Skadden

Privacy & Cybersecurity Update

1 FBI Warns Companies of Ransomware Attacks Targeting Confidential M&A Activity

3 CISA Orders Federal Agencies to Remediate Cybersecurity Vulnerabilities

3 National Association of Insurance Commissioners Report Shows Cyber Insurance Premiums Grew by Nearly a Third in 2020

4 European Data Protection Board Adopts Guidelines on International Transfers of Personal Data

5 New York Passes Pair of Laws Cracking Down on Illegal Robocalls

6 UK Supreme Court Constrains Data Protection-Based Representative Actions

FBI Warns Companies of Ransomware Attacks Targeting Confidential M&A Activity

The FBI provided guidance to companies regarding the increasing incidence of ransomware attacks directed to accessing material nonpublic information regarding mergers and acquisitions.

The Cyber Division of the FBI issued a Private Industry Notification on November 1, 2021, to address ransomware attacks against both public and private companies.[1] Specifically, the FBI warned of ransomware actors leveraging illicitly obtained material nonpublic information regarding major financial events, particularly regarding upcoming mergers and acquisitions, to extract substantial payments from victims. According to the Private Industry Notification, companies that do not implement adequate cybersecurity protocols run an elevated risk of extortion during particularly significant and sensitive periods of corporate decision-making.

Bad Actors Utilizing Dual-Stage Cyberattacks

The Private Industry Notification notes that as ransomware actors become more sophisticated in their tactics, they are increasingly utilizing a dual-stage approach — blanket reconnaissance followed by targeted strikes.

In the notification, the FBI explains that bad actors typically begin with mass-distributed trojan malware against employees at a wide range of companies. During this initial stage, the bad actors use varied techniques, such as phishing attacks, to gain access to companies' private networks and then gather information about corporate and financial activity. For example, the FBI noted a November 2020 technical analysis of a remote access trojan called Pyxie RAT that attackers used to run keyword searches for information that would indicate imminent and near-future stock share price changes. Keywords frequently searched include "10-Q," "10-SB," "N-CSR," "NASDAQ," "MarketWired" and "Newswire."

During the second stage, bad actors sift through data obtained during the information-gathering stage to identify prime targets for ransomware attacks. Specifically, cyber-attackers select companies for which they have discovered material nonpublic information, such as planned announcements of major corporate decisions or M&A

[1] The Private Industry Notification can be accessed here.

activity. Targeted companies are then subjected to blackmail (a threat to publicly disclose that information unless a payment is made), ransomware (malware that locks up or encrypts the company's data or systems unless a payment is made), or both. Such second-stage attacks have become so common that a market for ransomware-as-a-service has developed. As recently as April 2021, the transnational organized crime group DarkSide[2] advertised its ransomware services specifically for commercial extortion through threats against publicly traded companies.

The FBI indicated that between March and July of 2020 alone, at least three publicly traded U.S. companies actively involved in M&A activity (two of which were still in the confidential negotiation period) reported ransomware attacks to the FBI in which such M&A activity was expressly leveraged against them by the attackers. According to the Private Industry Notification, it is likely that the frequency of such attacks is even higher, as companies may choose not to report an incident where a ransom was actually paid. Indeed, the FBI estimates that at least 70-75% of ransomware attacks go unreported. The FBI strongly recommends against paying a ransom to avoid incentivizing or funding further ransomware attacks or illegal activities, but acknowledges in the Private Industry Notification that companies under attack will evaluate all options to protect the company, its shareholders and its customers. Even if a ransom is paid, the FBI urges companies to report the incident so that the agency can take steps to prevent future attacks and hold the attackers accountable.

Combating Ransomware Related to M&A Requires Proactive Cybersecurity Initiatives

To minimize the chances of a ransomware attack, companies should take steps to address each of the two stages described above. The FBI recommended that to reduce the likelihood of an initial intrusion, companies should implement policies, systems and training that guard against exploitation of technical or human vulnerabilities. Furthermore, even if there is a successful intrusion by a bad actor, it is less likely that bad actor will discover compromising corporate information if the company has in place strict internal information access and control systems. Companies also should ensure that their cybersecurity mechanisms appropriately address vulnerabilities from remote and hybrid work as a result of the COVID-19 pandemic, if applicable.

At the least, the FBI recommends that companies implement the following high-level security precautions:

- back up critical data offline;
- ensure copies of critical data are in the cloud or on an external hard drive or storage device;
- secure backups and ensure data is not accessible for modification or deletion from the system where the original data resides;
- install and regularly update antivirus or anti-malware software on all hosts;
- only use secure networks and avoid using public Wi-Fi networks;
- use two-factor authentication for user login credentials and use authenticator apps rather than email, as bad actors may gain control of victim email accounts; and
- implement least privilege for file, directory and network share permissions

The FBI further recommended that companies engaged in frequent or near-term M&A activity should consider additional specialized precautions against ransomware attacks. Such precautions may include a detailed incident response plan to utilize if an attack occurs, as well as cyber insurance policies covering these types of attacks. Companies also were directed to review the Ransomware Guide[3] issued by the Cybersecurity and Infrastructure Security Agency (CISA), a branch of the Department of Homeland Security.

Key Takeaways

Bad actors are developing increasingly sophisticated methods to extort companies for financial gain, through both advances in malware technology and careful selection of commercially vulnerable targets. Companies should ensure that their cybersecurity protections keep pace and take extra precautions in connection with sensitive M&A activity.

Return to Table of Contents

[2] DarkSide is the group responsible for the ransomware attack on the Colonial Pipeline Company that occurred in May 2021.

[3] The Ransomware Guide can be accessed here.

CISA Orders Federal Agencies to Remediate Cybersecurity Vulnerabilities

On November 3, 2021, CISA issued "Binding Operational Directive 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities" (directive),[4] which requires federal agencies to remediate certain known vulnerabilities. The directive forms part of the Biden administration's larger campaign to protect federal information systems and technology assets against malicious cyberattacks, such as the attack on SolarWinds Corp. that resulted in the breach of several federal agency networks, and the ransomware attack on Colonial Pipeline Co. that caused a temporary gas supply shutdown for nearly half of the East Coast of the United States.

The directive applies to "all software and hardware found on federal information systems, including systems managed on agency premises or hosted by third parties on an agency's behalf." Under the directive, CISA must establish, maintain and publish a catalog of known exploited vulnerabilities carrying significant risk to federal agencies,[5] which then must remediate any high-risk security flaws included in the catalog, currently counted at approximately 290 vulnerabilities. Of these vulnerabilities, 90 must have been addressed by November 17, 2021, while the remaining 200 must be resolved within six months, or by May 2022. Additionally, federal agencies must ensure that their internal vulnerability management procedures align with the following minimum requirements set forth in the directive:

- establish a process for ongoing remediation of vulnerabilities that CISA identifies through inclusion in the CISA-managed catalog of known exploited vulnerabilities as carrying significant risk to the federal enterprise within a timeframe set by CISA pursuant to the directive;
- assign roles and responsibilities for executing agency actions required by the directive;
- define necessary activities required to enable prompt response to actions required by the directive;
- establish internal validation and enforcement procedures to ensure adherence with the directive; and
- set internal tracking and reporting requirements to evaluate adherence with the directive and provide reporting to CISA, as needed.

In particular, the directive and the catalog are focused on vulnerabilities that are known to be exploited by bad actors. The directive notes that bad actors do not exclusively rely only on "critical" vulnerabilities, as defined by the Common Vulnerabilities and Exposures system, to achieve their goals, and that some of the most widespread attacks have included multiple vulnerabilities rated "high," "medium" or even "low." This methodology uses lower score vulnerabilities to gain entry to a system, and then exploits additional vulnerabilities to escalate privilege on an incremental basis.

Key Takeaways

Although the directive applies only to federal agencies, private sector organizations — especially those that work, or may work, with the government — should consider incorporating the directive's mandates into their own internal practices, while looking to CISA's catalog as a guide for ongoing cybersecurity risk management.

Return to Table of Contents

National Association of Insurance Commissioners Report Shows Cyber Insurance Premiums Grew by Nearly a Third in 2020

According to a cyber insurance report recently released by the National Association of Insurance Commissioners (NAIC), 2020 cyber insurance premiums grew 29.1% from the prior year as cyber threats continued to increase in frequency and severity.[6]

On October 20, 2021, the NAIC Property and Casualty Insurance Committee released its "Report on the Cybersecurity Insurance Market," the purpose of which is to provide an understanding of the U.S. cyber insurance market. The report is based on data collected from a total of 141 insurers (both U.S.-domiciled and alien surplus lines insurers) that wrote cyber insurance business in the U.S. According to the report, that data shows a cyber insurance market of roughly $4.1 billion in direct written premiums, reflecting a 29.1% increase from 2019.

Stand-alone Versus Package Policies

According to the report, U.S.-domiciled insurers writing stand-alone cyber insurance reported $1.62 billion in direct written premiums for 2020, a 29.1% increase from 2019. Direct written premiums for package policies also increased in 2020 to $1.14 billion (a 13.6% increase from 2019).

[4] The text of the directive is available here.

[5] The catalog can be accessed here.

[6] NAIC, "Report on the Cybersecurity Insurance Market," (Oct. 20, 2021).

Identity Theft Coverage

The NAIC reported that identity theft coverage continues to be the most common cyber product offered by U.S. insurers, with U.S. insurers writing "approximately 20.3 million policies, both standalone and package policies, up roughly 4% from the prior year." This increase aligns with an increase in identity theft reports in 2020. The Federal Trade Commission reported that it received nearly 1.4 million reports of identity theft in 2020, twice as many as it received in 2019.[7] While stand-alone policies for identity theft actually decreased from the prior year by roughly 3%, package policies increased by nearly 4% in 2020.

Ransomware Coverage

The report emphasizes the serious threat posed by ransomware attacks, noting that cybercriminals now often employ extortion by threatening to release or sell sensitive data. The NAIC posits that "[r]ansomware is likely one of the biggest reasons cyber insurance costs are on the rise," noting that in 2020 "there was a 400% increase in ransomware incidents."

Premium Trends

The NAIC also reported that cyber insurance premiums are on the rise, citing a recent survey of brokers that showed a 10%-30% increase in cyber insurance prices during the last quarter of 2020. According to the report, the survey was reflected in the increased pricing trend continuing in the first quarter of 2021, as renewal pricing on cyber insurance rose by an average of 18%. The NAIC also noted that premiums are expected to increase by 15%-50% overall in 2021. The report also stated that excess markets are charging almost as much for their policies as primary insurers are charging.

Cyber Insurance Changes

The report identifies several notable changes to the cyber insurance landscape, including the following:

- Insurers are incorporating sublimits into their policies and adding exclusions to standard coverage lines to avoid duplication of cyber coverage. According to the report, these changes will likely improve underwriting performance.
- Underwriters are raising retention levels while limits are dropping across some sectors.
- Underwriters have begun to conduct more careful evaluations of potential insureds, including using "tools to evaluate prospective insureds' computer networks to decide whether they will write the cyber business."

Key Takeaways

As the report indicates, companies are seeking out cyber insurance protection at a growing rate as one component of their risk management programs, and insurers continue to make adjustments to coverage, underwriting processes and pricing in response to market conditions. In light of the ever-growing frequency and severity of cyberattacks and related losses, we expect the cyber insurance market to continue to grow and evolve in 2022.

Return to Table of Contents

European Data Protection Board Adopts Guidelines on International Transfers of Personal Data

On November 19, 2021, the European Data Protection Board (EDPB) published its Guidelines 05/2021 (the guidelines"), outlining the interplay between the territorial scope of the EU General Data Protection Regulation 2016/679 (GDPR) under Article 3 and the provisions on transfers of personal data to third countries or international organizations under Chapter V. The guidelines will bring welcome clarification to companies regarding their data processing activities.

Background

In accordance with Article 44 of the GDPR, any transfer by a controller or processor of personal data which is undergoing processing or is intended for processing after transfer to a third country or to an international organization must comply with the provisions of Chapter V of the GDPR regarding transfers. The provisions of Chapter V aim to ensure that personal data continues to be protected once it is made accessible to entities outside the European Economic Area (EEA). For this reason, the personal data being transferred must be protected by alternative means, including though an adequacy decision issued by the European Commission or by one of the appropriate safeguards listed in Article 46 of the GDPR (*e.g.*, standard contractual clauses (SCCs)). The guidelines seek to assist controllers and processors operating in Europe to determine whether a specific data processing activity constitutes an international transfer of personal data and, accordingly, whether they are required to comply with the provisions of Chapter V.[8]

[7] FTC, "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020," (Feb. 4, 2021).

[8] The guidelines are subject to public consultation until January 31, 2022, and are available to read in full here.

Three Cumulative Criteria

Given that the GDPR does not specifically provide a legal definition of what constitutes a transfer of personal data to a third country or to an international organization, the EDPB determined that it was necessary to clarify the concept of a transfer. The guidelines identify three cumulative criteria which, when satisfied, qualify a particular processing of personal data as a transfer:

1. **A controller or a processor (the "data exporter") is subject to the GDPR for the given processing of personal data.** This requires that the particular processing of personal data meets the requirements that are outlined in Article 3 of the GDPR, in particular, that the data exporter is subject to GDPR for the specific processing of personal data. This will be the case when the data exporter is established in the EEA (Article 3(1)), or when the data exporter offers goods or services to, or monitors the behavior of, data subjects in the EEA (Article 3(2)).
2. **The data exporter transmits or otherwise makes available the personal data to another controller, joint controller or processor (the "data importer").** This requires a case-by-analysis of the particular processing of personal data and the roles of the actors involved. The EDPB emphasizes that transmission, or the making available of, personal data by the data exporter must be to a different controller, joint controller or processor. The second criterion is not satisfied if a controller in a third country collects data *directly* from an EEA-based data subject, or when an EEA-based employee of the controller remotely accesses personal data in a third country.
3. **The data importer is in a third country or is an international organization.** This requires that the data importer is based *geographically* in a third country (*i.e.*, a country outside of the EEA), is an international organization (*i.e.*, an organization that is governed by public international law) or any other body which is established through an agreement between two or more countries.

If all three criteria are satisfied, then it is determined that there has been a transfer to a third country or to an international organization, as defined under Article 44 of the GDPR. It follows that the controller or processor for the particular processing will be required to comply with Chapter V and, specifically, safeguard the transfer by using one of the means provided in the GDPR.

The EDPB also made clear that it supports the European Commission's proposals to introduce a set of streamlined SCCs to cover data transfers to data importers who are subject to Article 3(2) of the GDPR (*i.e.*, controllers or processors with no presence in Europe that target European individuals through the offering of goods or services, or that otherwise monitor European individuals' behavior in Europe). The EDPB notes that the new SCCs, which were published by the European Commission on June 4, 2021, do not fit a situation where the data importer is a controller or processor and at the same time also itself is subject to the GDPR. This is because the new SCCs partly duplicate GDPR rules, which, by virtue of Article 3(2), already apply to the data importer in the third country. In November 2021, at the IAPP Europe Data Protection Congress 2021, European Commission representatives announced that a streamlined set of SCCs are scheduled for publication in 2022. We discussed the publication of the new SCCs in our June 2021 *Privacy & Cybersecurity Update*, available here.

Key Takeaways

As summarized by EDPB Chair Andrea Jelinek, "[the] Guidelines provide a consistent interpretation of the concept of international transfers and clarify that, when a data importer is subject to the GDPR, the obligations under Chapter V of the GDPR apply both to the transfer from the [EEA] to the importer and to any further transfer that the importer undertakes." The guidelines will assist organizations operating in the EEA to determine which processing activities constitute international transfers and what safeguards must be put in place to ensure that personal data transferred to third countries is adequately protected, while also determining more generally whether the organization complies with Chapter V of the GDPR. Organizations should now be able to reassess their international data maps and, through an application of the three cumulative criteria, conclusively determine which processing activities are subject to Chapter V of the GDPR and what data protection safeguards must be put in place.

Return to Table of Contents

New York Passes Pair of Laws Cracking Down on Illegal Robocalls

On November 8, 2021, New York Gov. Kathy Hochul signed into law two bills that require telecommunications providers in the state to protect consumers by blocking unsolicited robocalls and validating incoming calls. The laws, which are effective immediately, are a codification of rules previously released by the Federal Communications Commission (FCC).

The Robocall Laws

One of the bills signed into law addresses call authentication by requiring companies that provide voice communications services

to New York customers to block certain incoming calls, such as those originating from a number that a subscriber has requested be blocked and those that originate from numbers that are not valid under the North American numbering plan.[9] The law is meant to crack down on illegitimate "spoofing" calls, in which callers attempt to mask their true identity.

The second law requires voice service providers to implement the Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using toKENs (STIR/SHAKEN) protocol, which is the FCC's standard for industrywide call authentication, over the next 12 months.[10] Voice service providers may instead implement an alternative technology that verifies and authenticates caller identification, provided that such technology is comparable or superior to the STIR/SHAKEN protocol. The framework uses cryptography that allows telephone service providers to validate that a call is being made from the number shown and makes tracing the source of illegal calls easier, as each call has a digital certificate assigned to it. The law also provides for enhanced state enforcement by granting the Public Service Commission the authority to oversee compliance with the protocols, including levying civil penalties for offenses and the power to request that companies provide documentation relevant to a suspected violation. Companies that knowingly or negligently violate the law face fines of up to $100,000 per offense for each day the call authentication framework is not implemented.

Key Takeaways

The new laws reflect New York lawmakers' stronger approach against predatory robocalls by attempting to block such calls and taking enforcement action against bad actors in the event such calls get through. The laws also provide more tools for telecommunications companies to prevent and/or trace unwanted calls. Companies that provide voice communications services in New York should be aware that such laws are in effect and ensure compliance by implementing the relevant authentication protocols.

Return to Table of Contents

[9] Details of the law can be accessed here.

[10] Details of the law can be accessed here.

UK Supreme Court Constrains Data Protection-Based Representative Actions

On November 10, 2021, the U.K. Supreme Court (UKSC) handed down its long-awaited judgement in *Lloyd v Google LLC* [2021] UKSC 50, unanimously allowing Google's appeal and reversing the Court of Appeal's decision. The UKSC ruled that a data subject will not have a right to compensation following breach of the Data Protection Act 1998 (DPA 1998, the predecessor of the current DPA 2018) by a data controller unless material damage can be proved, and that damages for loss of control of personal data are not available for breaches of the DPA 1998. The UKSC ruled that even if loss of control damages had been available, the claim could not be brought as a representative "class" action. The decision seemingly restricts the scope for bringing representative actions arising out of breaches of data protection laws. While expressly confined to claims brought under the DPA 1998, this case highlights the difficulty in satisfying the requirement that each claimant have the "same interest" in the claim. The decision therefore sharply limits the possibility of data protection-based class actions, which is viewed as a positive outcome for data controllers.

Background

Plaintiff Richard Lloyd brought a claim against Google in the English courts via the representative action procedure under Rule 19.6 of the Civil Procedure Rules (CPR). He brought this claim on behalf of himself and 4 million data subjects, alleging that Google had unlawfully processed browser data from his and the data subjects' iPhone devices for a purpose not known or disclosed to users and without their consent, referred to as the "Safari Workaround." This workaround allegedly allowed Google to circumvent browser privacy settings and track cookies for the purposes of targeting advertising, thereby monetizing users' data.

For the representative class action to proceed under CPR 19.6, Mr. Lloyd was required to demonstrate that the class of 4 million data subjects shared the "same interest" in the representative claim. He argued that each data subject had his or her data protection rights breached in the same way by Google on the basis of there being a "loss of control" over his and the data subjects' personal data. Mr. Lloyd also argued that it was not necessary to prove individual damage for each data subject affected if each user could be said to have suffered the lowest common denominator of damage, and sought a uniform amount of approximately £750 in compensatory damages for each data subject, for a total of £3 billion.

Google was successful in the first instance, but the decision was overturned in the Court of Appeal. On appeal by Google to the UKSC, two core issues were considered:

- **Loss of control damages.** Could damages be recovered under DPA 1998 for loss of control of personal data alone if the underlying breach of DPA 1998 did not result in material damage, such as mental distress or financial loss?
- **Same interest.** Did Mr. Lloyd and the 4 million data subjects share the "same interest" in the representative action, as required under CPR 19.6?

Decision

The UKSC allowed the appeal and addressed the two core issues[11] as follows:

- **Damages for loss of control of personal data.** The UKSC disagreed with Mr. Lloyd's claim that damages could be awarded for a mere loss of control of personal data under DPA 1998. Applying a textual analysis to DPA 1998, the UKSC concluded that the act did not allow for compensation for breach without proof of actionable damage, as the damage had to be material, for example, in the event of mental distress or financial loss caused by the breach. The UKSC stated that "[DPA 1998] cannot reasonably be interpreted as giving an individual a right to compensation without proof of material damage or distress whenever a data controller commits a non-trivial breach of any requirement of [DPA 1998]." Mr. Lloyd could not prove that he and the representative class of 4 million data subjects had suffered more than trivially. Additionally, Mr. Lloyd's attempt to draw parallels with the tort of misuse of private information, where damages are available for loss of control over private information, was rejected, as was any suggestion that compensation for "loss of control" over personal data was required by EU law.
- **"Same interest."** The UKSC found that a claim for compensatory damages cannot be brought as a representative action unless the damages claimed can be calculated on a uniform basis for each data subject. Any individualized assessment was inconsistent with the "same interest" requirement. In this instance, it could not be argued that Mr. Lloyd and the 4 million data subjects suffered uniform damage, as the impact of the Safari Workaround inevitably varied on a case-by-case basis across the representative class. Any attempt to rely on the lowest common denominator of damage suffered by the class would mean that the damage suffered would fall below the *de minimis* threshold for compensation. The UKSC did, however, acknowledge that a bifurcated claim would have been open to Mr. Lloyd, under which a representative action could be brought for a declaration of breach, after which injured parties could rely on that declaration for individual determination of compensation.

Key Takeaways

The judgement is a welcome development to data controllers, as the dismissal of Google's appeal would have almost certainly resulted in a significant increase in representative "class" action claims arising out of breaches of data protection laws. Questions are likely to be raised by other stakeholders, including claimant law firms and litigation funders, as to whether English law provides sufficient protection to large volumes of individuals who suffer nominal damage at the hands of organizations for serious breaches of data protection laws if representative actions are not permitted. Indeed, the UKSC expressly acknowledged the concern that it was specifically law firms and litigation funders who stood to benefit from any expansion in the scope for data protection-based representative actions.

As the landscape stands, it will now likely take legislative action to permit the types of large-scale "opt-out" representative class actions that are commonplace in the United States regarding data breaches arising in circumstances similar to those in the *Lloyd v Google LLC* action.

Return to able of Contents

[11] The UKSC judgement is available here.

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
213.687.5010
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

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

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

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

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

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@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

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000