that "Google's new smartphone platform is not a market substitute for Java SE. The record also showed that Java SE's copyright holder would benefit from the re-implementation of its interface into a different market."

In a dissenting opinion, Justice Clarence Thomas, joined by Justice Samuel Alito, argued the majority was wrong to skip the step of determining whether APIs are copyrightable because jumping to the fair-use analysis "distorts" the outcome. The dissent further stated that "Oracle's code at issue here is copyrightable, and Google's use of that copyrighted code was anything but fair."

Numerous amicus briefs were filed in the case. Unsurprisingly, IBM and Microsoft, the Computer & Communications Industry Association, and other groups representing software innovators and startups submitted amicus briefs arguing against the copyrightability of computer interfaces. While the Motion Picture Association, Recording Industry Association of America and other organizations representing the interests of copyright owners submitted amicus briefs arguing that if Google's approach to "transformative use" were applied to expressive works, it would unduly impair copyright owners' exclusive rights.

Many who were eagerly awaiting the Court's ruling on whether APIs are copyrightable were disappointed by the decision. The Court's holding finding fair use was highly dependent on the specifics of the case and it is unlikely the decision will dictate the results in future copyright disputes.

Google's triumph over Oracle is also a victory for innovation. Since 2010 when the case was initially filed, more and more technology companies have come to accept open-source software and open APIs because they have seen how openness and interoperability can lead to innovation that benefits everyone.

Lisa N. Thompson is chair of the New Hampshire Bar's IP Section and an attorney with Hage Hodes, PA in Manchester. Her practice focuses primarily on business and intellectual property matters. She can be reached at Lthompson@hagehodes.com

Trademark from page 26

shortened response deadline. Following implementation, trademark applicants and practitioners should pay close attention to office action response deadlines and make timely extension requests when applicable.

Restoration of the Presumption of Irreparable Harm

Effective upon enactment, the TMA creates a uniform rule establishing a rebuttable presumption of irreparable harm for plaintiffs seeking injunctive relief in federal trademark infringement actions. In *eBay Inc. v. MercExchange L.L.C.*, 547 U.S. 388 (2006), the Supreme Court eliminated a similar presumption in patent infringement cases. Circuit courts split on whether the eBay rule applied in trademark infringement matters, which led several courts to invalidate the presumption and encouraged forum shopping among plaintiffs. To resolve this issue, the TMA amends the Lanham Act to include a rebuttable presumption of irreparable harm upon a finding of infringement or likelihood of success upon the merits. This eases the evidentiary burden on plaintiffs and increases the likelihood of obtaining preliminary and permanent injunctive relief in trademark infringement actions.

Looking Forward

While the TMA provides powerful tools and protections for legitimate trademark owners, its provisions also expose applications and registrations to new challenges by competitors. As the USPTO continues implementation efforts in the upcoming months, trademark owners will want to consider how these new rules and regulations may impact their ability to protect and advance their brands.

Katelyn Burgess is an associate in the Corporate Department and Intellectual Property Practice Group at McLane Middleton. She can be reached at 603-628-1349 or katelyn.burgess@mclane.com.

Benefits from page 27

unlike patents, trademarks have the potential to survive into perpetuity. Therefore, ensuring a quick and effective recordal of all intellectual property transfers through separable intellectual property assignments will help avoid any contractual ambiguity should one company dissolve and will minimize the continued obligation between the companies to effectuate any necessary intellectual property transfers.

Chelsea VanderWoude is an associate at Grossman, Tucker, Perreault & Pfleger at the Manchester, NH office with a focus on trademark and copyright law. Chelsea's work includes domestic and international trademark clearance, prosecution, management, and enforcement; copyright filings, management, and enforcement; IP licensing; contract drafting; client counseling; and business strategy.

Privacy from page 25

cannot bind the public authorities of third countries (such as US government agencies), in which case it may be necessary to supplement the guarantees contained in those Standard Contractual Clauses. Unfortunately, the court did not elaborate as to what those supplementations would be, but the European Data Protection Board recently issued substantial guidance, including recommendations regarding encryption. The US Government also issued a white paper, criticizing the CJEU for focusing on US law and procedures in effect in 2016 when the Privacy Shield was adopted, and not recognizing newer US laws and procures designed to afford more protections and remedies to individuals subject to surveillance laws. The white paper also offers guidance for compliance with the *Schrems II* decision. Needless to say, *Schrems II* has a significant impact on the ability of businesses to conduct commercial activities involving transfers of personal information of data subjects from EEA based businesses to businesses located in the United States.

CPRA amendments to the CCPA

The CCPA applies to a "business," essentially defined to be (a) an entity or individual that does business in the state of California, (b) that collects the personal information of California residents ("consumers"), and (c) that meets at least one of the following criteria:

a. Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted under applicable law
b. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices
c. Derives 50 percent or more of its annual revenues from selling consumers' personal information

A "business" also includes any entity that controls or is controlled by a business as defined above and that shares common branding with the business. Unfortunately, the law does not define what it means to do business in California. The California authorities likely will interpret that provision broadly so that even limited contact with California could be enough to bring a business within the scope of the law.

The CPRA amended the CCPA in a number of ways. Some of the more significant amendments are:

- Changes the definition of who is a business covered by the CCPA by (i) increasing the threshold under paragraph (b) above from 50,000 to 100,000 or more consumers or households, and removing devices, and (ii) broadening the criteria under paragraph (c) above to include sharing, in addition to selling, consumers' personal information
- Creates a new category personal information ("sensitive personal information") and provides specific rights with regard to collection and use of the same
- Creates a new category of personal information recipients, "contractors," in addition to "service providers" and "third parties"
- Provides consumers the right to correct their personal information and expands other consumer rights
- Gives consumers a right to know the length of time the business retains each category of personal information (including sensitive personal information)
- Requires the California Attorney General to adopt regulation requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security: (a) to perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent, and (b) submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information
- Imposes data minimization requirements and storage limitations
- Eliminates the 30 day cure period prior to administrative enforcement
- Expands private right of action criteria
- Creates the first dedicated state privacy organization, the California Privacy Protection Agency

VCDPA

Virginia became the second state in the US to enact a comprehensive personal information privacy law. That law, effective January 1, 2023, applies to "persons" (presumably individuals and legal entities) that conduct business in the Commonwealth of Virginia or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers [as defined below] or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

While the law has similarities to the CCPA, it is not identical, and in fact it adopts some of the concepts from the GDPR. In many ways the VCDPA is simpler and more straightforward than the CCPA. One notable distinction is that unlike the GDPR and the CCPA, the VCDPA does not apply to collection of business-to-business or workforce personal information (although the CCPA as amended by the CPRA has limited B2B and workforce exemptions in effect that become inoperative on January 1, 2023). Specifically, it defines a "consumer" to whom the law applies, as "a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context." Moreover, unlike the CCPA, there is no provision for a private right of action.

Douglas Verge is co-chair of Sheehan Phinney's Data Privacy and Security Law Practice Group. He also is an integral member of the firm's intellectual property law practice, having previously chaired the IP Practice Group for close to 10 years. Doug's clients range from start-ups to multinational companies, representing diverse business interests, including manufacturing, technology, healthcare, education, and the arts..