Skadden

Privacy & Cybersecurity Update

Location Data Guidance From Irish Regulators

The Irish data protection regulator has issued guidance regarding the collection and processing of location data. Companies must minimize the amount of such data that they collect and obtain specific consent from the data subjects prior to collection.

On August 9, 2016, the Irish Office of the Data Protection Commission (DPC) issued a guidance note for data controllers regarding location data.[1] The Irish regulatory body's guidance is particularly influential because the European headquarters of many large multinational companies are located in Ireland.

The DPC acknowledged that although location data can be useful in allowing companies to offer individuals numerous services, including traffic reports, driving directions and local weather reports, such data's utility comes with an increased risk to individual privacy as location data, by its very nature, can reveal "very intimate details" about a person's life.

Location Data Is Personal Data

Location data is personal data within the meaning of the Irish Data Protection Acts of 1988 and 2003 if (i) it relates to a living person and (ii) it is possible to identify that person from the location data itself or from a combination of the location data with other data that the company has or is likely to acquire. Location data that tracks a person's movements over a period of time is likely to be sufficient, by itself, to identify a person because a person's identity often can be inferred without the location data being linked to a person's name, phone number, e-mail address or other unique number. If location data provides insight into certain sensitive traits, such as religious or political beliefs, or physical or mental health (*e.g.*, by tracking visits to a place of worship or a hospital), then such location data may be deemed sensitive personal data that is subject to stricter processing requirements.

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

The DPC's guidance confirms that data collected from the movement of a smartphone should always be considered personal data because the smartphone's movements are likely those of its user. In addition, data collected from a website that relates to the location of the website user is also personal data because it indicates the user's location at the time the data is collected.

Limitations on Collection of Location Data

The DPC emphasized that data controllers must assess the need for any particular granularity or frequency of location data collection in the context in which the data is used, and must tailor their collection to that which is necessary to facilitate the use. For example, if location data is collected for purposes of an app that offers information about points of interest in an area, it is likely not necessary to collect information about a user's location every five seconds. Companies should consider whether a decreased level of granularity in location data collection (*e.g.*, county or town versus an individual building) would be sufficient for their purposes while avoiding inadvertently collecting sensitive personal data.

Consent Required

The DPC noted that data controllers must obtain personal data fairly by obtaining specific consent to the collection of the location data in certain circumstances, such as the collection of patterns of location data from smartphones. If the collection is taking place on an ongoing basis, data controllers should provide periodic reminders that location data is being collected. In addition, consent only may be obtained for the uses that are made explicit to the data subjects, and any change in the use of the data requires data controllers to obtain renewed consent. Data subjects also must be given an option to withdraw their consent to the processing of location data at any time through a simple and cost-free mechanism.

Finally, the DPC notes that data subjects have certain rights to request access to information that a company holds about them. Companies are required to provide the data subject with the information "in intelligible form," which, according to the DPC, may include plotting the location data on a map, as simply providing numerical coordinates alone is not sufficient.

Key Takeaway

Companies that are subject to regulation by the DPC should examine their location data collection practices to ensure that they are aligned with the guidance issued by the DPC, particularly as such guidance relates to the increasing collection and use of location data from smartphones.

Return to Table of Contents

FTC Requests Comments on Standards for Safeguarding Customer Information

The Federal Trade Commission has requested public comment on its Standards for Safeguarding Customer Information no later than November 7, 2016.

As part of a systematic review of all of its regulations and guidelines, the Federal Trade Commission (FTC) has requested public comment on its Standards for Safeguarding Customer Information (Safeguards Rule) no later than November 7, 2016.[2] The review process is meant to ensure that the FTC's regulations and guidelines remain relevant and are not overly burdensome on companies.

Background

The Safeguards Rule originally was promulgated by the FTC pursuant to the Gramm-Leach-Bliley Act (GLB Act), which required the FTC and other federal agencies to establish standards for financial institutions relating to the measures taken by them to protect certain customer information.[3] The Safeguards Rule, which became effective on May 23, 2003, requires financial institutions to develop, implement and maintain a comprehensive written information security program describing the administrative, technical and physical safeguards used to protect customer information. These measures must be designed to ensure the security of customer information, including protecting against any anticipated threats to the security of such information and protecting such information against unauthorized access that could result in substantial harm to the customer.

The current Safeguards Rule applies to those financial institutions under the jurisdiction of the FTC, specifically those significantly engaged in financial activities described in the Bank Holding Company Act of 1956,[4] as well as activities deemed to be financial in nature by the Federal Reserve Board at the time the GLB Act was enacted in 1999. The Safeguards Rule does not presently apply to institutions engaged in activities that the Federal Reserve Board found to be only incidental or complementary to financial activities, nor does it apply to activities determined after 1999 to be financial in nature.

[2] The request for comment can be found here.

[3] A copy of the current Safeguards Rule can be found here.

[4] See 12 U.S.C. §1843(k).

Issues for Comment

The FTC has highlighted certain issues on which it requests comment, although the public is free to comment on other issues as well. Among the issues highlighted by the FTC are:

- Should the Safeguards Rule apply to institutions significantly engaged in activities that are incidental to financial activities, or activities that were found to be closely related to banking or incidental to financial activities after the enactment of the GLB Act in 1999?
- What modifications should be made to the Safeguards Rule to increase its benefits to businesses?
- What costs, including costs of compliance, has the Safeguards Rule imposed on businesses? What modifications should be made to reduce costs?
- What modifications should be made to the Safeguards Rule to account for changes in relevant technology or economic conditions?
- Should the Safeguards Rule be modified to include more specific and prescriptive elements for information security plans, or to reference any other information security standards, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards?

Key Takeaway

Financial institutions and other interested parties should review the request for comment and consider whether to submit comments by the November 7, 2016, deadline. In addition, some pundits wondered whether the FTC would seek comment on its definition of "Customer Information." Under the Safeguards Rule, customer information is limited to nonpublic personal information about individuals who obtain or have obtained a financial product or service from the financial institution, or have a continuing relationship with a financial institution that provides personal financial products. However, the FTC elected not to seek comments on that definition.

Return to Table of Contents

NAIC Releases Revised Cybersecurity Draft Model Law

The NAIC's Cybersecurity (EX) Task Force introduced a revised cybersecurity draft model law for public comment. The draft model law, which establishes minimum data security standards and obligations applicable to insurers, is part of a greater initiative to bolster insurers' cybersecurity safeguards and instill confidence among policyholders that their personal information is protected.

On August 17, 2016, the National Association of Insurance Commissioners (NAIC) Cybersecurity (EX) Task Force released a revised draft of its Insurance Data Security Model Law (Model Law)[5] after considering comments on its initial draft, which was introduced earlier this year. The Cybersecurity (EX) Task Force, which was appointed by the NAIC executive committee in late 2014 to consider cybersecurity issues as they pertain to the role of state insurance regulators, designed the Model Law "to establish the exclusive standards in [enacting states] for data security and investigation and notification of a data breach."

In its current form, the Model Law requires "licensees" — defined to include any person or entity licensed, authorized or registered pursuant to the insurance laws of the enacting state — to develop and implement comprehensive written information security programs detailing the safeguards each licensee has in place to protect "personal information," defined broadly to include financial, health and biometric information. Each licensee's board of directors must oversee the development and implementation of the program and assign specific responsibility for the program to executive management, which in turn must provide, at least annually, written reports to the board as to the program's overall status, compliance with the Model Law and any other related material matters.

Developing a Cybersecurity Program

To develop an information security program, the Model Law requires that licensees identify "reasonably foreseeable internal or external threats" that could result in a data breach and assess those threats while taking into consideration their likelihood, the potential damage that would result should they occur and the adequacy of any safeguards in place. The Model Law further requires that licensees, at a minimum, (i) design their information security programs to mitigate identified risks "commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities," (ii) account for cybersecurity risks in their enterprise risk management process, and (iii) utilize generally accepted cybersecurity principles to share information and remain informed of emerging threats or vulnerabilities.

Data Breach Notice Requirements and Remedies

If a licensee learns that a data breach has or may have occurred, the Model Law requires that the licensee promptly conduct an investigation to assess the nature and scope of the breach. The Model Law also imposes stringent rules in the event of a data breach. The licensee must notify the insurance commissioner of

[5] National Association of Insurance Commissioners Cybersecurity (EX) Task Force, Draft Insurance Data Security Model Law (Version 2), August 17, 2016, available here.

any data breach no later than three days after the licensee learns of the breach and include in the notice certain key information (to the extent available) concerning the breach. The licensee also must notify affected consumers in writing within 60 days after identifying the data breach and provide the insurance commissioner with a draft of the proposed written notification before doing so. After reviewing the draft, the insurance commissioner must prescribe the appropriate level of consumer protection required following the data breach, and may order the licensee to offer to pay for 12 months or more of identity theft protection services for affected consumers, pay for a credit freeze or take other consumer protection actions. The Model Law also requires that the licensee notify appropriate law enforcement agencies, any relevant payment card networks and, if the breach involves personal information relating to 500 or more consumers, consumer reporting agencies. The Model Law would not supersede or otherwise displace existing laws and regulations, except to the extent such existing laws and regulations are inconsistent with the Model Law, and then only to the extent of the inconsistency.

Powers of the Insurance Commissioner

In addition, the Model Law grants the insurance commissioner certain enforcement powers, including the power to investigate the affairs of any licensee to determine whether it has engaged in any conduct in violation of the Model Law, to commence administrative proceedings if there is reason to believe that a licensee is engaged in conduct in violation of the Model Law, and to "issue such rules, regulations and orders as shall be necessary to carry out the provisions" of the Model Law.

Looking Ahead

While it remains to be seen whether and to what extent state legislatures will adopt the Model Law in its final form, the establishment of minimum data security measures and mandatory protocols for responding to a data breach may help offer some level of certainty and predictability in the aftermath of a data breach and instill confidence among policyholders that their insurers are adequately protecting personal information. Increased consumer confidence, in turn, at least theoretically may lead to greater demand for insurance across various coverage lines, and thus more premiums for insurers. Widespread adoption of the Model Law also may help promote uniformity across jurisdictions in cybersecurity requirements applicable to insurers. The key will be to strike the proper balance between achieving these goals and avoiding overly burdensome regulations. Comments on the revised Model Law are due September 16, 2016.

Return to Table of Contents

Online Retailer Reaches Data Breach Settlement With New York Attorney General

A New York online retailer agreed to pay a $100,000 penalty and implement certain security measures as part of a deal reached with the New York attorney general to settle an action brought against the retailer for failure to notify its customers of a data breach and for misrepresenting the security of its website.

Provision Supply, LLC (doing business as EZcontactsUSA.com) (EZContactsUSA) entered into a settlement with New York Attorney General Eric T. Schneiderman after the Brooklyn-based online contacts and eyewear e-tailer failed to notify customers of a data breach that resulted in the potential exposure of more than 25,000 credit card numbers and other cardholder data. Under the settlement, EZContactsUSA agreed to pay $100,000 and to improve its data security practices.

The breach occurred in August 2014 when a third party gained access to EZContactsUSA's website, but the company was unaware of the breach until its merchant bank notified it nearly a year later that fraudulent charges were appearing on customer credit accounts. EZContactsUSA hired a forensic investigation firm to conduct an investigation into the charges, after which the firm found malware and removed it from EZContactsUSA's website. EZContactsUSA never informed its customers of the breach. This failure to notify was in violation of New York's Information Security Breach and Notification Act,[6] which requires notice be provided to individuals affected by the breach and various government agencies, including the attorney general's office, in the most expedient time possible and without unreasonable delay.

The attorney general also found that EZContactsUSA misrepresented the safety and security of its website by advertising it as "100% safe and secure" and "utilizing the latest security technology available," when in reality the website contained numerous security vulnerabilities.[7] For example, EZContactsUSA failed to maintain a written security policy addressing information security problems, did not implement a firewall or anti-virus or anti-malware software on its computer systems, and did not otherwise conduct vulnerability and penetration testing.

[6] N.Y. Gen. Bus. Law Section 899-aa.

[7] The New York attorney general found that these misrepresentations violated General Business Laws §§ 349 and 350, which prohibit deceptive trade practices and false advertising.

In addition to the $100,000 penalty, the settlement requires EZContactsUSA to conduct thorough investigations of any future data security breaches, provide prompt notice of data security breaches to affected New York residents and state law enforcement agencies, maintain reasonable security policies and procedures designed to protect consumers' personal information, remediate the many security vulnerabilities found on its website, and provide security training to its employees.

Key Takeaways

Companies that experience a data breach in which personally identifiable information is compromised must be sure to comply with all applicable state data breach notification laws. A company's cybersecurity incident response plan should incorporate these notification requirements to ensure that the company provides these notices in a timely manner following a data breach. The settlement also highlights the importance of maintaining written security policies and procedures. Finally, companies should examine the statements they make to the public regarding their cybersecurity practices to confirm that those statements are factually accurate and, if they are not, take steps to reconcile the statements with actual practice.

Return to Table of Contents

Federal Health Officials Call for Scrutiny of Social Media Policies in Nursing Homes

The Centers for Medicare and Medicaid Services issued a memorandum to state health officials directing survey agencies to request and examine nursing home social media policies designed to protect the privacy of nursing home residents as part of the agencies' review process.

The Centers for Medicare and Medicaid Services (CMS), a division of the Department of Health and Human Services, issued a memorandum to state health officials on August 5, 2016, directing survey agencies to examine nursing home social media policies as part of general inspections aiding federal enforcement of compliance with Medicare and Medicaid standards and regulations.[8] The instructions come in the wake of media reports documenting dozens of posts on Facebook, Snapchat, Instagram and other social media platforms containing demeaning, embarrassing or otherwise exploitative photographs and recordings of nursing home residents.

In the memo, CMS directs survey agencies to ensure nursing homes have policies in place preventing the use of cameras and smartphones to photograph residents and post embarrassing or demeaning pictures on social media. Federal nursing home regulations require that each nursing home provide care and services in a "person-centered environment in which all individuals are treated as human beings." To this end, the regulations include provisions regarding resident privacy and mental abuse. The CMS memo explains that sharing demeaning, or even simply unauthorized, photographs and recordings of nursing home residents or their private rooms and furnishings on social media violates these regulations.

CMS notes that in addition to having policies in place, nursing home facilities should actively supervise and enforce these policies through appropriate corrective actions. The nursing homes should not only train full-time employees on the policies, but also volunteers, contractors and other caregivers. CMS further calls for the nursing homes to report, and state officials to investigate, complaints regarding these violations. Offending workers should be reported to licensing agencies for possible discipline.

The CMS memo is one of the latest reminders of the importance of maintaining and enforcing employee social media policies, particularly in the health care context. In another recent incident, Mount Sinai Hospital in Chicago has been sued under state law for intentional infliction of emotional distress in connection with a nurse's Twitter post depicting a deceased patient's blood-soaked hospital room. Notably, this incident is a cautionary tale for employees as well as companies — the nurse also is a party to the suit and could be held personally liable for significant damages. While the complaint has not yet been served, the incident has resulted in unflattering press for Mount Sinai Hospital.

Key Takeaways

For the health care industry, both the CMS memo and the Mount Sinai Hospital suit demonstrate that certain content shared on social media, such as images of private rooms and furnishings, may be subject to legal action even if it is unclear whether that content would be considered personally identifiable information under HIPAA.

Generally, the CMS memo and Mount Sinai Hospital incident serve as reminders to companies to implement, actively oversee and enforce carefully considered social media policies. Employees and other individuals associated with the company should be trained regarding appropriate social media use, and should be asked to acknowledge their understanding of the company's social media policies.

Return to Table of Contents

[8] A copy of the memorandum is available here.

DC Court Dismisses Second Data Breach Class Action Against CareFirst for Lack of Standing

In *Chambliss v. CareFirst, Inc.*, a D.C. federal court held that a data breach class action could not proceed because the named plaintiffs failed to allege an actual injury-in-fact and thus lacked standing to sue. This is the second time in three months that CareFirst has successfully defeated a putative class action based on a 2014 data breach.

On August 10, 2016, a D.C. district court dismissed a putative class action brought by CareFirst policyholders affected by a 2014 data breach, holding that the plaintiffs lacked standing because the complaint did not allege facts showing "certainly impending" harm or a "substantial risk that the harm will occur" as a result of the breach. This decision is the latest in a growing number of federal cases holding that where information is compromised as a result of a data breach, speculative harm or mere statutory violations will not suffice to establish standing. Rather, plaintiffs must identify an injury that is concrete, particularized, and actual or imminent.

Background and Claim

CareFirst, Inc. is a health insurance provider operating in Maryland, Virginia and the District of Columbia. In 2014, CareFirst suffered a data breach that compromised the personal information of 1.1 million policyholders. The breach affected subscribers' personal information, such as names, birth dates, email addresses and subscriber identification numbers. The plaintiffs' complaint did not allege that more sensitive data, such as social security or credit card numbers, was implicated in the breach.

After CareFirst announced the data breach in mid-2015, seven plaintiffs filed a putative class action against CareFirst and its affiliates, alleging that CareFirst violated a variety of state laws and legal duties by failing to safeguard policyholders' personal information. Two other policyholders filed a similar class action in a Maryland federal court, which the judge dismissed on May 27, 2016, for lack of standing.

In the D.C. action, two of the named plaintiffs alleged they had experienced tax-refund-related fraud as a result of the breach. The other five named plaintiffs alleged that as a result of the data breach they faced an increased likelihood of identity theft. All of the plaintiffs alleged they were harmed by the breach through overpayment for insurance coverage, out-of-pocket mitigation costs related to the breach, loss of the intrinsic value of their personal information and violation of their statutory rights under consumer protection acts. CareFirst moved to dismiss the plaintiffs' complaint on the ground that they lacked standing because they did not (i) allege that their personal information was misused, or (ii) explain how the stolen information could be used to assume the policyholders' identities.

The Court's Decision

Following the logic of the Maryland court's decision in the related class action, the D.C. district court dismissed the plaintiffs' claims. The court held that the plaintiffs did not have Article III standing because none of their alleged injuries constitute an injury-in-fact.

Rejecting each of the plaintiffs' theories in turn, the court first held that any increased risk of identity theft was too speculative to support a claim. The court ruled that "[a]bsent facts demonstrating a substantial risk that stolen data has been or will be misused in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from whom the information was taken." Quoting the Maryland court's decision, the D.C. court held that, "at a minimum," to find a concrete harm, the court would need to assume that the hackers had the ability to read and understand the stolen information, had future criminal intent, and had the ability to use the stolen information to the detriment of the plaintiffs.

Second, the court rejected the notion that the plaintiffs already had suffered an injury in the form of tax fraud merely because they had not yet received an expected tax refund. The court held that although tax refund fraud can satisfy the injury-in-fact requirement for standing, the plaintiffs failed to plausibly allege that their purported injury was "fairly traceable" to the data breach because their complaint did not allege that the stolen information included social security numbers, a necessary component to tax fraud.

Lastly, the court rejected the plaintiffs' other assertions of injury (*i.e.*, that they faced economic harm through overpayment of insurance and mitigation costs, that they suffered a loss of value of their information and that their statutory rights were violated) because the complaint failed to allege facts supporting any of those theories. In rejecting the plaintiffs' theory of injury-in-fact because their statutory rights were violated, the D.C. court followed the Supreme Court's recent ruling in *Spokeo v. Robins* that "statutory rights cannot confer Article III standing on a plaintiff who does not have it otherwise."

Key Takeaway

CareFirst's successful defense of two putative class actions in three months illustrates the increased difficulty plaintiffs face when alleging speculative harm in data breach cases, and the necessity of pleading facts linking any alleged actual harm to the breach. This second CareFirst decision is yet another example of courts applying *Spokeo* to reject theories of statutory harm where plaintiffs fail to allege concrete injury. Companies who suffer data breaches and subsequent litigation should carefully consider whether the complaints filed against them show actual harm as a result of the breach or at least a "substantial risk that the harm will occur."

Return to Table of Contents

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

James R. 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

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

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

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

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

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

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

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

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@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

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com