Skadden

Privacy & Cybersecurity Update

California Enacts Sweeping New Privacy Law

California has passed a far-reaching new privacy law that will have a significant impact on any company that does business in California and holds information about its residents.

The state of California has enacted the California Consumer Privacy Act (CCPA), which is by far the broadest and most comprehensive privacy law enacted in the United States to date. Due to come into effect in January 2020, the law will impact any organization collecting or storing data about California residents, and may effectively set the floor for nationwide privacy protection since organizations may not want to maintain two privacy frameworks – one for California residents and one for all other citizens. In general, the CCPA will give consumers more information and control over how their data is being used and requires companies to be more transparent in their handling of personal information.

For more information on the CCPA and its impact – including a comparison with the EU's General Data Protection Regulation – please see our July 11 *Insights article*.

US Departments of Commerce and Homeland Security Bank on Awareness and Voluntary Initiatives to Curb 'Botnet' Threat

The Department of Commerce and the Department of Homeland Security have released a report on the dangers posed by "botnets" and certain proposals to address those dangers.

On May 30, 2018, the Department of Commerce and the Department of Homeland Security released "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" (the Report).[1] The Report identified five goals to improve global resilience to "botnet" attacks and suggested voluntary, industry-driven standards and awareness campaigns to achieve these objectives.

[1] A copy of the report can be found here.

Background

The Report confirmed the widespread view that the expanding array of poorly protected internet of things (IoT) devices reaching the market has dramatically increased the potential for automated, distributed threats, which are launched through networks of devices known as "botnets." These devices typically are compromised without their owners' knowledge. Attackers use botnets to launch attacks on other systems, and to create additional botnets. In the past two years, high-profile botnets like Mirai and Reaper have exploited known code vulnerabilities and weak passwords to compromise tens of thousands of devices. Responding to these threats in May 2017, President Trump issued an executive order directing the secretaries of Commerce and Homeland Security to find ways of "dramatically reducing threats perpetrated by automated and distributed attacks."

The Report framed the challenge of mitigating this threat as one of implementation rather than technological inadequacy. Services that disrupt distributed denial-of-service attacks, security development tools like fuzzers and static analyzers, and network control opportunities offered by the most recent new Internet Protocol (IPv6) can greatly mitigate the botnet threat. However, awareness and adoption of these tools is limited.

Mitigating Botnet Attacks Through Awareness and Voluntary Collaboration

The Report identified five objectives for encouraging the uptake of botnet mitigation strategies and technologies:

- creating an adaptable, sustainable and secure technology marketplace;
- promoting infrastructure innovation;
- encouraging innovation in "edge devices," which are internet-connected devices that serve as network entry points;
- supporting coalitions across communities addressing the botnet threat; and
- increasing awareness and education.

The Report recommended voluntary, industry-led awareness and cooperation initiatives as the best way to achieve these goals.

The Report urged industry to lead the development of voluntary IoT and network baseline standards, including by leading the development of "suites of voluntary standards, specifications, and security mechanisms" that reduce the vulnerability of IoT devices to botnet attacks. It also suggested developing best-practice frameworks tailored toward helping smaller enterprises mitigate the botnet threat. Finally, the Report encouraged industry to work with government to promote these standards internationally.

The Report suggested that industry launch business-to-business and consumer-facing awareness and information-sharing efforts. These efforts must be broad-based and involve discussions among internet service providers, the cybersecurity community and the broader industry, in discussions about information sharing protocols, domestic and international botnet threats, and the uptake of cybersecurity technology.

For consumers, the Report recommended the creation of voluntary cybersecurity labeling programs and information tools to promote more informed device shopping. These efforts, modeled on certification programs like the 5-Star Safety and Energy Star ratings, would be designed to reorient IoT manufacturers' market incentives by encouraging consumers to make purchase decisions with cybersecurity in mind.

While voluntary industry efforts are the centerpiece of the Report, the federal government is expected to be the first mover. To spur cross-sector cooperation, the Report urged the Departments of Commerce and Homeland Security to develop a "prioritized road map" of action items. This show of commitment would be intended to boost industry's confidence that its own investments in voluntary initiatives will be productive. At the same time, the Report urged the federal government to "lead by example" by strengthening the resilience of its networks and drawing on its procurement spending to encourage best practices in IoT development.

Taking a dim view of broad regulatory efforts, the Report doubted that "one size fits all" rules for IoT devices could promote security without rapidly being rendered obsolete. Instead, the Report suggested that "sector-specific regulatory agencies" would be better equipped to promote product security within their industries. The Report cited the FDA's medical device guidelines as an example of how sector-specific regulatory agencies can promote cybersecurity and regulatory certainty for manufacturers. The Report also recommended the use of sector-specific agencies, such as the federal Department of Health and Human Services, for industry-specific enforcement actions.

The Report also urged the Federal Trade Commission (FTC) to police commercial deception and unreasonable security practices in the IoT market through its "unfair practices" authority under Section 5 of the FTC Act. For over 15 years, the FTC has been using this authority to bring actions against companies that engaged in particularly poor cybersecurity practices, developing a "quasi-common law" set of standards in this area. We reported in our October 2017 *Privacy and Cybersecurity Update*[2] that, based on statements from then-acting FTC Chairman Maureen

[2] Available here.

Ohlhausen, the FTC would likely take a light touch in cybersecurity matters while "refraining from imposing general standards." The Report endorsed that rejection of general cybersecurity standards but seemed to envision a broad enforcement role for the FTC.

Key Takeaways

For companies that develop and market IoT devices and other botnet targets, the Report suggests the federal government generally will not promulgate specific regulations in the near-term, relying instead on industry players to address the threat through voluntary, industry-led initiatives – with the possible exception of certain specific sectors, such as medical devices. Should they fail to do so, however, public and political pressure may drive regulators to take more aggressive steps in this area.

Return to Table of Contents

European Parliament Calls to Suspend EU-US Privacy Shield

The European Parliament has passed a nonbinding resolution calling on the European Commission to suspend the EU/U.S. Privacy Shield arrangement.

On July 5, 2018, the European Parliament passed a nonbinding resolution calling on the European Commission to suspend the Privacy Shield, a data-sharing arrangement between the EU and the U.S., unless the U.S. is "fully compliant" with the arrangement's terms by September 1, 2018. The vote approved the Motion for Resolution presented by the European Parliament Committee on Civil Liberties, Justice and Home Affairs (the Committee) on June 12, 2018, which addressed the protection of EU citizens' personal data.[3]

Background

In 2016, the United States and the European Commission adopted the EU-U.S. Privacy Shield, a self-certification program designed to enable companies in the U.S. to receive personal data from the EU and the three European Economic Area member states — Norway, Liechtenstein and Iceland. Under the Privacy Shield, companies self-certify their adherence to seven broad data privacy principles. Although enacted when the EU Data Protection Directive was in effect, the Privacy Shield still applies under the set General Data Protection Regulation (GDPR).

The Privacy Shield replaced the previous data sharing structure between the EU and U.S. known as the Safe Harbor, which the Court of Justice of the European Union invalidated in October 2015 in *Schrems v. Data Protection Commissioner*. In the *Schrems* decision, the court found that the Safe Harbor failed to adequately protect the privacy of EU citizens, mainly due to the U.S. government's ability to access personal data for national security purposes. The Privacy Shield aimed to remedy the perceived inadequacies of the Safe Harbor by imposing certain restrictions on the collection of EU personal data by the U.S. government and appointing an ombudsman to oversee such collection practices. After the Privacy Shield's adoption, many privacy advocates criticized the replacement framework for failing to address the governmental surveillance concerns raised in *Schrems*.[4]

The Resolution

In their resolution, members of the European Parliament (MEPs) echoed the Civil Liberties Committee's recent criticism and pointed to the recent Cambridge Analytica scandal to demonstrate the ineffectiveness of the Privacy Shield. Particularly, the European Parliament noted that although this disclosure occurred before the Privacy Shield was in place, Cambridge Analytica's affiliate company SCL Elections is listed on the Privacy Shield register. MEPs emphasized a greater need for monitoring under the agreement, particularly when "data is used to manipulate political opinion or voting behavior."

MEPs also echoed the Committee's concern about the recent adoption by the U.S. of the Clarifying Lawful Overseas Use of Data (CLOUD) Act in March 2018, which grants U.S. and foreign police services access to personal data across borders. The European Parliament indicated that this new U.S. law, which essentially provides a loophole to the Privacy Shield and the *Schrems* decision, runs into direct conflict with EU data protection laws, and may have serious implications for EU citizens.

The European Parliament also expressed apprehension about the executive order signed by President Trump in January 2017, commonly referred to as the "Enhancing Public Safety" order, which stripped privacy protections from non-U.S. citizens.

[3] For more information regarding the Civil Liberties Committee's criticism of the Privacy Shield, see our June 2018 *Privacy and Cybersecurity Update*.

[4] For more information regarding criticism of the Privacy Shield, see our April 2017 *Privacy and Cybersecurity Update*.

MEPs argued that the substance of the order indicates "the intention of the U.S. executive to reverse the data protection guarantees previously granted to EU citizens and to override the commitments made towards the EU during the Obama Presidency." The European Parliament is likely referring to Presidential Policy Directive 28, an Obama-era directive that backed extending privacy protections to non-U.S. nationals in regard to warrantless surveillance.

In addition, MEPs explicitly criticized the U.S. Department of Commerce (DOC) in its review of Privacy Shield certification applications, expressing concern that the DOC has not been requesting copies of agreements used by certified companies with third parties to ensure compliance, despite the availability of this option under the Privacy Shield. The European Parliament concluded that there is no effective control over whether certified companies actually comply with the Privacy Shield provisions.

Notably, in Europe only the European Commission can revoke the Privacy Shield, so the European Parliament's resolution is nonbinding. However, an annual review of the Privacy Shield is due in September, which presents an opportunity for the Commission to reconsider the arrangement in light of Parliament's resolution and the introduction of GDPR to implement more restrictive safeguards.

Effect of Suspension

Members of the Commission have publicly stated that, while the concerns surrounding the Privacy Shield are valid, a suspension may be premature and could result in panic and legal uncertainty. A complete suspension of the Privacy Shield would result in reverberating disruption across the world economy, in that many major companies rely on the agreement to run their businesses effectively.

Should the Privacy Shield be suspended, companies will need to find alternative lawful mechanisms to transfer data between the U.S. and the EU. One option is for companies to incorporate EU-approved contractual clauses between transferors and transferees to facilitate data transfers. An option for affiliated companies is to adopt binding corporate rules for data transfers. At any rate, companies that rely on the Privacy Shield would be wise to begin considering backup plans for cross-border data transfers should the Privacy Shield be suspended by the European Commission.

Key Takeaways

Although a sweeping suspension of the EU-U.S. Privacy Shield is unlikely to take effect within the next few months, the European Parliament's passage of the suspension resolution indicates deep concerns with the existing arrangement. U.S. companies currently relying on the Privacy Shield would be well-advised to seek alternative solutions to lawfully transferring data across borders.

Return to Table of Contents

Second Circuit Holds That Computer Fraud Coverage Is Triggered by Fraudulent Transfer Resulting From Email Spoofing Scam

In a highly anticipated decision, the U.S. Court of Appeals for the Second Circuit, applying New York law, recently held that an insurance policy's computer fraud coverage extends to losses resulting from an email spoofing scam.

On July 6, 2018, the Second Circuit affirmed a district court decision in favor of cloud-based service provider Medidata Solutions, Inc., concluding that its computer fraud insurer Federal Insurance Company (Federal) must cover a $4.8 million loss suffered after Medidata fell victim to an email spoofing scam that caused it to fraudulently wire money overseas.[5]

The Email Spoofing Scam and Medidata's Insurance Claim

The lawsuit, discussed in our March 2018 *Privacy & Cybersecurity Update*,[6] arose from events in September 2014, when a Medidata employee received an email from a fraudster posing as the company's president explaining that an attorney copied on the email (in fact another fraudster) would be contacting the employee for assistance with a transaction. The email appeared legitimate – it contained the president's email address, name and picture. Following telephone and email communications with the fake attorney and approval from legitimate Medidata officers, the employee wired $4.8 million overseas to the fraudsters.

[5] The decision is *Medidata Solutions., Inc. v. Fed. Ins. Co.*, No. 17-2492, 2018 WL 3339245 (2d Cir. July 6, 2018).

[6] See our March 2018 *Privacy & Cybersecurity Update*.

After discovering that it had fallen victim to a spoofing scam, Medidata made a claim under its "Executive Protection" policy issued by Federal. The policy provided coverage for a variety of risks, including "direct loss[es]" suffered by Medidata as a result of "Computer Fraud," defined to include the "fraudulent entry of Data into . . . a Computer System" and the "fraudulent . . . change to Data elements or program logic of a Computer System." Federal denied coverage on the basis that there was no manipulation of Medidata's computers and Medidata "voluntarily" transferred the funds.

The District Court Finds Coverage

Medidata sued Federal in the U.S. District Court for the Southern District of New York. The district court sided with Medidata, relying on the New York Court of Appeals' decision in *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*,[7] which interpreted the phrase "fraudulent entry" of data, as used in a computer fraud policy, as a "violation of the integrity of the computer system through deceitful and dishonest access." Applying a broad reading of *Universal*, the court held that "the fraud on Medidata falls within the kind of 'deceitful and dishonest access' imagined by the New York Court of Appeals" because the fraudster used a computer code to alter a series of emails to make them appear as though they originated from Medidata's president. The court also held that the fraud resulted in a "direct loss," pointing out that the Medidata employee sent the money as a direct result of the fraudster's emails. Federal appealed.

The Second Circuit Affirms

In a brief Summary Order, a three-judge panel of the U.S. Court of Appeals for the Second Circuit affirmed the district court's decision, concluding "that the plain and unambiguous language of the policy covers the losses incurred by Medidata here." The court reasoned that while no hacking incident occurred, "the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system." Because the spoofing code enabled the fraudsters to send messages that appeared to be from senior Medidata employees, "the attack represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system." The attack also made a change to a data element because "the email system's appearance was altered by the spoofing code to misleadingly indicate the sender."

The court found Federal's reliance on the *Universal* decision to be misplaced, concluding that the decision actually *supported* coverage for Medidata's losses. In *Universal*, the court explained, the computer service was only incidentally involved because the company happened to use a computer as opposed to paper to process fraudulent health care insurance claims. Here, by contrast, the fraudsters compromised the email system itself by changing the emails' appearance, resulting in a "violation of the integrity of the computer system through deceitful and dishonest access."

The panel similarly rejected Federal's contention that Medidata did not sustain a "direct loss" as a result of the email scam. "It is clear to us that the spoofing attack was the proximate cause of Medidata's losses," as the chain of events "was initiated by the spoofed emails, and unfolded rapidly following their receipt." Although the Medidata employees had to take actions to effectuate the transfer following receipt of the spoofed emails, those actions were not "sufficient to sever the causal relationship between the spoofing attack and the losses incurred," the court reasoned.

Key Takeaways

The issue of whether losses resulted from email spoofing scams has been increasingly litigated in recent years. While some courts have determined that such losses are covered, other courts have concluded that spoofing scams do not trigger computer fraud coverage either because the losses resulted from voluntary transfers of funds by insureds (as opposed to hacking incidents) or because the insureds took intervening steps to wire funds to the fraudsters, thereby breaking the causal chain. The Second Circuit flatly rejected such restrictive readings of the policy at issue in the *Medidata* case.

The Second Circuit's decision may be valuable for policyholders in future coverage disputes regarding losses arising from spoofing scams and other forms of social engineering fraud. The decision also may cause insurers to revisit and clarify the scope of coverage intended for such incidents.

Return to Table of Contents

[7] 25 N.Y.3d 675 (2015).

The Global Cost of a Data Breach Increases in 2018

An IBM study reported that the average cost of a data breach globally is $3.86 million, a 6.4 percent increase from the 2017 report.

On July 11, 2018, IBM Security announced that the average cost to companies resulting from a data breach increased to $3.86 million in 2018. This amount is a 6.4 percent increase over the average cost of a breach in 2017. The study, titled "The 2018 Cost of a Data Breach Study" (the Study),[8] was based on in-depth interviews with nearly 500 companies that experienced a data breach and an analysis of hundreds of cost factors surrounding a breach, including technical investigations, recovery, notifications, legal and regulatory activities, and cost of lost business and reputation.

Significant Findings

The U.S. experienced the highest average data breach cost at almost $8 million per data breach. The Study speculates that this deviation is due in part to notification costs, which are five times the global average. The Middle East also fell on the high end of the spectrum, suffering from the highest proportion of malicious or criminal attacks, which are the most expensive type of breach to identify and address.

In addition, the average cost for each lost or stolen record containing sensitive information also increased by 4.8 percent from last year, rising to $148 per record. The Study also found that the average total cost of a breach ranges from $2.2 million for incidents with fewer than 10,000 compromised records to $6.9 million for incidents with more than 50,000 compromised records.

The Study also found that companies that operate in the health care or financial services spheres have the highest overall per capita mean for data breach costs. Highly regulated industries, such as health care and finance, often incur additional costs in the instance of a data breach because of fines and penalties, consulting on regulatory requirements, and activities such as credit monitoring or reissuing accounts, which may be required by regulations. As a result, data breaches that impact health care services cost the affected company $408 per compromised record, a cost nearly three times higher than the cross-industry average.

Further, for the first time, the Study calculated the cost associated with "mega breaches" – breaches ranging from 1 million to 50 million records lost – and projected that these breaches cost companies between $40 million and $350 million, respectively. For these large-scale breaches, the biggest expense category was associated with lost business. Researchers also found that the vast majority of these mega breaches stemmed from malicious and criminal attacks, as opposed to system glitches or human error, and the average time to detect and contain a mega breach was almost 100 days longer than a small-scale breach.

Methods for Reducing Costs of a Data Breach

The Study found that the cost of a breach is heavily impacted by the amount of time spent containing a data breach, as well as investments in technologies that speed response time. Companies that contained a breach in less than 30 days saved over $1 million compared to those that took more than 30 days.

The amount of lost or stolen records also impacts the cost of a breach. The Study noted that having an incident response team was the top cost-saving factor, reducing the cost by $14 per compromised record. In addition, companies that used an artificial intelligence platform for cybersecurity reduced the cost by $8 per compromised record and organizations that had extensively deployed automated security technologies saved over $1.5 million on the total cost of a breach.

Key Takeaways

The Study's findings demonstrate that data breaches continue to pose a significant financial risk to companies, and the risk is increasing. The information in the Study should help companies assess the costs and benefits associated with implementing certain procedures and technologies to prevent and respond to data breaches. For example, developing an incident response plan is a relatively low-cost step that the Study shows can have a significant impact on data breach costs. Companies should evaluate the options available to them and invest their resources accordingly.

Return to Table of Contents

[8] Cost of a Data Breach Studies, performed annually since 2005, are sponsored by IBM Security and conducted by Ponemon Institute, an independent institute that researches privacy, data protection and information security policy. The most recent study is available here (registration required).

EU and Japan Reach Bilateral Dealon Data Protection

The EU and Japan have agreed to recognize each other's privacy laws as adequate, allowing transfers of personal information between the two regions.

On July 17, 2018, the European Union and Japan agreed to recognize each other's data protection regimes as providing adequate personal data protections. Once finalized, the "reciprocal adequacy" decisions will allow personal data to flow between the EU and Japan without being subject to additional safeguards.

Background on Adequacy Decisions

The EU's General Data Protection Regulation generally prohibits the transfer of personal information from the EU to a jurisdiction that does not have adequate data protection laws in place, as determined by the European Commission. Japan's Act on the Protection of Personal Information has a similar prohibition on transferring personal information out of Japan.

If the European Commission determines that a country provides a comparable level of data protection to that provided in the EU, it may issue an "adequacy decision." After that decision issues, personal data may flow from any country in the European Economic Area to the country subject to the adequacy decision without additional safeguards. The European Commission has adopted adequacy decisions for several countries and is currently engaged in talks with South Korea to reach an adequacy decision.

In Japan, the Personal Information Protection Commission has the authority to recognize another country's data protection regime as having equivalent standards to those established under Japanese law. After Japan's Personal Information Protection Commission recognizes a country as having equivalent data protection standards, personal data may flow to that country without additional safeguards otherwise required by Japanese law.

The EU-Japan Reciprocal Adequacy Decisions

The EU and Japan agreed to issue reciprocal adequacy decisions regarding each other's data protection regimes as part of a broader trade deal between the two countries. As part of the deal, Japan agreed to implement additional safeguards for personal data, including stricter guidelines for the transfer of personal data that originated from the EU to a third country and limitations on the use of sensitive data. Japan also agreed to implement a new mechanism to allow EU residents to file complaints with Japan's data protection authority if public authorities in Japan unlawfully access their data.

The European Commission's press release regarding the reciprocal adequacy decisions did not outline any additional steps that the EU would need to take for Japan's approval.

Process for Adopting Adequacy Decisions

The European Commission will adopt its decision after it has been approved by a committee composed of representatives from EU member states and the European Data Protection Board. The European Commission expects to adopt its adequacy decision by the fall of this year.

Japan also will follow its own internal approval procedures to adopt its adequacy decision with respect to the EU.

Key Takeaways

The reciprocal adequacy decisions between the EU and Japan will make it easier to exchange personal data for business purposes. Although adequacy decisions are not time-limited, companies that exchange personal data between the EU and Japan should remain aware of any developments that could impact the reciprocal adequacy decisions, including any changes under EU or Japanese law that eliminate protections for personal data.

Return to Table of Contents

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000