Skadden

Privacy & Cybersecurity Update

FINRA Issues Report on Cloud Computing's Benefits, Risks and Regulatory Obligations in the Securities Industry

On August 16, 2021, the Office of Financial Innovation of the Financial Industry Regulatory Authority (FINRA) issued a report that analyzes the adoption of cloud computing across the securities industry and affirms that regulatory requirements, including those relating to cybersecurity and data privacy, continue to apply to functions that have been outsourced to a cloud computing model.

Background

FINRA issued a report titled "Cloud Computing in the Securities Industry,"[1] in which it surveys the proliferation of cloud computing technology in the securities industry and requests comments on the regulatory implications of cloud computing. In the release, FINRA reminds firms that securities laws and FINRA regulations, including those relating to cybersecurity and data privacy, applicable in firms' on-premises environments also remain applicable in the cloud. The report is the most recent development in a series of warnings and proposals issued by FINRA, the Federal Reserve and other banking regulators regarding the risks associated with third-party dependencies and outsourcing in the context of continued financial technology innovation.

The Securities Industry Sees Benefits From Cloud Adoption

As cloud computing continues to widely be adopted across industries, the securities industry has started to take notice. Accordingly, reliance on on-premises systems is waning as firms increasingly integrate cloud computing services into their infrastructure, particularly as cloud computing increasingly becomes a valuable asset to firms industry-wide, especially in an era of remote work. In compiling the report, FINRA sourced data from approximately 40 broker-dealer firms, cloud service providers, industry analysts and technology consultants, noting that cloud computing enhances firms' capacity to scale operations, create reliable business continuity solutions and deploy products faster while potentially lowering costs.

[1] The full text of the report can be found here.

Firms Must Ensure Third-Party Providers Comply With FINRA and Securities Regulations

Cloud computing increases reliance on third-party providers for information technology, data storage and processing capabilities. With that increased third-party reliance comes heightened risk of running afoul of securities regulations. The report asserts that a firm's regulatory obligations remain equally applicable in the cloud as they would in a firm's on-premises technology infrastructure. To the extent a firm outsources an activity or function to a cloud service provider or cloud vendor, the firm still has a continued responsibility to comply with all applicable FINRA rules and securities laws and regulations as they relate to the outsourced activity.

The report urges firms to conduct thorough diligence on cloud service providers to leverage the benefits of cloud computing while ensuring providers can comply with regulations concerning:

i. cybersecurity;

ii. data privacy protections to safeguard customer records and information in accordance with SEC Regulation S-P (Privacy of Consumer Financial Information);

iii. business continuity pursuant to FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information); and

iv. recordkeeping as required by FINRA Rule 4511 (General Requirements) and the Securities Exchange Act books and records rules 17a-3 and 17a-4.

FINRA's outsourcing guidance further provides that firms using third-party service providers have ongoing responsibilities to monitor and supervise such providers' performance of covered activities and to establish supervisory systems with written oversight procedures. In a separate regulatory notice issued the same day as the report, FINRA warned firms that failure to track regulatory violations committed in connection with outsourced technology and third-party vendors is a violation of such firms' supervisory obligations.[2]

Key Takeaways

We can expect the conversation surrounding this topic to continue as firms expand their use of the cloud. Firms should make sure that they build appropriate provisions into agreements with third-party cloud providers that are sufficient to ensure compliance with applicable regulations, including with respect to cybersecurity, data privacy, business continuity, recordkeeping and vendor management. FINRA has requested comments to the report by October 16, 2021.

Return to Table of Contents

[2] A copy of the regulatory notice is available here.

Connecticut Creates Safe Harbor for Companies Following Cybersecurity Protocol

The state of Connecticut adopted a safe harbor from punitive damages in the event of a security breach for companies that adopt certain cybersecurity measures.

On July 6, 2021, Connecticut joined Utah and Ohio as states that have adopted a data breach litigation safe harbor law.[3] In recognition of the growing prevalence of cybersecurity attacks, the law prohibits Connecticut courts from assessing punitive damages in data breach litigation against defendants that implemented a cybersecurity program that meets certain requirements. The law, which will go into effect on October 1, 2021, aims to incentivize businesses of all sizes to implement more powerful safeguards over their information systems.

The Safe Harbor Law

Public Act No. 21-119 prohibits the awarding of punitive damages against a covered entity defendant in any tort action that is brought under either Connecticut law or in Connecticut courts if certain conditions are met. Such tort action must allege a failure by the covered entity defendant to implement reasonable cybersecurity controls that resulted in a data breach involving personal information or restricted information. To take advantage of the safe harbor, the covered entity defendant must have created, maintained and complied with a written cybersecurity program that contains administrative, technical and physical safeguards designed to protect sensitive information and must conform to an industry-recognized cybersecurity framework.

Covered Entities Under the Law

The new law applies to "covered entities," which are defined to include any business that "accesses, maintains, communicates or processes personal information or restricted information in or through one or more systems, networks or services located in or outside [Connecticut]."

- "Personal information" is defined as an individual's first name or first initial and last name in combination with any one, or more, of the following data:
  - Social Security number; driver's license number; state identification card number; credit or debit card number; financial account number in combination with any required security code, access code or password that would permit access to such financial account;
  - individual taxpayer identification number; identity protection personal identification number issued by the IRS;

[3] The full text of Connecticut Public Act No. 21-119 (2021) can be accessed here.

- passport number, military identification number or other identification number issued by the government that is used to verify identity;
- medical information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional; health insurance policy number or subscriber identification number, or any unique identifier by a health insurer to identify the individual;
- biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics and used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; and
- user name or email address, in combination with a password or security question and answer that would permit access to an online account.

- "Restricted information" is defined as "any information about an individual, other than personal information or publicly available information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is reasonably linked or linkable to an individual, if the information is not encrypted, redacted or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to a person or property."

Industry-Recognized Cybersecurity Frameworks

In order to take advantage of the safe harbor, the covered entity must conform to an industry-recognized cybersecurity framework. The law lists a number of standards that would meet the requirement, including: the "Framework for Improving Critical Infrastructure Cybersecurity" published by the National Institute of Standards and Technology (NIST); NIST's special publication 800-171; NIST's special publications 800-53 and 800-53a; the Federal Risk and Management Program's "FedRAMP Security Assessment Framework"; the Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense"; and the "ISO/IEC 27000-series" information security standards published by the International Organization for Standardization and the International Electrotechnical Commission. Adherence to certain state or federal security requirements may also satisfy the requirement (*e.g.*, conforming to HIPAA security requirements). If a particular cybersecurity framework's requirements are updated, to remain subject to the safe harbor a covered entity that sought to conform with such framework must revise its own program to meet the criteria of the updated framework within six months of the update.

The Connecticut law recognizes that the size and nature of a particular business may impact the scale and scope of the covered entity's cybersecurity program. Factors such as the sensitivity of protected information and the cost and availability of tools seeking to reduce risk will also be considered in assessing the adequacy of a covered entity's cybersecurity program.

Key Takeaways

Connecticut's law provides covered entities with incentives to adopt robust protections for personal information, providing companies who comply with certain data protection protocols with a shield against punitive damages in certain tort claims alleged in data breach litigation. Companies should seek to avoid these damages by adopting industry-recognized cybersecurity frameworks to protect the integrity of personal and restricted information they may process.

Return to Table of Contents

UK Information Commissioner's Office Publishes International Data Transfer Agreement and Enters Consultation Period

On August 11, 2021, the U.K. Information Commissioner's Office (ICO) initiated a period of public consultation on its draft international data transfer agreement (the draft IDTA). The draft IDTA seeks to offer a U.K.-specific data transfer mechanism for data transfers to third countries, following the U.K.'s exit from the EU (Brexit) and the Court of Justice of the European Union's decision in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II)*.

Background

The landmark case of *Schrems II* invalidated the EU-U.S. Privacy Shield as a valid data transfer mechanism and imposed enhanced due diligence requirements on organizations relying on standard contractual clauses (SCCs) to transfer data to third countries. Consequently, the European Commission published a new set of SCCs in June 2021.[4] The new SCCs apply only to data transfers out of European Economic Area (EEA) jurisdictions, but, following Brexit, not the U.K. As such, the ICO has had to consider how data transfers from the U.K. will be conducted lawfully in line with the U.K. General Data Protection Regulation (U.K. GDPR) going forward.

[4] For further information, please see our June 2021 *Privacy & Cybersecurity Update*.

The International Data Transfer Agreement

The ICO's response to the new European SCCs consists of three documents, all of which are currently in draft form:

- **The draft IDTA.** Structurally, the draft IDTA is very different from the new European SCCs as it does not follow the modular approach used by the European SCCs, but does provide language for controller-to-controller, controller-to-processor and processor-to-processor transfers (though, notably, not processor-to-controller transfers). It is made up of (1) tables, (2) extra protection clauses, (3) commercial clauses and (4) mandatory clauses. The tables allow parties to easily input contact information of the importer and exporter, as well as details regarding the transfer itself. The extra protection clauses are optional, but companies may wish to provide additional information on technical security protection, and organizational and contractual protections. The commercial clauses are also optional and can be added at the parties' discretion, but will be unenforceable if they inadvertently reduce the level of protection surrounding the transfer. The mandatory clauses, similarly to the European SCCs, cannot be amended by the parties and make up the bulk of the draft IDTA. These clauses outline the obligations of both the exporter and the importer, and establish the level of protection for transferred personal data required by the ICO and the U.K. GDPR. The full text is available here.
- **A draft international transfer risk assessment and tool.** The *Schrems II* judgment requires organizations that transfer personal data of EEA/U.K. data subjects to third countries to complete a risk assessment of the destination country. The ICO's draft international risk assessment and tool, available here, is designed to be used for this purpose. This document requires organizations to consider (1) the particular facts of the restricted transfer, (2) the particular facts about the destination country and (3) the potential impact of the transfer on the data subjects.
- **A draft U.K. addendum to the EU SCCs.** This addendum can be appended to the European SCCs and will be a welcome addition for organizations transferring data from both the EEA and the U.K. to third countries. It appears that, once finalized, this addendum will allow such multinational businesses to avoid having to enter separately into both the IDTA and the new set of SCCs. The full text of the addendum is available here.

Timing and Key Takeaways

The ICO is encouraging participation in the consultation from all parties, including businesses subject to the U.K. GDPR who will need to implement the draft IDTA once available in its final form.[5]

It remains to be seen how multinational businesses and privacy professionals respond to the draft IDTA and how it deviates from the European SCCs once published in its final form. Organizations should continue to monitor these updates and pay particular attention to any timelines and transitional periods imposed by the ICO. Currently, it seems unlikely that the final documents will be published before the end of 2021.

Return to Table of Contents

China Enacts New Comprehensive Privacy Law

On August 20, 2021, China enacted its Personal Information Protection Law (PIPL), a comprehensive national privacy law that includes a number of elements that are similar to the EU's GDPR, including extraterritorial applicability. It is scheduled to go into effect on November 1, 2021.

The PIPL defines personal information in a similar way to the GDPR, and also features a definition of sensitive information that includes biometric information, religious beliefs, health information, financial account information and personal information of children under age 14. In addition, the PIPL has extraterritorial application to processing of personal information outside of China for purposes of providing products or services to individuals in the country, analyzing the behavior of individuals in the country, or other purposes to be specified by laws and regulations.

The PIPL requires that organizations have a lawful basis to process personal information of Chinese individuals, which can include informed consent or processing necessary to (1) perform a contract to which the individual is party, (2) engage in human resources management, (3) perform legal responsibilities and (4) respond to a public health emergency, among others. Consent is required for the processing of sensitive information.

The law provides data subjects with certain rights, such as the right to know what personal information has been collected about them and to access and correct such information, the right to request deletion of such information, and the right to withdraw consent to processing previously given. If the data processor is transferring personal information out of China, it must provide the data subjects with certain information about the transfer and obtain separate consent for the transfer, take steps to ensure adequate protection of such personal information by the transferee and perform an impact assessment. The PIPL contemplates the release by the Cyberspace Administration of China (CAC) of a standard contract to be entered into between the transferor and

[5] Organizations or individuals wishing to respond must complete the consultation paper (available here) and email it to IDTAconsultation@ico.org.uk by 5 p.m. U.K. time on October 7, 2021.

the transferee, although the timing of such release is unclear. The CAC also is expected to promulgate additional rules applicable to cross-border transfers.

Other elements of the PIPL that will be familiar from the GDPR include provisions requiring that automated decision-making be transparent, as well as requiring that individuals be given the opportunity to opt out of targeted marketing. In addition, the PIPL limits the use of facial recognition, which has been a focus of increased legal action in China by individuals objecting to the widespread use of surveillance cameras.

While the PIPL includes a number of similarities to the GDPR, one key area in which they differ is in relation to government surveillance. Unlike the GDPR, the PIPL is not expected to limit the Chinese government's access to personal information. On the other hand, companies may not provide personal information of Chinese individuals to foreign judicial or law enforcement institutions without the approval of Chinese authorities. Multinational companies with operations in China will need to consider how to address this in the context of reporting requirements in jurisdictions outside of China.

Under the PIPL, individuals have the right to make a complaint to a regulator if they believe their rights have been violated. In addition, individuals may bring tort actions against violators and, if a large number of individuals' rights are violated, certain designated organizations may file public interest lawsuits. Violations of the PIPL could result in enforcement actions that require companies to take remedial measures or suspend services, or that impose fines of up to RMB 50 million or 5% of the prior year's revenue (although it is unclear at this time whether this is a percentage of global revenue or revenue generated in China).

Key Takeaways

As with other comprehensive privacy laws, it will take time to develop certainty regarding the preferred implementation of the PIPL's requirements into companies' privacy programs, and to understand the manner in which law will be enforced. However, because the PIPL will become effective on November 1, 2021, companies that may be subject to the law should move swiftly to review their practices with respect to Chinese data processing activities and update those practices to take the regulation's requirements into account.

Return to Table of Contents

Northern District of California Dismisses Case Without Ruling on Section 230 of the Communications Decency Act

On August 9, 2021, the U.S. District Court for the Northern District of California dismissed *Enigma Software Group USA LLC v. Malwarebytes Inc.* without leave to amend.[6] The case had garnered attention due to its potential ruling on the applicability of Section 230 of the Communications Decency Act (Section 230), a law that provides certain immunities for internet service providers and other technology companies in relation to content posted by third parties. However, the court dismissed the plaintiff's claims without deciding on that point.

In *Enigma Software Group US LLC v. Malwarebytes Inc.*, both the plaintiff (Enigma) and the defendant (Malwarebytes) to the lawsuit are software companies that sell anti-malware products to consumers. In 2017, Enigma sued Malwarebytes after discovering that Malwarebytes' products were flagging certain of Enigma's anti-malware software on consumers' computers as "malicious," "threats" or "potentially unwanted programs." Enigma alleged that Malwarebytes' actions (1) violated the Lanham Act and the New York General Business Law, and (2) constituted tortious interference with Enigma's contractual relations and business relations.

The district court granted Malwarebytes' motion to dismiss, finding that the company was entitled to immunity under Section 230 with respect to all of Enigma's claims. Section 230 provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," subject to certain exceptions for criminal and intellectual property-related claims. Under that broad protection, internet platforms and other service providers that publish third-party content are generally immune from liability for such third-party content.

Additionally, the statute provides that "[no] provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to [such material]." This

[6] A copy of the order can be found here.

provision has been relied on in several cases to grant immunity to anti-malware software providers and other providers of content-filtering technology.

On appeal, the Ninth Circuit reversed and remanded the district court's order to dismiss, holding that Section 230 does not shield Malwarebytes from liability for blocking Enigma's products for anti-competitive reasons, ruling that the phrase "otherwise objectionable," as used in Section 230, does not apply to software that the provider of anti-malware software finds objectionable for such reasons. Certain technology companies and other industry participants took issue with this ruling, arguing that the Ninth Circuit's interpretation of the scope of the immunity under Section 230 would lead to unprecedented litigation with respect to content filtering and security technologies.

Malwarebytes subsequently filed a petition to the U.S. Supreme Court for a writ of *certiorari*. The Supreme Court denied Malwarebytes' petition and remanded the case to the district court for further proceedings, though Justice Clarence Thomas filed a statement that the Supreme Court should, "in an appropriate case," consider whether the "increasingly important" Section 230 aligns with the "sweeping" immunity enjoyed by internet platforms.

Earlier this month, the district court dismissed all of Enigma's claims without ruling on whether Section 230 confers immunity for actions taken for anticompetitive reasons. Instead, the district court focused on the fact that the Malwarebytes characterizations of Enigma programs were opinions, rather than facts, and that once the Enigma programs were flagged by the Malwarebytes program, Malwarebytes users were still free to make their own determination regarding whether to quarantine the Enigma programs or not.

Key Takeaways

Enigma v. Malwarebytes has been part of the broader conversation regarding the scope of the immunity under Section 230. Most notably, there have been calls to narrow that immunity in the context of the use of social media to spread false information. However, as the discussions regarding this case make clear, revisions to Section 230 to address one issue may have consequences in other areas as well. For now, it remains to be seen whether there will be any changes to the broad statutory protection.

Return to Table of Contents

SEC Heightens Focus on Cybersecurity

On August 30, 2021, the Securities and Exchange Commission announced the resolution of enforcement actions arising from cybersecurity incidents at various companies that involved exposure of customers' and clients' personally identifying information. These SEC actions demonstrate the agency's increasing priority to address cybersecurity issues for public companies and SEC-regulated entities. Issuers and other SEC-regulated entities should continuously monitor their cybersecurity protections and disclosure controls and provide complete, accurate and timely updates to disclosures, particularly in the wake of a cybersecurity incident. Read more.

Return to Table of Contents

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