Editor’s Note: Right to Be Forgotten
Victoria Prussen Spears 167

The Right to Be Forgotten in the United States – Part I
C. W. Von Bergen, Martin S. Bressler, and Cody Bogard 169

CCPA: Impacts and Significance for Business
Natasha G. Kohne and Michelle A. Reed 179

The Rise of Internet of Things Security Laws – Part II
Jeffrey N. Rosenthal and David J. Oberly 189

When Creatively Engaging with Socially Distanced Kids,
Be Sure to Avoid Creating COPPA or CCPA Compliance Concerns
Ronald G. London, Kara K. Trowell, and Alexander B. Reynolds 193

U.S. Justice Department Issues Guidance on
Online Intelligence Gathering for Cybersecurity
Jonathan G. Cedarbaum and Benjamin A. Powell 197
Editor’s Note
The Right to Be Forgotten

Victoria Prussen Spears*

This issue of Pratt’s Privacy & Cybersecurity Law Report begins with the first part of a two-part article discussing the right to be forgotten. We also have an interview on CCPA impacts, the second part of a two-part article discussing Internet of Things security laws, an article covering COPPA and CCPA compliance concerns, and an article examining guidance on online intelligence gathering.

The Right to Be Forgotten

Article 17 of the General Data Protection Regulation (“GDPR”) looks at the right to be forgotten, otherwise known as erasure, delisting, or de-referencing. This and similar legislative initiatives are increasingly inducing some in the United States to implement similar data protection plans; however, such initiatives may conflict with the First Amendment. In this first part of a two-part article, “The Right to Be Forgotten in the United States,” C. W. Von Bergen, Martin S. Bressler, and Cody Bogard, professors at Southeastern Oklahoma State University, discuss the history on the right to be forgotten, the applicability of the GDPR to the issue, and concerns about personal data privacy. The second part of the article, which will appear in an upcoming issue of Pratt’s Privacy & Cybersecurity Law Report, discusses privacy initiatives and legislation in the United States, and the right to be forgotten and the First Amendment.

CCPA Impacts

In this interview, “CCPA: Impacts and Significance for Business,” Natasha G. Kohne and Michelle A. Reed, co-heads of the cybersecurity, privacy and data protection practice at Akin Gump Strauss Hauer & Feld LLP, discuss the California Consumer

* Victoria Prussen Spears is a researcher, writer, editor, and marketing consultant for Meyerowitz Communications Inc. A graduate of Sarah Lawrence College and Brooklyn Law School, Ms. Spears was an attorney at a leading New York City law firm before joining Meyerowitz Communications. Ms. Spears, who is Editor of The Banking Law Journal, Pratt’s Journal of Bankruptcy Law, Pratt’s Energy Law Report, Pratt’s Government Contracting Law Report, and Pratt’s Privacy & Cybersecurity Law Report, all published by Lexis, can be reached at vpspears@meyerowitzcommunications.com.
Privacy Act, its significance on the state and federal levels, and some of the key issues and implications raised by the law.

Internet of Things Security Laws

This two-part article, “The Rise of Internet of Things Security Laws,” by Jeffrey N. Rosenthal and David J. Oberly, attorneys at Blank Rome LLP, examines the enactment of California’s Internet of Things (“IoT”) security law, and the wave of similar IoT laws expected to follow close behind in 2020. The first part of the article, which appeared in the June 2020 issue of Pratt’s Privacy & Cybersecurity Law Report, discussed the current legal landscape as it relates to the security of connected devices and took a closer look at California’s new IoT security law – which went into effect at the start of the year. This second part provides tips and strategies for IoT device manufacturers to comply with the IoT security regulations expected to begin to blanket the country.

COPPA or CCPA Compliance Concerns

Businesses engaging in new online outreach and engagement efforts involving children during the COVID-19 pandemic should carefully assess whether their offerings are directed at children and should understand the requirements of the Children’s Online Privacy Protection Act and Children’s Online Privacy Protection Act – and ensure that they have compliance measures in place. Ronald G. London, Kara K. Trowell, and Alexander B. Reynolds, attorneys at Davis Wright Tremaine LLP, discuss the issues in their article, “When Creatively Engaging with Socially Distanced Kids, Be Sure to Avoid Creating COPPA or CCPA Compliance Concerns.”

Online Intelligence Gathering

Next, Jonathan G. Cedarbaum and Benjamin A. Powell, partners at Wilmer Cutler Pickering Hale and Dorr LLP, review the U.S. Department of Justice’s recent guidance addressing online intelligence gathering in their article, “U.S. Justice Department Issues Guidance on Online Intelligence Gathering for Cybersecurity.”

Enjoy the issue, and please stay safe.
The Right to Be Forgotten in the United States – Part I

By C. W. Von Bergen, Martin S. Bressler, and Cody Bogard*

The General Data Protection Regulation ("GDPR") is a European Union-wide law on data protection and privacy that applies to European Union citizens and organizations based outside the EU that offer goods or services to European Union residents, monitor their behavior, or process their data. Article 17 of the regulation looks at the right to be forgotten, otherwise known as erasure, delisting, or de-referencing. This and similar legislative initiatives are increasingly inducing some in the United States to implement similar data protection plans; however, such initiatives may conflict with the First Amendment. This first part of a two-part article discusses the history on the right to be forgotten, the applicability of the GDPR to the issue, and concerns about personal data privacy. The second part of the article, which will appear in an upcoming issue of Pratt’s Privacy & Cybersecurity Law Report, discusses privacy initiatives and legislation in the United States, and the right to be forgotten and the First Amendment.

The digital age has made the world smaller, more accessible, and communication much more relaxed. Individuals produce more than 2.5 quintillion bytes of data each day, and much of this data consists of information that would allow people to be identified. There are over two billion active Facebook users. Every minute, approximately half a million Snapchat users share photos while Instagram adds another 50,000 photos to that total. There are half a million tweets sent every minute. The amount of personal information exchanged each day is staggering and growing.1 While there are many benefits of such activities, some, especially the Europeans, have recognized the potentially harmful effects of such actions and have initiated laws and regulations giving individual employees the “right to disconnect” from their workplace and to be off the grid; i.e., the freedom to not have to engage with job activities outside of official work hours.2

This right is making its way to America.3 More recently, another European initiative – a new data protection framework and specifically the “right to be forgotten” – may be

---

1 Carol Piovesan, How Privacy Laws Are Changing to Protect Personal Information. FORBES (Nov. 29, 2019).


gaining traction in the United States. When personal information is uploaded online, it is stored permanently, and “our most embarrassing or painful moments may acquire lasting significance and haunt our lives” forever, even when circumstances substantially change.

**SOME HISTORY ON THE RIGHT TO BE FORGOTTEN**

The right to be forgotten is one part (Article 17) of the General Data Protection Regulation ("GDPR") in the European Union ("EU"), which came into effect on May 25, 2018. The regulation brings more significant obligations on organizations processing the personal data of individuals (referred to as data subjects in the legislation). It gives those individuals more control over their personal information. A data subject is essentially under GDPR law, a living individual within the EU whose personal data is being processed. A data subject within the legislation could also be a U.S. citizen living or traveling within the EU. Examples of where the GDPR allows greater rights for data subjects include introducing the rights for individuals to data portability, the right of rectification, the right to object to processing and to be informed or request a copy of the personal data a company holds on them – and the right to be forgotten. The right to be forgotten also includes the right to ask search engines (e.g., Google) to delist specific results for queries with respect to a person’s name. The search engine must comply if the links in question are “inadequate, irrelevant or no longer relevant, or excessive,” considering public-interest factors including the individual’s role in public life.

The central concern lies in the longevity of digital data and the potential undue influence that such search results may exert upon a person’s online reputation almost endlessly if not removed. According to Mayer-Schönberger, information societies, to their detriment, have transitioned from the norm of forgetting over time to a world where information is stored permanently, in what has been called almost perfect memory

---

4 Stefania Alessi, Eternal Sunshine: The Right to be Forgotten in the European Union After the 2016 General Data Protection Regulation. 32(1) EMORY INTERNATIONAL LAW REVIEW, 145-171 (Nov. 29, 2019).


6 The rules were passed in 2016, but the directive gave companies until May 25, 2018 to come into compliance.


in a “digital eternity.”\textsuperscript{11} It has been most commonly understood in preventing someone from referencing another concerning his or her criminal past.\textsuperscript{12} This right is tied not only to the social goals of rehabilitation but also to cultural ideas of informational self-determination and privacy.

**CASE HISTORY ON THE RIGHT TO BE FORGOTTEN**

In *Google Spain SL v. Agencia Española de Protección de Datos*\textsuperscript{13} in March 2010, a Spanish citizen complained to a Spanish newspaper with Spain’s Data Protection Agency and against Google Spain and Google Inc. The man complained that an auction notice of his repossessed home on Google’s search results infringed upon his privacy rights because the proceedings concerning him occurred many years before. Hence, the reference to this information was entirely irrelevant. He first requested that the newspaper either remove or alter the pages in question so that the personal data relating to him no longer appeared.\textsuperscript{14} He also requested Google Spain or Google Inc. to remove his data, so that it no longer showed in search results. The agency dismissed the complaint against the newspaper, stating the publication was justified according to a government order. It however, upheld the complaint against Google, finding that internet search engines are also subject to data protection laws and must take necessary steps to protect personal information.

On appeal, the National High Court of Spain stayed the proceedings. It presented several questions to the Court of Justice of the European Union\textsuperscript{15} concerning the applicability of the EU Data Protection Directive 95/46/EC\textsuperscript{16} (protection of personal data) to internet search engines. The court ruled that individuals can remove results on searches of their names if the data is “inadequate, irrelevant or no longer relevant, or excessive”\textsuperscript{17} considering public interest factors, including the individual’s role in public life. The court also held that individuals whose personal data are publicly available

---

\textsuperscript{11} David F. Lindsay, *Digital Eternity or Digital Oblivion: Some Difficulties in Conceptualising and Implementing the Right to Be Forgotten*, in THE RIGHT TO PRIVACY IN THE LIGHT OF MEDIA CONVERGENCE: PERSPECTIVES FROM THREE CONTINENTS 322, 324 (Dieter Dörr & Russell L. Weaver eds., 2012).

\textsuperscript{12} Meg L. Ambrose & Jeff Ausloos, *The Right to be Forgotten Across the Pond*. 3 JOURNAL OF INFORMATION POLICY, 1-23 (2013).

\textsuperscript{13} *Google Inc. v. Agencia Española de Proteccion de Datos*, (2014) C-131/12 (Spain).

\textsuperscript{14} Id.


\textsuperscript{16} GDPR, et al., supra note 5.

\textsuperscript{17} Google Inc, et al. supra note 13 (93-94).
through internet search engines might “request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results.”

The court ruled that an individual’s right to privacy and protection of personal data override “not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject’s name.” However, the court emphasized the right to initiate such a request may cease to exist when access to personal information “is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.” Determining whether content is in the public interest is complex. It may mean considering many diverse factors, including – but not limited to – whether the content relates to the requester’s professional life, a past crime, political office, position in public life, or whether the content is self-authored, consists of government documents, or is journalistic.

The ruling led to the creation of the EU General Data Protection Regulation (“GDPR”), which replaced the Data Protection Directive 95/46/EC. The GDPR was approved by the EU Parliament in April 2016 and became enforceable in May 2018. This legislation marks the triumph of a distinctive EU variant of the right to be forgotten that derives directly from data privacy, and that can be expected to have massive international consequences. It sharply poses the general theoretical question of how fair information practices can reconcile with freedom of expression. Companies that breach GDPR can face fines of up to €20 million or four percent of annual revenues, whichever is larger. So far, regulators have not imposed any of the billion-dollar fines some expected, while the complexity of the law has frustrated some users and companies during its first year in effect.

Because of Google’s dominance in worldwide search engine market share (at 92.37 percent versus Bing at 2.63 percent and Yahoo! at 1.8 percent) the information provided below on the right to be forgotten is presented for this influential player. From May 29, 2014, to August 31, 2019, Google reported that it received 843,181 delist requests from European Union citizens and 3,323,836 requests for URLs for delisting. After an individual review by Google representatives, 55.1 percent of the

---

18 Id. at 99.
19 Id. at 81.
20 Id. at 99.
URLs were delisted. One percent of all requesters accounted for approximately 20 percent of the total URLs requested for delisting.\textsuperscript{24}

The following are examples of requests Google received from individuals whose information it removed:\textsuperscript{25}

- Information about an individual in Belgium who convicted of a severe crime in the last five years, but whose conviction was overturned on appeal.
- An article about a political activist stabbed at a protest in Latvia.
- An article about the conviction of a teacher in Germany for a minor crime more than 10 years ago.
- A page showing the address of a woman in Sweden (even though Google states elsewhere that addresses are the kind of information generally not removed).
- Pages that discuss the victim of a crime in Italy that occurred decades ago.
- An article reporting on a contest in which a man in Belgium participated when he was a minor.

Google also included examples of requests received from individuals that it did not remove:\textsuperscript{26}

- Recent articles about a decades-old conviction of a public official in Hungary.
- Articles reporting on the conviction of a priest in France for possession of child sexual abuse images and the priest’s banishment from the church.
- Multiple articles about the arrest of a professional in Italy for financial crimes.
- Articles reporting on embarrassing content posted on the internet by a media professional in the United Kingdom.
- Articles about an individual who was fired from a job in the United Kingdom for sexual misconduct.
- Articles and blog posts about an individual in the Netherlands accused of abusing welfare services.
- A copy of an official state document reporting on fraud committed by an individual in Italy.

THE SCOPE AND APPLICABILITY OF THE GDPR AND THE RIGHT TO BE FORGOTTEN

The GDPR was designed to protect data belonging to EU citizens and residents. The law, therefore, applies to organizations that handle such data, whether they are EU-
based firms or not, known as the extra-territorial effect. The GDPR spells out in Article 3\(^{27}\) the territorial scope of the law:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union but in a place where Member State law applies under public international law.

Article 3.1\(^{28}\) states that the GDPR applies to organizations that are based in the EU, even if the data are being stored or used outside of the EU. A controller or data processor will be considered to have an establishment in the EU if it exercises a real and effective activity (even a minimal one) exercised through stable arrangements, regardless of its legal form (e.g., subsidiary, branch, office, etc.), in the territory of a Member State. The threshold for “stable arrangement” can be quite low (e.g., presence of a single employee or agent of the non-EU entity in the EU, provided that such employee or agent acts with a degree of stability). However, the non-EU entity may not be considered as having an establishment in the EU merely because, for example:

- Its website is accessible from the EU;
- It has designated a representative under Article 27\(^{29}\) of GDPR; or
- It uses a data processor established in the EU.

Article 3.2\(^{30}\) goes even further and applies the law to organizations that are not in the EU if two conditions are met: 1) the organization offers goods or services to people in the EU, or 2) the organization monitors their online behavior. These are discussed below in greater detail.

---

\(^{27}\) General Data Protection regulation, Article 3, 2016 (EU).

\(^{28}\) Id.

\(^{29}\) GDPR Directive 95/46/EC, et al., supra note 5.

\(^{30}\) GDPR Art. 3, et al., supra note 27.
Firms That Are Offering Goods or Services

The internet makes goods and services in far-flung places accessible anywhere in the world. A teenager in Italy could easily order a pizza online from a local restaurant in Miami and have it delivered to a friend’s house there. However, the GDPR does not apply to occasional instances. Rather, regulators look for other clues to determine whether the organization set out to offer goods and services to people in the EU. To do so, they will look for things like whether, for example, a Canadian company created ads in German or included pricing in euros on its website. In other words, if the company is not in the EU, but it caters to EU customers, then it should endeavor to be GDPR-compliant.31

If a Firm Is Monitoring Consumer/Employee Behavior

If an organization uses web tools that allow it to track cookies or the IP addresses of people who visit its website from EU countries, then it falls under the scope of the GDPR. Practically speaking, it is unclear how strictly this provision will be interpreted or how conscientiously it will be enforced. Suppose a firm operates a golf course in Ottawa focused exclusively on its local area, but sometimes people in France stumble across its site. It is unlikely that the organization would be held accountable, but technically it could be because it was tracking these data.

AMERICANS’ CONCERNS ABOUT THEIR PERSONAL DATA

The U.S. currently lacks a comprehensive data privacy law or legal equivalent to the GDPR; nevertheless, the implementation of the GDPR by the EU and ongoing news about data privacy and insecurity in the U.S. has led to increased concerns of Americans about their personal information. Trujillo32 reported that polls have shown that 88 percent of Americans support legislation to allow individuals to have information, videos, or photographs about themselves deleted from search engines. A 2018 SAS33 survey found that Americans are increasingly concerned about their data. Of 525 U.S. adults surveyed, 73 percent34 said their concern over the privacy of personal data has increased in the past few years. What was perhaps unexpected was that U.S. consumers seem to be ready for regulation. Sixty-seven percent35 of survey participants think the U.S. federal government should do more to protect data privacy.

31 Id.
34 Id.
35 Id.
A 2019 Pew Research Center report also showed that Americans have an overall wariness about the state of privacy these days.\textsuperscript{36} Data-driven products and services are often marketed with the potential to save users time and money or even lead to better health and well-being. Still, large shares of U.S. adults are not convinced they benefit from this system of widespread data gathering. Some 81 percent of the public say that the potential risks they face because of data collection by companies outweigh the benefits, and 66 percent say the same about government data collection. At the same time, most Americans report being concerned about the way their data is being used by companies (79 percent) or the government (64 percent).

Most also feel they have little or no control over how these entities use their personal information. Moreover, Americans’ concerns about digital privacy extend to those who collect, store and use their personal information. Additionally, majorities of the public are not confident that corporations are good stewards of the data they collect. For example, 79 percent of Americans say they are not too or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information, and 69 percent report having this same lack of confidence that firms will use their personal information in ways they will be comfortable with.

In part, this more significant concern with privacy has been energized by headlines showing increasing numbers of data security breaches. For example, according to Risk Based Security research,\textsuperscript{37} the first six months of 2019 have seen more than 3,800 publicly disclosed breaches exposing an incredible 4.1 billion compromised records. Compared to the midyear of 2018, the number of reported breaches was up 54 percent, and the number of exposed records was up 52 percent.\textsuperscript{38}

Such a growing American public anxiety with the idea of unfettered data accumulation and indefinite access through sophisticated search engines has led to a patchwork of data protection regulations. At the federal level, the U.S. has implemented sectoral legislation as specific issues of privacy arise due to the development of new technologies. Over time there have been many data privacy laws enacted including, but not limited to, the Cable Communications Policy Act\textsuperscript{39} relating to privacy protection for cable subscribers, the Gramm-Leach-Billey Act\textsuperscript{40} protecting access to personal financial and

---


\textsuperscript{37} 2019 on Track to Being the “Worst Year on Record” for Breach Activity. SECURITY (Nov. 29, 2019), available at https://www.securitymagazine.com.

\textsuperscript{38} Id.


banking information, and the Health Insurance Portability and Accountability Act\textsuperscript{41} promoting privacy of health and medical information. These various privacy laws apply to specified societal segments and enforced by different agencies.

Judicial rulings have also periodically addressed privacy issues. In \textit{Hartzell v. Cummings},\textsuperscript{42} a Pennsylvania man filed an emergency request for an injunction against two websites. The websites had suggested both that the man had a criminal record and that he was a participant in the federal witness protection program. In response, a state trial court ordered that the websites be “immediately take[n] down, disable[d], and remove[d].” On appeal, the court clarified its position on prior restraint of free speech by saying that only the defamatory content need be removed. “Cummings still has access to, and operational control of both . . . domain names and Cummings is currently free to publish truthful information regarding Hartzell at each domain name.”\textsuperscript{43} The court decided that only illegal content that would cause irreparable harm could be enjoined. “Moreover, this Court’s order does not impermissibly reach beyond the limits of Cummings’ illegal conduct, and is narrowly tailored to preserve his rights to freedom of speech and expression.”\textsuperscript{44} “The long-ago crime, the court wrote, did not make the plaintiff a present public figure: the plaintiff did not live his current life in the limelight of politics or celebrity, “and the details about his past [were] likely not newsworthy twenty-five years after the fact.”\textsuperscript{45}

Shortly thereafter in \textit{Bloomgarden v. U.S. Dep’t of Justice},\textsuperscript{46} the judge kept information regarding a former prosecutor’s alleged misconduct out of public hands, expressing concerns that the release of past information could harm the individual. In that case, however, the potential danger seemed limited to the individual’s career: “without question,” the court wrote, the former prosecutor “has a strong interest in avoiding decades-old disclosures” and, in contrast, the public “has only a negligible need to know about a largely unremarkable, decades-old disciplinary proceeding.”\textsuperscript{47} In cases such as these, the final decision is based in large part upon whether the public interest outweighs the privacy interests. The court noted, “In sum, we think privacy interests sufficiently outweigh the limited public interest in the letter to make its disclosure unwarranted.”\textsuperscript{48}

\textsuperscript{41} Health Insurance Portability and Accountability Act, Public Law 104-191 (1996).


\textsuperscript{43} \textit{Id.} at 10.

\textsuperscript{44} \textit{Id.} at 11.

\textsuperscript{45} \textit{Id.} at 4.


\textsuperscript{47} \textit{Id.} at 4.

The second part of this article, which will appear in an upcoming issue of *Pratt’s Privacy & Cybersecurity Law Report*, discusses privacy initiatives and legislation in the United States, and the right to be forgotten and the First Amendment.
CCPA: Impacts and Significance for Business

With Natasha G. Kohne and Michelle A. Reed*

Co-heads of the cybersecurity, privacy and data protection practice at Akin Gump Strauss Hauer & Feld LLP discuss the California Consumer Privacy Act, its significance on the state and federal levels, and some of the key issues and implications raised by the law.

Question:

Privacy and data security are headline issues for consumers, and top-line agenda items for businesses around the United States and internationally. One state that has taken strong legislative action on the topic is California, whose California Consumer Privacy Act, or CCPA, took effect January 1.

Analogous to, and perhaps inspired by, the European Union’s General Data Protection Regulation, the CCPA is broad in scope, and vigorous in its assertion of rights and penalties. Given the oft-cited statistic that California’s would be the world’s fifth-largest economy were it a sovereign nation, its laws and its markets are unignorable by other states and even the federal government.

To begin with, Michelle, could you provide readers a bit of background concerning the CCPA and why it is considered significant as a bellwether for state-level and even federal privacy legislation?

Michelle Reed:

Sure. The CCPA is the innovation of real estate developer Alastair Mactaggart. His story really began with a conversation that he had with a Google engineer. That engineer told Mactaggart that he would be horrified to know how much data Google collects on its users. After that, Mactaggart, who really, by all accounts, is a political novice, learned about the ballot initiative process in California, which is a very powerful but often controversial tool that Californians use to ultimately drive state policy, and that resulted in an extensive negotiation that became a legislative effort, the CCPA.

The reason CCPA is considered so important on the privacy landscape is because CCPA is the first comprehensive privacy law enacted in the United States. Before its passage, the only privacy laws in the United States were generally sectoral. Think about HIPAA [the Health Insurance Portability and Accountability

---

* Natasha G. Kohne and Michelle A. Reed, partners in Akin Gump Strauss Hauer & Feld LLP, are co-heads of the firm’s cybersecurity, privacy and data protection practice. They may be contacted at nkohne@akingump.com and mreed@akingump.com, respectively.
Act] for health care or Gramm-Leach-Bliley Act for financial services, COPPA [Children’s Online Privacy Protection Act] for children’s online privacy, and various others.

Europe had actually made sweeping changes to its comprehensive privacy law with the passage of GDPR, and the CCPA really doesn’t follow in the GDPR’s footsteps but does only to the extent that it is really a comprehensive privacy legislation. So, it’s not aimed at a single industry. It’s not aimed at a single right or a single responsibility, but, rather, addresses privacy on a comprehensive scale.

Natasha Kohne:

Just to add to what Michelle said, the CCPA was a catalyst for producing state legislation across the country, and, by our count, since the CCPA passed, around 26 states introduced legislation across the country. Also, this catapulted the federal government into action. I mean, some businesses spend around a hundred thousand to millions of dollars just in getting ready for the CCPA, so I think businesses are really vying for the federal government to act and to potentially preempt the CCPA.

Question:

Thank you. Let’s stay with you, Natasha. There are a few terms noted in the CCPA that stand out, and I think have been commented on fairly extensively in the public forum. One of them is “private right of action,” and the other is “reasonable security.” Could you explain what they mean and their significance?

Ms. Kohne:

Sure. These are some of my favorite subjects as it relates to the CCPA. I think that the private right of action is really a game changer, and just specifically to describe it, it gives California residents an explicit right to sue businesses if their personal information is compromised, and if their personal information is compromised as a result of a business’s failure to maintain reasonable security.

Now, the main issue with the private right of action is that the statute calls for statutory damages, and those damages include $100 to $750 per consumer per incident, whichever is greater. Now, let’s just put that into context for a little while. If there is a breach of unencrypted and unredacted personal information for, let’s say, around 100,000 California residents, then the potential minimum exposure at $100 per consumer – for one incident – is $10 million. This is a significant sum of money for a relatively small breach and definitely more than we’ve been seeing generally in settlements.

So, the bottom line is: We do expect to see an uptick in data breach litigation, and we think the inclusion of these statutory damages really incentivizes plaintiffs’ lawyers to bring claims, not just against some of the larger companies, which is
what we’ve seen historically, but also against the smaller and midsize companies. That’s because, in the Ninth Circuit especially, plaintiffs may now believe that, because of these statutory damages, it’ll be easier to establish harm, they might have an easier time getting past the initial stages of litigation and then they can tee up a settlement quickly since many of these companies may not want to spend the resources to continue to summary judgment or trial, which, in turn, I think, continues to incentivize plaintiffs to bring cases when breaches are just frankly smaller in numbers.

Lastly, I think that leads me to the issue of reasonable security. We do think that reasonable security will be heavily litigated now because it’s an element of the private right of action in California under the CCPA. And whether a business has reasonable security is such a fact-intensive inquiry. Plaintiffs may ask all sorts of intrusive questions during discovery about the implementation of the business’ information security plan and pick at any flaws in those plans or the implementation of those plans. And as we all know, it’s almost impossible to maintain perfect security. So, it’s a real dilemma for businesses because plaintiffs’ lawyers will hone in on some of these inevitable weaknesses.

So, the narrative around what a business does to ensure the safety of consumer data will even be more important for us to focus on before and after a breach occurs.

Question:

Thank you, Natasha. So, let’s circle back a bit. We had talked about state-level legislation a little bit, and Michelle, how does CCPA compare with other state-level privacy legislation from the business perspective, and are states copying CCPA in their own bills?

Ms. Reed:

That’s a great question. So, there are only three states that currently have privacy laws on the books: California, Maine, and Nevada right now. They differ pretty significantly at this point. California gives lots of rights and plenty of requirements: right of deletion, right of portability, right of opt out, right of action for data breaches as Natasha outlined, notice and transparency requirements, and prohibition on discrimination for exercising rights.

The other state laws are a lot narrower than the California law. For example, Maine has a right of restriction, so it has the right to restrict a business’s ability to process personal information about the consumer. It has opt-in requirements, notice and transparency requirements and has a similar prohibition on discrimination but doesn’t have several of the other rights that are outlined in the California legislation, particularly the private right of action.
Nevada’s even, I think, more narrow than that, which provides a right of opt-out and has notice and transparency requirements. Also, their privacy legislation tax on data breach notification requirements, which, frankly, all 50 states and all the U.S. territories now have. So, the reason why California, ultimately, serves as the bellwether is because it’s the most comprehensive.

Now, there’s many states that have proposed legislation that, really, substantially mimics it. There was a competing proposal in Washington, really, which took a more GDPR-like approach than the CCPA did. Ultimately, that bill failed because the House and the Senate in Washington were disagreeing particularly on whether there should be a private right of action included in that. We’ll see if it gets proposed again and what the next steps are. I don’t think it’s down and out forever, but certainly at this point, it’s considered not passed.

There are bills pending in Florida, Hawaii, Illinois, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, New York, and Wisconsin, and there’s active task forces that have replaced bills in Connecticut, Hawaii, Louisiana, Massachusetts, North Dakota, and Texas. So, I think as the next years unfold, you’re going to see lots of legislation that pops up all over the United States. I think it’s going to differ from state to state.

Clearly, the hottest point on these legislative initiatives that’s causing the most contention amongst houses and senates and the various governing bodies is the private right of action.

Obviously, a lot of people consider that to be very concerning and adding a lot of costs and risks for businesses, and, on the flip side, the privacy advocates claim that, without a private right of action, it’s going to be without teeth. I think it remains to be seen where it ends up.

I think that the CCPA is ultimately going to serve as a really important data point on whether or not a private right of action passes another stage because if they see tons and tons of litigation at high cost in California, I think it’s unlikely that the private right of action will pass in the others. But if you see a more measured approach in California, I wouldn’t be surprised if, ultimately, you saw more private rights of action included.

Ms. Kohne:

And just to that end, I think, at the federal government level, the private right of action is also a contentious point that our federal government cannot seem to agree upon. In addition to what is preemption going to look like as well as what is the role of the FTC [Federal Trade Commission], will the FTC actually have more power and more teeth to issue fines, or will it be business as usual and the status quo?
Question:

Thank you, Natasha. Let’s stay with you because another topic that stands out is attorney-client privilege. What are some of the things readers should be considering in the context of the CCPA?

Ms. Kohne:

Thank you for that question, and this question might be a bit self-serving, but I think, honestly, the CCPA makes it more imperative for businesses to think through how to use lawyers, not just when they experience a data breach, but also before any breach actually occurs. For example, it’s commonplace now for regulators in certain industries to require businesses to conduct risk assessments of their information security programs.

Now, these risk assessments often identify gaps in a business’ programs, and then they prioritize risks within that organization. But the problem is that these risk assessments can also sometimes serve as roadmaps for security flaws within an organization, and plaintiffs’ lawyers may ask for them during a data breach litigation. So, businesses should really think through ensuring that these risk assessments are conducted under the privilege. Consider: what are some of the best practices businesses can use to maximize the privilege?

I think it’s also very important for businesses even more so now to ensure that outside counsel or, at a minimum, their in-house counsel is involved in their data breaches from the very beginning. The likelihood of being sued is even higher now, and businesses really cannot risk that their entire data breach investigation is deemed non-privileged because it wasn’t conducted at the direction of lawyers or under the umbrella of the attorney-client privilege.

There is an abundance of case law in the data breach contexts where some companies were successful in maintaining the privilege of their forensic reports, for example, and some were not. So, I’d recommend that businesses and their outside counsel know these rulings cold and when the privilege sticks and when it doesn’t.

Ms. Reed:

I think that there are some really complex considerations that companies have to make when they’re going through these investigations because any kind of reporting that comes out of a data breach is going to be desired by many different parties. So, you know, clearly, if you’re sued in a class action related to it, the plaintiffs will want to see that report. If you’ve maintained the privilege, you can protect it. But, on the flip side, oftentimes you have the auditors who want to see the report. You have state attorneys general who want to see the report. You have Department of Justice or other agencies who would like to see the report.
So, there’s some really serious strategic considerations on how to compile the reports, who to share the report with, how to maintain the privilege on the report. Because, newsflash, when you share it, it can be challenging to maintain the privilege; not impossible, but it can be challenging. All of these considerations need to be made by experienced counsel and experienced consultants who deal with this on a day-to-day basis so that you set up the company for success.

**Question:**

Natasha, you mentioned the California plaintiffs’ bar. What are the principal CCPA-related issues that are being raised by the plaintiffs’ bar that business owners should know about, and are class actions being filed under CCPA?

**Ms. Kohne:**

Yes, this is a good question, and it’s actually a question we’ve been waiting for ever since January 1 has passed, and, predictably, we are seeing CCPA claims being filed already. We saw one very early in January, then many being filed in February. But, interestingly, we’re also seeing CCPA claims being filed not just in the context of a data breach. So, the private right of action really only relates to the context of the data breach. We were concerned that the plaintiffs’ bar would try to use the private right of action and expand it outside of a data breach violation, and so was the California legislature, and they even addressed this issue when they amended the CCPA to make clear that nothing in the statute should serve as a basis for a private right of action under any other law.

And, yet, we are seeing CCPA claims being filed in cases where the crux of the case is about, for example, the failure by companies to give proper notice. So, there was a recent case where a plaintiff’s lawyer cites to Section 100B of the CCPA to argue that California residents require notice at or before the time of collection of personal information being collected by the business. Yet this type of cause of action is clearly prohibited by the CCPA. So we’ll see how this all pans out in litigation, and whether plaintiffs will drop these claims, or whether these businesses are going to have to go ahead and fight these claims and hopefully get them dismissed.

We’re also seeing cases where plaintiffs’ lawyers are citing to the CCPA, not within a cause of action, but to show that a company, for example, knew of the risk of the CCPA because they cited it as a risk factor in their public filings. Or plaintiffs’ lawyers might cite to the CCPA to argue that California has a strong interest in privacy rights, and that California resident data is valuable. So, we expect to see all sorts of different types of arguments, and we’re monitoring these cases and not surprisingly . . . there are a number of cases that have already been filed with CCPA claims.
Question:

Thank you. Let’s look at something else. The CCPA took effect January 1st, but, just the other month, the California Attorney General Office issued revised proposed regulations regarding CCPA. How do these proposed regulations change the legislation? Natasha, please?

Ms. Kohne:

Well, I think just to back up and provide the timeline, I think that’s important and interesting here. I mean, the attorney general first issued draft regulations last October; they were definitely more than what we bargained for. He seemed to go out of his way at the time to add additional requirements to the CCPA that can be viewed not just as interpretations of the law.

Just to give you an example – I like examples – he had businesses required to respond to consumer requests even when those requests were deficient. He’s also requiring businesses to tell third parties not to further sell personal information when those businesses received opt-out requests. These were requirements that were not in the law, and we think actually go beyond just interpreting the law. Then, in February, he issued extensive modifications to the regulations, and I think, on balance, we viewed those as a little bit more business friendly.

Just to give you another example, for a long time, it wasn’t really clear how service providers could disclose personal information to their own subcontractors without triggering a sale. So, it seems that, in February, the attorney general cleared that up along with a few other business-friendly modifications. Then, actually just around two days ago, we got additional modifications – we can call that sort of “version 3.0” – and I think some of these comments continue to be helpful to businesses. But one of the most controversial modifications that he made back in February where he actually tried to clarify what the definition of “personal information” is, well you can say that, that potential clarification backfired. He ended up deleting this modification completely at the behest of some of the privacy advocates.

So, I think overall, this has really been an iterative process, where we’re sort of taking two steps forward, maybe one step back. For every clarification, we sometimes get a little bit more confusion or some more onerous requirements on businesses. But we are getting there, and I think the first question that our clients are asking us is, “How many more rounds are we going? When is this going to stop?” My hope is that we are almost to the finish line on these regulations.

Question:

Thank you. So, now in closing, how would readers know if they have CCPA compliance obligations and what are some next steps that readers should take to ensure they’re compliant with CCPA? Michelle, if you would, please.
Ms. Reed:

Sure. So, the CCPA applies to businesses that do business in California, that collect personal information, that ultimately alone or jointly with others determines the purposes or the means of processing that data. Then they have to satisfy at least one of the following things. They have to either have annual gross revenue in excess of $25 million; they have to alone or in combination annually buy or receive for commercial purposes personal information of at least 50,000 consumers, households or devices; or they have to derive at least 50 percent of its annual revenues from selling consumers’ personal information.

Now, there’s some other details that obviously you want to do a real analysis of how it applies to you, but I think, in general, most businesses that do more than $25 million and have California residents, they’re going to be stuck having to comply with the CCPA. So that leaves, I think, the most important question, which is what should they be doing?

There’s a lot of companies that really had a mad scramble at the end of 2019 to comply. I’ll say throughout this year, we’ve definitely advised clients on CCPA as other companies, a lot of times outside of California, realize that the CCPA applies to them. So, the first step is to determine whether or not you are covered by the CCPA. If you are, the next best step is to conduct a data inventory or some kind of mapping exercise that assesses what data flows and how personal information is used, processed, shared across all the various entities of your organization.

That’s a really extensive process. It requires time and effort and for people to really dig in and see how data is being used. Then another really important consideration is to identify key vendors and whether or not you’re going to characterize them as service providers or third parties. The CCPA treats vendors differently if they are service providers with the proper contractual provisions or if they are ultimately considered third parties. So, evaluating the vendor program is critical. Then making sure that you adopt mechanisms to provide the required notice at or before you collect personal data. You update privacy policies, online privacy policies, and make sure that if you’re selling data that you have a “do not sell” button on your website, and you have procedures to facilitate that opt-out.

It’s important to have a consumer request tracking and response system. There’s rights that consumers have, and they’re going to send it in, and if you don’t have a way to track it, you’re likely not going to be able to comply with the very short requirements on responding to those requests. Then you want to make sure that your employees are trained and that your internal policies and procedures are updated to comply with the CCPA.

Then, I think this gets a little bit to what Natasha was talking about earlier,
you want to lay the groundwork for later application of safe harbors. For example, using redaction and encryption when you’re dealing with personal information and then making sure that you have procedures in place that you could characterize as reasonable security so that you can ultimately use the safe harbors. You want to adopt or create a system for tracking violation notices – they require you to monitor that.

Then this is a key tip that I think a lot haven’t necessarily thought through, but you want to evaluate customer incentive programs. If you have differential pricing for something, you give rewards for sharing information or for providing information, you want to really evaluate that to make sure two things: Number one, that you’re not discriminating against people who say, “I don’t want you to have my information,” and number two, if you say, “No, we’re not discriminating against it. It’s just that we put a value on your information,” think through what that value is. Because sometimes I’ve seen companies look at it, and they have some sort of promotion, they use it through a loyalty program, and then they later discover that, that differential pricing that they say is used so that they can essentially have their data, the access to their personal data, can get thrown back at them in litigation and can really start, in a plaintiff’s mind, to quantify damages.

Obviously on the defense side, we would dispute that as an unreasonable approach, but certainly something to consider when you’re looking at a differential pricing option. So, there’s lots of things to do, lots of work to be done. But I think companies are working hard at trying to comply.

Ms. Kohne:

Just to add to what Michelle said, in particular focusing on the data mapping exercise, the CCPA has a number of exemptions in it. Now those exemptions are really based on personal information. They’re not exemptions based on institutions or entities. So, I think it’s important, in thinking through your obligations, to determine what data is protected by Gramm-Leach-Bliley? What data is protected by HIPAA? How much employee data do you have? What data do you collect in the B2B [business-to-business] context?

Right, now there are exemptions that exist for each of these situations. Almost all businesses have additional data outside of these circumstances that they have to think through. So the data mapping exercise is super important to determine what groups of data sets are applicable to the CCPA. I think the last thing also to emphasize is that virtually every exemption that the CCPA has is not a full-scale exemption. So, even if you have an employee exemption right now in place for the next year, that it’s not a full-scale exemption, and you still will
have obligations to your employees under the CCPA. So, just remember that exemptions are not a full exemption of the CCPA. There are provisions that are still applicable.

**Question:**

Thank you both.
The Rise of Internet of Things Security Laws: Part II

By Jeffrey N. Rosenthal and David J. Oberly*

This is the second part of a two-part article examining the enactment of California’s Internet of Things (“IoT”) security law, and the wave of similar IoT laws expected to follow close behind in 2020. The first part of this article, which appeared in the June 2020 issue of Pratt’s Privacy & Cybersecurity Law Report, discussed the current legal landscape as it relates to the security of connected devices and took a closer look at California’s new IoT security law – which went into effect at the start of the year. This second part provides tips and strategies for IoT device manufacturers to comply with the IoT security regulations expected to begin to blanket the country.

In the blink of an eye, Internet of Things (“IoT”) technology – which connects household and consumer items to the internet – brought about advanced capabilities that were just years ago thought to be matters of science fiction. Notable examples include connected cars, smart homes, and wearable tech, just to name a few.

At the same time, IoT technology also presents a unique set of risks and challenges – particularly around data security. Because of security vulnerabilities inherent in smart devices, and as IoT technology continues to be applied in numerous new and creative ways, legislators have responded with laws specifically geared toward regulating such connected devices.

Consequently, manufacturers of connected devices must find a way to address the mounting security threat posed by hackers and other cyber criminals, while also complying with the growing body of law governing smart technology. Fortunately, there are several actionable steps IoT manufacturers can take to produce IoT devices with enhanced features and functionality in a manner that complies with the law and provides robust security controls to combat cyber risk.

THE ONCE AND FUTURE IOT SECURITY LAWS

California’s new IoT security law requires connected devices be equipped with “reasonable security features” to “protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.” The Federal Trade Commission (“FTC”) and state attorneys general have used their enforcement powers to penalize manufacturers that fail to implement “reasonable steps” to secure smart devices. Combined, IoT manufacturers and vendors should approach

* Jeffrey N. Rosenthal is a partner at Blank Rome LLP. Mr. Rosenthal concentrates his corporate litigation practice on consumer and privacy class action defense. David J. Oberly, an associate at the firm, is a member of the firm’s Cybersecurity & Data Privacy group. The authors may be contacted at rosenthal-j@blankrome.com and doberly@blankrome.com, respectively.
their compliance efforts with an eye toward implementing “reasonable” security measures in a manner that protects the security of not only consumers, but the general public at large.

Critically, while the California IoT law mandates the implementation of “reasonable security features,” the law provides no discussion or insight as to what is sufficient to satisfy this standard. Nor has the FTC (or any other legislative or regulatory body) issued standards or guidance as to what constitutes “reasonable security features” in the context of IoT technology. Without clear direction, IoT manufacturers are placed in a precarious position in terms of determining whether their efforts satisfy the requirements for compliance.

**PASSWORD/AUTHENTICATION PRACTICES AND PROTOCOLS**

Ultimately, to comply with California’s new IoT security law (and expected state laws modeled heavily off the California law), the first step for IoT manufacturers is to revamp their password/authentication practices and protocols. As the California law makes clear, connected devices can no longer rely on default passwords, but must instead feature initial password management requirements that entail – at a minimum – preprogramed passwords for each device or, alternatively, forced generation of new passwords before users can access a device for the first time.

To effectively ensure the security of IoT technology, in most instances it will be necessary to go beyond these minimal password requirements. Here, IoT manufacturers can look to the National Institute of Standards and Technology’s (“NIST”) Special Publication 800-63B, which offers guidelines on best practices for authentication and digital identity, and which can be directly applied to smart technology. Among NIST’s recommendations are to remove password hints and knowledge-based authentication (e.g., what is the first city you lived in?); move from a six-character password minimum to an eight-character minimum; and utilize passphrases instead of simpler passwords (which are common and easily guessed by hackers).

**IMPLEMENTATION OF CYBERSECURITY FRAMEWORKS**

Ultimately, IoT manufacturers’ compliance obligations do not end with enhancement of their devices’ password/authentication mechanisms. Importantly – as exemplified by the California IoT law – in addition to implementing new password/authentication protocols, IoT manufacturers must also tailor their smart device security controls to satisfy three broader, more general “reasonable security features” principles to achieve compliance: e.g., appropriate to the nature and function of the device; appropriate to the information collected, contained, or transmitted; and designed to protect the device from unauthorized access, destruction, use, modification, or disclosure, as is required as part of California’s IoT security law.
In the absence of any clear direction, IoT manufacturers can look to several well-recognized cybersecurity frameworks for guidance.

First, IoT manufacturers can look to the Center for Internet Security’s Critical Security Controls (“CIS Controls”), which offers a list of 20 controls frequently characterized as the gold standard for effective security.

Importantly, in its 2016 Data Breach Report, the California attorney general endorsed the CIS Controls as constituting reasonable security measures. As such, these defensive cyber controls – and, in particular, the CIS Controls’ Internet of Things Companion Guide that focuses specifically on assisting organizations in applying the CIS Controls to IoT technology – can serve as a blueprint to satisfy the “reasonable security features” standard. At the same time, compliance with the Companion Guide can also put IoT manufacturers in a position to quickly respond to the changing legal landscape and achieve compliance with any similar laws added to the mix in 2020.

In addition, IoT makers should also consider supplementing the CIS Controls by incorporating best practices and recommendations from several other widely-accepted IoT-specific cybersecurity frameworks.

In particular, NIST recently released its Core Cybersecurity Feature Baseline for Securable IoT Devices (“NIST Core Baseline”), which establishes a baseline guide for security that manufacturers may adopt for the IoT devices they produce to build secure devices that incorporate “reasonable security features” from the ground up, as well as information on how to identify and implement features most appropriate for their devices and recommendations for what security features an IoT device should possess.

The Cloud Security Alliance (“CSA”) IoT Security Controls Framework also offers guidance on base-level security controls, and is applicable across many IoT domains – from systems which process only “low-value” data with limited impact potential to highly-sensitive systems that support critical services. The CSA Framework can also assist manufacturers in identifying appropriate security controls applicable to specific IoT devices and allocating them to specific components within their systems.

While none of these programs will absolutely ensure IoT devices are impervious to security vulnerabilities, adhering to these programs/frameworks can provide IoT manufacturers with an extra layer of compliance which, in turn, would further aid in demonstrating compliance with “reasonable” security features in the event the manufacturer’s security controls are questioned or challenged by enforcement authorities.

OTHER VITAL SECURITY CONTROLS

Finally, in addition to implementing one or more of the above frameworks, IoT manufacturers should also consider implementing several specific, targeted security controls essential to combating the security risks associated with IoT technology:
• IoT manufacturers should incorporate the principle of least privilege, which entails limiting access rights for users, devices, accounts, and programs to only that information/resources that are absolutely necessary to performing legitimate activities which, in turn, can significantly minimize the overall attack surface that can be exploited to compromise smart devices.

• IoT manufacturers should ensure all IoT data is encrypted, both while in transit and while at rest.

• IoT manufacturers should incorporate effective mechanisms into their IoT devices that allow for post-market patching, monitoring, and vulnerability handling after smart devices have entered the stream of commerce.

THE FINAL WORD

California’s new IoT security law, which officially went into effect on January 1, 2020, represents the beginning of a new era in IoT regulation – one that will be marked by mandatory security requirements designed to combat the significant vulnerabilities that exist in connection with IoT technology. While California’s IoT security law is the first of its kind, it will not be the last. IoT manufacturers should expect to see similar laws popping up in other state legislatures across the United States.

To ensure compliance with this new wave of IoT security laws, IoT manufacturers should take immediate action to confirm security is built into their IoT devices at the outset of the design planning process, which will not only allow manufacturers to align their devices with today’s heightened security requirements, but will also enable IoT makers to ensure that their smart devices are secured from today’s growing cyber risks to the greatest extent possible. Including experienced counsel in this process remains an important first step that can pay significant dividends.
When Creatively Engaging with Socially Distanced Kids, Be Sure to Avoid Creating COPPA or CCPA Compliance Concerns

By Ronald G. London, Kara K. Trowell, and Alexander B. Reynolds*

Businesses engaging in new online outreach and engagement efforts involving children during the COVID-19 pandemic should carefully assess whether their offerings are directed at children and should understand the requirements of the Children's Online Privacy Protection Act and Children's Online Privacy Protection Act – and ensure that they have compliance measures in place.

With kids having been housebound 24/7 for months, and expected to remain so for the foreseeable future, many have resumed schooling remotely and are otherwise engaging online, through social media, and via web-based video-conferencing. And companies across a wide spectrum of interests and services have been creative in innovating how to meet these needs and to occupy idle youth during the pandemic. It is important, however – particularly with younger audiences – that these companies properly handle kids' personal information which they may collect and/or use or disclose along the way. In particular, companies must ensure that they comply with the Children's Online Privacy Protection Act (“COPPA”) and rules the Federal Trade Commission (“FTC”) maintains to implement it (the “COPPA Rule”).

Additionally, if companies make online offerings available to kids who are California residents, they also must comply with the California Consumer Privacy Act (“CCPA”) and implement regulations proposed by the California Attorney General (the “CCPA Proposed Regulations”).

COPPA

COPPA and the COPPA Rule govern the online collection, use, and disclosure of personal information from children under 13 years old. Any operator of a website or online service directed to children under 13, or that has actual knowledge a given user is under 13 (regardless of the nature of the site or service), must obtain verifiable parental consent before collecting any personal information from the child as well as for the use and disclosure of it. Once an operator has the child’s name and/or online contact information and that of the parent, it must refrain from collecting additional personal information, or using or disclosing it, until parental consent is obtained, and it must discard the information if consent is not obtained within a reasonable time.

* Ronald G. London is of counsel in the Washington, D.C., office of Davis Wright Tremaine LLP. Kara K. Trowell is an associate in the firm’s New York office. Alexander B. Reynolds is counsel in the firm’s Washington, D.C., office. The authors may be contacted at ronnielondon@dwt.com, karatrowell@dwt.com, and alexreynolds@dwt.com, respectively.
Under COPPA, “personal information” of a child under 13 means much more than just name, address, phone number, email address, social security number, and the like. It includes any online contact information that permits direct interaction with the child online, including screen names that allow for such contact as well as geolocation data sufficient to identify street name, city or town. It also includes any video or photo image, or audio file of the child's voice, as well as “persistent identifiers” – such as a cookie, IP address, processor or device serial number, or unique device identifier – that can be used to recognize a user over time and across different websites or online services. Any other piece of information concerning the child or their parent(s) also qualifies, if it is collected from the child and combined with any of the foregoing. Additionally, “collecting” this personal information under COPPA includes not only when the child affirmatively enters or provides it, but also passive collection or tracking.

If the operator of a website or online service directed to children under 13, or with actual knowledge a user is under 13, needs or wishes to collect the child's personal information, the operator must obtain verifiable parental consent using means specified in the COPPA Rule. The operator must also have a children's privacy policy accurately describing its collection, use, and disclosure practices with respect to children's personal information and must give parents direct notice of the policy as part of the verifiable consent process.

The FTC’s rules and policies also provide exceptions to the verifiable parental consent requirement and specify circumstances under which less stringent or more demanding forms of verifiable consent may be required. The operator must also enable parents to withdraw consent, review their children's information, and have the information deleted upon request. All children's personal information must be properly secured, using reasonable measures to prevent unauthorized access, and deleted when no longer necessary to fulfill the purpose for which the website or online service collected it.

**CCPA**

If a company processes the personal information of California residents and meets certain threshold requirements, it must also comply with the CCPA and the CCPA Proposed Regulations (which are not yet finalized). Therefore, businesses subject to both COPPA and the CCPA must be aware of the potential scenario that some data will be subject to the CCPA even if not subject to COPPA. The CCPA requires businesses to give California residents transparency about their personal information processing activities and rights to access, delete, and opt out of the sale of their personal information. Unlike COPPA, the CCPA is not primarily intended to protect children online, but it has specific requirements for children under 16.

**Sales Opt-In Requirements**

The CCPA requires a business, having actual knowledge a given user is under 16 years old, to obtain affirmative consent before “selling” that user’s personal information – and a business that willfully disregards the user’s age is deemed to have actual knowledge.
A “sale” under the CCPA occurs any time a business provides personal information to a third party in exchange for monetary or other valuable consideration, whether by transfer, disclosure, provision of access, or like method. (However, it does not include provision of personal information to co-branded corporate affiliates, or to service providers with whom the business has a written contract that restricts their use of the personal information beyond the scope of the agreement in accordance with the CCPA’s requirements.)

Notably, opt-in consent for “sales” of personal information under the CCPA must be obtained in addition to any verifiable parental consent required under COPPA, though it may be possible to design a single consent framework to obtain consent under both statutes just once since their requirements are not mutually exclusive. A parent or guardian must opt in to sales on behalf of children who are under 13, but children between 13 and 15 may opt in on their own behalf. The CCPA Proposed Regulations provide guidance and specific requirements for the opt-in process. A business with actual knowledge that it sells the personal information of minors under 16 must state that fact in its privacy policy and include a description of the opt-in process.

“Personal Information”

The CCPA’s definition of “personal information” is quite expansive, covering non-publicly available information that relates to, describes, reasonably can be associated with, or could be reasonably linked to, directly or indirectly, a particular individual or household.

In contrast, COPPA’s definition of personal information is a small subset of the CCPA’s definition; therefore, businesses subject to both statutes must be aware of the potential scenario that some data subject to the CCPA is not subject to COPPA.

The CCPA provides a lengthy list of categories and specific types of information that fall within its scope, which includes “identifiers” such as real name, user name, contact information, online identifiers and unique personal identifiers, and IP address; internet or network activity information, such as browsing and search history and interaction data; and audio, electronic, and other multimedia information. It also includes education information insofar as that information meets the definition of non publicly available “personally identifiable information” under the Family Educational Rights and Privacy Act (“FERPA”), so for-profit educational institutions should examine their obligations under the CCPA and FERPA.

“Collecting”

“Collecting” is also broadly defined as a business’ acquiring any personal information about a California resident by any means. This covers information provided directly by the individual, but also information that is collected passively or through tracking, or received from a corporate affiliate, service provider, or other third party.
The CCPA Proposed Regulations also set forth specific process requirements for businesses in connection with individuals’ rights to request to know, access, delete, and opt in or out of sales of personal information relating to minors. Businesses must establish a “reasonable method” for verifying that an adult exercising these rights on behalf of a minor is, in fact, the parent or guardian of the minor in question. In the case of a request to delete or access specific pieces of personal information relating to a household – that is, a person or group of people who reside at the same address, share a common device or the same service provided by a business, and are identified by the business as sharing the same group account or unique identifier – which contains members under age 13, businesses must obtain verifiable parental consent before complying with any such request.

THE BOTTOM LINE

Those engaging in new online outreach and engagement efforts involving kids during the COVID-19 pandemic should carefully assess whether their offerings are directed at children under 13 and/or under 16 (in full, or for a substantial subset of its audience); whether they have actual knowledge that their users fall into this demographic; and whether the offerings involve the collection (and use and/or disclosure or sale) of kids’ personal information.

If so, such entities should ensure they understand the COPPA and CCPA requirements and rules and have compliance measures in place. The respective enforcement arms – the FTC for COPPA, and the California Attorney General for CCPA – take compliance seriously, and are concerned with protecting children’s privacy in general. As such, this subject should be top of mind as innovative engagement efforts with homebound kids move forward.
U.S. Justice Department Issues Guidance on Online Intelligence Gathering for Cybersecurity

By Jonathan G. Cedarbaum and Benjamin A. Powell*

The authors review the U.S. Department of Justice’s recent guidance addressing online intelligence gathering.

The Cybersecurity Unit of the U.S. Justice Department’s Computer Crime and Intellectual Property Section has released a guidance document addressing “Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources.”

The guidance considers only federal criminal law, not potential civil liability or risks under state or foreign law, and it emphasizes the importance of seeking legal guidance about particular activities “because minor changes in facts can substantially alter the legal analysis.”

Nonetheless the guidance offers a number of best practice recommendations that may be helpful to the growing number of organizations that engage in or hire another organization to undertake “cyber threat intelligence-gathering efforts that involve online forums in which computer crimes are discussed and planned and stolen data is bought and sold.”

Two Fundamental Rules

At the outset the guidance emphasizes “two rules to always follow”:

- Don’t be a perpetrator: Consult with legal counsel and consider cultivating a relationship with local Federal Bureau of Investigation and U.S. Secret Service field offices if contemplating these types of operations.
- Don’t be a victim: Because online cyber intelligence gathering “may involve interacting with sophisticated criminal actors” organizations undertaking these activities should “remain vigilant, institute appropriate security safeguards, and adhere to cybersecurity practices that will minimize the risk [of being] victimized.”

* Jonathan G. Cedarbaum, a partner in the Washington, D.C., office of Wilmer Cutler Pickering Hale and Dorr LLP, leads the firm’s False Claims Act Group and is a member of its Cybersecurity, Privacy and Communications Group. Benjamin A. Powell, a partner in the firm, is co-chair of the firm’s Cybersecurity and Privacy Practice. Resident in the firm’s office in Washington, D.C., the authors may be contacted at jonathan.cedarbaum@wilmerhale.com and benjamin.powell@wilmerhale.com, respectively.

Three Guideposts

The guidance then offers three tips for online intelligence collection:

• Passively collecting intelligence typically is not illegal: “Doing nothing more than passively gathering information from an online forum, even one on which criminal conduct related to computer crime is conducted, is unlikely to constitute a federal crime, particularly when done without any criminal intent.”

• Access forums lawfully: “Accessing a forum in an unauthorized manner, such as by exploiting a vulnerability or by using stolen credentials, can implicate” the Computer Fraud and Abuse Act\(^2\) and the Access Device Fraud statute.\(^3\)

• Do not assume someone else’s identity without consent: “Using a fake online identity to gain access to or participate in a forum where criminal conduct is occurring, standing alone, is typically not a violation of federal criminal law. However, assuming the identity of an actual person without his or her permission rather than manufacturing a false persona can cause legal problems.”

Six Recommended Best Practices

The guidance then considers a series of scenarios in which actors seeking information for legitimate cybersecurity purposes may interact with participants in different kinds of sites and forums on the dark web: lurking; asking questions; exchanging information with others; purchasing stolen data; and purchasing vulnerabilities. From those scenarios, the guidance derives six best practice recommendations:

• Create “rules of engagement”: Establish and follow “deliberately crafted protocols that weigh legal, security, and operational considerations beforehand.”

• Be prepared to be investigated: “Having trusted lines of communication established in advance” with federal law enforcement “can avoid misunderstandings.

• Practice good cybersecurity: “[U]se systems that are not connected to your company network and are properly secured when communicating with cyber criminals.”

• Promptly report information about an ongoing or impending computer crime uncovered during intelligence gathering activities to law enforcement.

• Do not provide any valid, useful information that can be used to facilitate a crime.

• Involve your legal department in operational planning.

\(^2\) 18 U.S.C. § 1030.

\(^3\) 18 U.S.C. § 1029.
Two Additional Takeaways

There are two additional thoughts to keep in mind:

• The Justice Department’s issuance of this guidance reflects the department’s welcome recognition that “[i]nformation gleaned from . . . online forums and other communication channels where illegal activities are planned and malware used to commit illegal acts and stolen data are sold . . . can be a rich source of cyber threat intelligence and network defense information about past, current, or future cyber attacks or intrusions; malware samples; criminals’ tactics, tools, and procedures that are in current use or under development; and aliases and identities of individuals engaged in attacks and intrusions.” But such cyber intelligence activities raise difficult legal questions that will often turn on the precise facts about methods and intent because “when private parties join or participate in these online forums to collect information for lawful purposes, the line between gathering threat intelligence and engaging in criminal activity can be hard to discern.”

• Online cyber intelligence-gathering activities may raise substantial legal risks under state or foreign law as well as federal law. Purchasing data or cyber information, for example, may implicate state statues governing receipt of stolen property or possession or use of certain kinds of personally identifiable information. Those non-federal legal regimes should also be considered in assessing whether to undertake particular online intelligence-gathering efforts.