Skadden

Privacy & Cybersecurity Update

Deadline for New Safe Harbor Agreement Passes; Negotiators Remain Optimistic

U.S. and EU negotiators have failed to meet a January 31 deadline for agreeing on a replacement Safe Harbor framework to allow companies to send personal data from the EU to the U.S., but negotiations continue.

The January 31, 2016, deadline for a new Safe Harbor agreement between the United States and the European Union has passed with no agreement, but U.S. negotiators remain optimistic that they will reach an agreement in coming days. Until then, uncertainty remains as to the status of personal data transfers between the EU and the United States.

Background

As we reported in our October 2015 edition of the *Privacy and Cybersecurity Update*,[1] in October the Court of Justice of the European Union invalidated the then-current Safe Harbor framework between the EU and the United States. This framework had allowed companies to transmit personal information from the EU to the U.S., despite the EU's assessment that the United States does not have "adequate" data protection laws in place. In its *Schrems* decision, the court declared that the existing framework did not adequately protect the interests of data subjects.

As we also reported in that *Update*, the Article 29 Working Party, which is primarily comprised of representatives from the data protection authorities of each EU member state, and which generally seeks to coordinate data protection efforts in the EU, issued a statement in mid-October stating that it would give U.S. and EU negotiators until January 31, 2016, to agree on a new Safe Harbor framework. According to the statement, if the deadline was missed and if EU regulators determine that the other mechanisms do not afford adequate data protections, national authorities will take "all necessary and appropriate actions" to protect personal data. These may include "coordinated enforcement actions" against violators.

[1] Available online at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_Update_October_2015.pdf.

Deadline Missed, But Negotiators Still Working on Replacement Framework

Despite an intense effort by EU and U.S. negotiators, the January 31, 2016, deadline has passed with no new Safe Harbor agreement. However, according to statements to the media and a report via conference call on January 29, representatives from the U.S. Department of Commerce that have participated in the negotiations have indicated that the negotiators are focusing on having an agreement by February 2, when EU data protection authorities are scheduled to meet. However, the U.S. negotiators note that even the new deadline is non-binding, as it was not required by any legislation or statute or imposed by the *Schrems* decision.

According to reports and statements from the Department of Commerce representatives, key outstanding issues include (a) U.S. intelligence agencies' ability to access information, (b) the ability of EU data subjects to obtain redress for misuse of their information and (c) the EU's desire for there to be independent data privacy regulators in the U.S. who can resolve individual complaints. U.S. negotiators say they are optimistic that they can reach an agreement soon. Some media reports suggest, however, that their EU counterparts are not as optimistic.

Uncertainty and Next Steps

While negotiators work to develop a replacement Safe Harbor, it is not clear whether local data protection authorities will refrain from taking action to prevent improper data transfers now that the initial January 31 deadline has passed. During this period of uncertainty, companies seeking to transfer personal information from the EU to the U.S. face a difficult problem. The existing Safe Harbor no longer affords protection and, following *Schrems,* the effectiveness of the other two main alternate methods — the use of the EU-approved model contracts and binding corporate rules — remains uncertain. Absent any other approved mechanisms, however, and recognizing that their status could change, if companies must transfer personal data from the EU to the U.S., the model contracts approach and binding corporate rules approach may be the safest for now.

Return to Table of Contents

Delaware Multipronged Privacy Law Goes Into Effect

A new Delaware law addressing online marketing to children, posting of privacy policies and privacy protections for digital book services went into effect January 1.

A new Delaware law regulating the way certain services may collect personally identifiable information (PII) about users went into effect on January 1, 2016. The Delaware Online Privacy and Protection Act (DOPPA),[2] which very closely tracks the California Online Privacy Protection Act, defines PII as information that can be used to distinguish or trace the identity of the individual, including, for example, the individual's name, physical characteristics, residence, financial information and passport number. DOPPA addresses three distinct issues: (a) online marketing or advertising to a child, (b) privacy policy posting and (c) privacy protections for users of digital book services. The Delaware Consumer Protection Unit of the Department of Justice may investigate and prosecute violations of the law.

Prohibitions on Online Marketing or Advertising to a Child

Under DOPPA, website, application and other Internet service providers are subject to important restrictions on the types of advertising they can display to children.

- **Prohibition on Advertising Certain Content on Services Directed to Children.** Websites, apps and other Internet service operators may not market or advertise certain enumerated products or services — including alcohol, tobacco, firearms and tattoos — if their service is directed to children.
- **Limits on Advertising Certain Content on Services Not Directed to Children.** Websites, apps and other Internet service operators that are not directed toward children but that have actual knowledge that a child uses the site may not use PII to market or advertise those enumerated products and services.
- **Limits on Third-Party Advertising Services.** Websites, apps and other operators of Internet services directed to children must notify any advertising services they use that the service is for children, and upon such notice the advertising service may not market or advertise those enumerated products and services.

It is important to note that, under DOPPA, all minors under the age of 18 are considered "children." This age is significantly higher than the 13-year-old limit set under the federal Children's Online Privacy Protection Act, which addresses the types of information that companies can collect about children.

Commercial Internet Service Providers Must Post Privacy Policies

Under DOPPA, an operator of a commercial Internet service that collects PII through the Internet about Delaware residents visiting the site must make its privacy policy "conspicuously available." The policy will be considered conspicuously available

[2] Del. Code Ann. tit. 6 § 12C.

if it is either displayed or linked to on the website's homepage in a way that stands out so that a reasonable individual would notice it (*e.g.*, with contrasting color or font from the rest of the page).

This privacy policy must contain certain information, including categories of PII collected, third parties with whom PII is shared and processes through which users may review and request changes to PII collected about them. The policy also must contain information about how the operator informs users of material changes to the policy.

The new law limits the circumstances in which an operator can be found liable for violating these requirements. First, the operator must be either (a) knowingly and willfully violating the law or (b) negligently and materially violating the law. Second, operators have 30 days after notice of noncompliance to post the privacy policy as required.

Privacy Information Regarding Book Service Users

Finally, DOPPA prohibits digital book service providers from disclosing users' PII to law enforcement and governmental entities or to other persons, except in certain detailed circumstances. For example, providers may disclose such information if there is a legal obligation to do so pursuant to a court order if certain conditions are met, and in situations where there is an imminent danger or death or serious physical injury.

Providers that disclose information relating to 30 or more total users (either in Delaware or from unknown locations) also must post a publicly available annual report on their disclosures of users' PII.

Commercial entities only fall under the law if book service sales exceed 2 percent of the entity's total annual gross sales of consumer products sold in the United States.

Key Points to Note

DOPPA closely tracks the California law, so companies compliant with California law likely will be compliant with DOPPA as well. However, it is important to note that DOPPA is more expansive than the federal Children's Online Privacy Protection Act, so companies should be particularly careful about advertising enumerated products and services and collecting PII if they know users under 18 years of age access their online services.

Return to Table of Contents

Changes to California Breach Notification Go Into Effect

Amendments to California privacy laws on data breach notification and on using automated readers of license plate data went into effect January 1.

Effective January 1, 2016, three important changes to California's data breach laws went into effect.[3] The first[4] deals with the specific information that must be included in data breach notification letters. The second[5] clarifies the definition of "encrypted" for purposes of data breach notifications. The third addresses regulations for users of and information resulting from automated readers of license plate data.

Notification Letter Changes

In an effort to make data breach notifications simple for consumers to understand, California has specified headings and titles that must be clearly and conspicuously displayed. Specifically, notifications must be titled "Notice of Data Breach" and must present the information under headings that address issues notification recipients might want to see addressed:

- "What Happened?"
- "What Information Was Involved?"
- "What We Are Doing"
- "What You Can Do"
- "For More Information …"

Notifications must include a general description of the breach incident (if known); a list of the types of personal information reasonably believed to be the subject of the breach; and the date, estimated date or date range of the breach (if known). Notifications also must state the name and contact information of the reporting organization and, if the breach involved social security numbers, driver's licenses or California identification card numbers, the toll-free numbers and addresses of the major credit reporting agencies. Additionally, notifications must state whether the notification was delayed as a result of a law enforcement investigation.

[3] Cal. Civ. Code §§ 1798.29, 1798.82, 1798.90.5.
[4] Cal. Civ. Code §§ 1798.29, 1798.82.
[5] Cal. Civ. Code §§ 1798.29, 1798.82.

At the discretion of the reporting organization, the notifications also may include information detailing what the organization has done to protect individuals whose information was breached, and advice on steps individuals whose information was breached may take to protect themselves.

The amendments even include specific formatting requirements. Notification letters must be in font larger than 10-point size and should be formatted in such a way as to call attention to the significance of the information provided. The amendments also provide a model notification form, which satisfies the law's requirements.

Organizations that must submit security breach notifications to more than 500 California residents as a result of a single breach must submit a sample notification to the attorney general, excluding personal information. Notice may be provided in writing or electronically, so long as the notice abides by electronic records and signature requirements under the United States Code, or substitute notice by email, conspicuous posting or through the media, if the other forms of notice would be too expensive or have to be sent to too large a number of individuals.

Defining "Encrypted"

Another amendment to California's data breach notification laws clarifies the definition of "encrypted." Under the state's existing law, companies that suffer a data breach do not need to notify California residents whose personal information was compromised if the information is properly encrypted. There was some confusion, however, as to what would be considered encrypted.

Under the amendment, information is encrypted if it is "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." As with most states, California has opted not to include a specific encryption standard, deferring instead to industry norms.

Automated License Plate Recognition Technology

Finally, California's data privacy laws have been amended to expand the definition of "personal information" to include certain information collected through automated license plate recognition technology (LPR). Many local police departments in California use LPR to extract license plate numbers from video images of motor vehicles and they store this information in searchable databases. The amendment expands existing California privacy laws to apply to this license plate information. The amendment adds additional requirements for both public and private entities that obtain and use LPR information, including maintaining reasonable security procedures and practices to protect the LPR information, as well as implementing a usage and privacy policy. It also requires operators to maintain records of those who access the LPR information, and only allows such access for authorized purposes.

The amendment provides a right of action to individuals harmed by a violation of the bill's provisions against a person who knowingly caused the harm.

Key Points to Note

California often has taken the lead in enacting privacy and information security laws, so these new amendments may be a sign that similar laws will be passed in other states that do not already have similar laws in place. In the data breach notification requirements in particular, these changes may reflect growing dissatisfaction among privacy advocates over the form and content of data breach letters sent to consumers in the past.

Companies that are preparing data breach notification letters likely will use the California requirements as a model for letters sent under many different state laws, in order to avoid creating different letters for each jurisdiction.

Return to Table of Contents

Illinois Courts Consider the State's Biometric Information Privacy Act

Two Illinois courts recently considered the reach of Illinois' Biometric Information Privacy Act, shedding light on how the act may be applied.

Two different Illinois courts recently considered Illinois' broadly worded Biometric Information Privacy Act (BIPA),[6] with differing results. In each case, the plaintiffs alleged that the defendants violated BIPA by using automatic facial recognition algorithms on photographs loaded to their websites.

Background of BIPA

BIPA originally was enacted in 2008, in response to concerns regarding the increased use of biometrics in the commercial and security sector. The Illinois legislature noted that because biometric data is uniquely tied to an individual, if such data was compromised, the individual has no recourse or ability to change his or her identifier. BIPA regulates the collection, storage and use of this information.

[6] 740 Ill. comp. stat. 14/1 (2008).

Since it was passed, there has been concern over the scope of BIPA's definition of "biometric identifiers," which includes retina or iris scans, fingerprints, voice prints, or scans of hand or face geometry. Many have questioned whether the definition is so broad as to apply to features that scan photographs in social media to identify people.

Private entities that collect biometric identifiers are required to have and comply with a written policy that sets out a retention schedule and guidelines for destruction of biometric information. At a minimum, the biometric information must be destroyed within three years of the individual's last interaction with the private entity. BIPA also sets forth guidelines on when the information can be disclosed or disseminated, including requiring private entities to obtain the consent of each person and to meet a reasonable standard of care within the private entity's industry for storing, transmitting and protecting the biometric identifiers.

Where a plaintiff can demonstrate that a private entity was negligent in its failure to comply with the statute, BIPA provides for a private right of action, and a private entity can be held accountable for the greater of either $1,000 or the sum of the actual damages. In instances where the plaintiff shows the defendant acted intentionally or recklessly, the recovery is increased to the greater of $5,000 or the sum of the actual damages. The statue also provides for the collection of attorneys' fees and other any other relief as the court may deem appropriate.

Norberg v. Shutterfly[7]

On December 29, 2015, the U.S. District Court for the Northern District of Illinois denied Shutterfly Inc. and its subsidiary ThisLife LLC's motion to dismiss a lawsuit alleging Shutterfly's use of facial recognition technology to gather biometric data from users' photos violated BIPA. Shutterfly is a widely used photo publishing service through which customers create photo books, calendars, cards and other materials using their own photographs.

In the complaint, the plaintiff alleged that Shutterfly analyzed photographs uploaded to its site and used this information to identify the plaintiff in other photographs. The court concluded on a plain meaning interpretation of the statue that the plaintiff stated a claim for relief under BIPA, because the suit alleged Shutterfly was scanning the geometry of the faces in the photographs, which falls within the definition of a biometric identifier under BIPA. The court also noted that the suit alleged that the plaintiff was not presented with a written policy, nor did he consent to the defendants using his biometric identifiers.

The court concluded that personal jurisdiction could be established in the case, finding that although the defendants are incorporated in Delaware and headquartered in California, Shutterfly provides hard-copy photographs and other products directly to customers in Illinois and is registered to do business in that state.

Gullen v. Facebook[8]

On January 21, 2016, also in the Northern District of Illinois, Facebook succeeded in having a BIPA claim against it dismissed for lack of personal jurisdiction.

The plaintiff, who was not a Facebook user, had his photo uploaded to Facebook by a third party. He alleged that Facebook then violated BIPA when it scanned the plaintiff in the photo to generate biometric identifiers and used the identifiers to create a template of the plaintiff's face, allowing the third-party Facebook user to "tag" the photo with the plaintiff's name.

Without discussing the merits of the claim, the court dismissed the case for lack of personal jurisdiction. According to the court, the plaintiff could not establish that Facebook "targets its alleged biometric collection activities at Illinois residents" and the mere fact that its interactive site is accessible to Illinois residents did not establish personal jurisdiction in the case.

Key Points to Note

The *Shutterfly* and *Facebook* decisions illustrate courts' ongoing struggle to apply state laws to companies that are based in other states but whose services are available online and therefore nationally. In the *Shutterfly* case, the additional fact that the company shipped products into Illinois distinguishes it from the *Facebook* case. More generally, online companies need to take into account BIPA and other similar laws when developing and offering services. We expect that as technologies utilizing biometric information increase, we are likely to see a growing number of state, or even federal, laws.

Return to Table of Contents

European Court Affirms a Company's Right to Monitor Employee's Use of Company Computer Systems

The European Court of Human Rights has rejected an individual's claim that his former employer violated his rights when it monitored his access to company computers and then used the records of that access in a litigation against the employee.

[7] *Norberg v. Shutterfly, Inc.*, No. 15 CV 5351 (N.D. Ill. Dec. 29, 2015).

[8] *Gullen v. Facebook.com, Inc.*, No. 15 CV 7681, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016)

A recent decision of the European Court of Human Rights (ECHR) in *Bărbulescu V. Romania (Application No. 61496/08)* has confirmed that there was no violation of an employee's right under Article 8 of the European Convention on Human Rights (the right to respect for private and family life, the home and correspondence) where an employee was dismissed for using his employer's computer systems for personal purposes during working hours. It found that, although the employee's Article 8 right had been engaged, the employer's monitoring of his communications pursuant to its internal regulations had been reasonable in the context of disciplinary proceedings.

The plaintiff was employed by a private company in Romania. At his employer's request, he created a Yahoo Messenger account to respond to clients' enquiries. On July 13, 2007, the company informed the employee that his Yahoo Messenger communications had been monitored from July 5-13, 2007, and that the records showed that he had used the Internet for personal purposes, contrary to internal regulations. When the employee denied this, he was presented with a transcript of messages he had exchanged with, among others, his fiancée and his brother, some of which related to personal matters such as his health and sex life. His employment was terminated on August 1, 2007, for breach of the employer's regulations.

The employee claimed that his employer had violated his right to correspondence protected by the Romanian Constitution. The Romanian County Court dismissed his complaint on the grounds that his employer had complied with domestic legislation on disciplinary proceedings and that he had been duly informed of the employer's regulations prohibiting use of company computers for personal purposes. Following an unsuccessful appeal, the employee applied to the ECHR, contending that the employer's conduct had disproportionately infringed his Article 8 rights.

The ECHR accepted that Article 8 was engaged as the employer had accessed the employee's Yahoo Messenger account and used the transcripts of his communications as evidence in the domestic litigation. It held, however, that there had been no violation of Article 8. In the ECHR's view, it was not unreasonable for the employer to seek to verify that employees were completing their professional tasks during working hours. Furthermore, the employer had accessed his messaging account in the belief that it contained client-related communications only.

Key Takeaway

It is worth noting that the employer in this case had in place internal regulations, which expressly prohibited the use of the employer's computer systems for personal use. This was taken into account by both the domestic courts and the ECHR and therefore highlights the importance of having well-drafted IT policies in the workplace and bringing these to the attention of employees. This is particularly true if the employer wants to reserve the right to monitor communications in the workplace, take necessary action for the purpose of protecting its IT systems and ensure its employees are carrying out their tasks during working hours.

Return to Table of Contents

EU Member States Approve First EU-Wide Cybersecurity Legislation

The EU is close to approving a major directive on network security and security incident notifications that will apply to providers of essential services, including some that are not based in the EU.

After nearly three years of negotiation, the European Union is close to establishing the first EU-wide legislation on cybersecurity. The legislation would impose network security and incident notification obligations on providers of essential services across the member states.[9] While the EU has focused prominently on the personal privacy of its citizens in other initiatives, the Network Information Security (NIS) Directive aims to increase competency and cooperation throughout the EU on cybersecurity matters in order to ensure a high common level of network and information security and to minimize disruption to essential services. The directive would place requirements on governments and companies to achieve these goals.

Overview of the Directive

When and if approved, the directive would require member states to establish competent national authorities and Computer Security Incident Response Teams (CSIRT) to provide cross-border support and strategic cooperation. The directive contains rules and best practices designed to promote cooperation through sharing of early threat warnings and other cybersecurity intelligence.

Notably, the directive also would impose obligations on public and private entities that provide a service that is "essential for the maintenance of critical societal or economic activities," where such a service depends on network and information systems, and where security incidents could have significant disruptive effects on the services provided or public safety. Such providers will be required to implement "appropriate and proportionate" security systems and to notify competent authorities of security incidents.

[9] The most recently publicized draft of the text, a finalized version of which has not yet been released, can be found at http://www.consilium.europa.eu/en/press/press-releases/2015/12/pdf/st15229-re02_en15_pdf.

The directive divides these service providers into two categories — operators of essential services and digital service providers — with varying security and notification requirements.

Essential Service Operators

Because the NIS Directive is primarily aimed at ensuring the continuous functioning of essential services, it imposes high security standards on what it deems "operators of essential services." Essential service operators covered by the law fall into the following specific categories:

- energy;
- transport;
- banking;
- financial market infrastructures;
- health;
- drinking water supply and distribution (excluding those who distribute water for human consumption as only part of the general distribution of goods and commodities); and
- digital infrastructure (including DNS service providers, internet exchange points, and top-level domain name registries).

Each member state is required to maintain and update a list of essential service operators in its territory, or to otherwise devise "objective quantifiable criteria" to communicate which providers will fall under its jurisdiction. Essential service operators may fall under the jurisdiction of more than one member state.

Broadly, the NIS Directive mandates that essential service operators adopt "appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems which they use in their operations." Recognizing that the requirements must be flexible due to constantly evolving technology, the directive makes no specific recommendations as to measures that must be undertaken, but notes that the network and information security systems of essential service operators must have "regard to the state of the art." The directive indicates that member states will be able to impose stricter requirements than those laid out in the directive.

In addition to system security requirements, essential service operators will be required to notify competent authorities "without undue delay" after experiencing a security incident that has a "significant impact" on the provision and continuity of the operator's service. In determining whether notification is necessary, operators should consider the number of service users affected, the duration of the incident, and the geographical spread affected by the incident. The notification must include all information relevant to enable the competent national authorities or CSIRT to determine the cross-border impact of the incident. The competent authorities may further notify the public if necessary to manage the incident or prevent further disruptions.

Digital Service Providers

The NIS Directive also applies to entities that provide critical digital services. These include providers of online marketplaces, search engines and cloud computing services, but do not include small or micro-enterprises with fewer than 50 employees and an annual balance sheet total under €10 million.

Unlike essential service operators, a digital service provider only will fall under the jurisdiction of the single member state in which it has its "main establishment" in the EU. A digital service provider with no physical presence in the EU nevertheless may be subject to the directive if it "offers services" within the EU. This can be determined, for example, by whether the provider's services are offered in the language of or using the currency of one or more member states. Where a covered digital service provider does not have a physical presence in the EU, it must designate a representative in one of the member states in which it offers services.

Digital service providers have to implement "state of the art" security systems that are "appropriate and proportionate" to the risks presented by their systems and also meet specific security guidelines. Security measures undertaken by digital service providers should take into account the security of systems and facilities, incident management, business continuity management, monitoring, auditing and testing, and compliance with international standards.

Under the directive, a digital service provider must notify competent authorities "without undue delay" after experiencing a security incident that has a "substantial impact" on the provision of its service. In addition to the number of users affected, the duration of the incident and the geographical area affected, digital service providers must consider the extent of the disruption of the functioning service, as well as its impact on other economic and societal activities. The competent authority or CSIRT may inform the public about individual incidents, or require the digital service provider to do so, when disclosure is necessary to manage or prevent an incident, or is otherwise in the public interest.

Enforcement and Interaction with Other Laws

In implementing the directive, member states are instructed to craft sanctions for noncompliance that are "effective, proportionate, and dissuasive." The directive further empowers authorities to audit covered service providers for suspected noncompliance and to issue "binding instructions to the [providers] … to remedy their operations." Providers who are found to have

knowingly failed to submit a security incident notification will be subject to penalties.

Although the NIS Directive would be the first EU-wide cybersecurity legislation, some existing sector-specific regulatory regimes already target network security issues. Where current or future sector-specific EU legal acts provide protection that is at least equivalent to the NIS Directive, the sector-specific acts will instead apply to the directive.

It is also important to consider the relationship of obligations imposed under the proposed EU General Data Protection Regulation (GDPR) and the directive. The GDPR is primarily concerned with securing personal data, while the NIS Directive seeks to ensure the continuity of services that are essential to a functioning society. How the NIS Directive and GDPR will interact at the enforcement level is uncertain. While there likely will be additional liability when both laws are violated, it is unclear if compliance with one will provide any defense against enforcement under the other.

Next Steps

The NIS Directive was approved by the member states on December 18, 2015, and was endorsed by the Internal Market Committee of the European Parliament on January 14, 2016. Formal approval by the European Council and Parliament is expected by spring, after which member states will have 21 months to implement the directive by passing legislation in accordance with its provisions. The member states will then have six months to identify the operators of essential services to which the law will apply. It is predicted that the directive will enter into force in spring of 2018.

Return to Table of Contents

Facebook's 'Friend Finder' Violates German Privacy Laws

In a decision relating to German competition and privacy law, the German Federal Court of Justice found that Facebook's "Friend Finder" feature is unlawful.

On January 14, 2016, the German Federal Court of Justice ruled that the 2010 version of Facebook's "Friend Finder" feature violated German unfair competition and advertising laws. This service allowed Facebook to send invitations on behalf of its members to Internet users who were not registered on Facebook. The court also found that the Friend Finder registration procedure misled Internet users, as they were not provided with sufficient information regarding the use of their personal data. The full judgment has not yet been published.

Background

At issue was Facebook's Friend Finder tool, which invited users to grant Facebook permission to collect the e-mail addresses of friends or contacts in the user's address book. After collecting these addresses, Facebook could then send invitations to non-Facebook members to join the service.

The Federation of German Consumer Organizations (*Verbraucherzentrale Bundesverband* (VZBV)) brought its action against Facebook in November 2010, arguing that the users who were not registered on Facebook never had consented to receiving emails from Facebook through this service. The regional court of Berlin granted the action in March 2012.[10] This decision was confirmed by the chamber court in Berlin in February 2014.[11]

German Privacy Laws and the Ruling

In this case, the VZVB (as plaintiff) argued that the Facebook feature violated the German Unfair Competition Act, a statute originally implemented in 1909, which had undergone various amendments since 2004 and which provides rules on the protection of businesses, consumers and other market participants from unfair business practices.

Among other things, the German Unfair Competition Act generally prohibits business practices that unreasonably harass market participants.[12] This particularly applies to advertising in cases in which it is apparent that the addressed market participant does not wish to be provided with the advertisements. The use of automated telephone, fax or e-mail is always considered unreasonable harassment for these purposes unless the explicit consent of recipients has been obtained.

Moreover, the German Unfair Competition Act generally prohibits misleading business practices that may cause a consumer or other market participant to make a business decision that he would not have made otherwise.[13] A business practice is misleading if it contains untrue information or information that is likely to deceive or to cause confusion.

The Federal Court of Justice declared that the invitations to non-registered users are deemed to be advertisements from Facebook even though they are sent by Facebook's members, because the feature applied is provided by Facebook and is

[10] See Regional Court of Berlin, March 6, 2012 – 16 O 551/10.

[11] See Chamber Court in Berlin, January 24, 2014 – 24 U 42/12.

[12] Sec. 7 paras. 1 and 2 of the German Unfair Competition Act.

[13] Sec. 5 para. 1 of the German Unfair Competition Act.

intended to promote the Facebook services to these users. The recipients would not regard the invitations as private emails from the Facebook members, but as an advertisement by Facebook.

Also the information provided by Facebook in its November 2010 Friend Finder registration procedure was deemed in violation of the German Unfair Competition Act. The court held that Facebook had been deceptive about the type and scope of use of email contact data. In particular, although the first question in the registration step was "Are your friends already on Facebook?" it was not made clear that email contact data would be analyzed and that invitations would be sent to friends who are not registered on Facebook. Further, the statement "Your Password will not be stored by Facebook" was not sufficient to clear the caused deceit because it could not be assured that the user had taken note of it.

Impact of Decision

The decision not only will affect Facebook, but also many other companies that use similar features. Companies have to consider Germany's privacy laws and review their online services to the extent they access the user's address books.

Facebook modified its Friend Finder feature prior to the date on which the court judgment was handed down. It is not yet clear if the current version will be affected by this judgment. The full judgment should provide further clarification following its publication.

Return to Table of Contents

FTC Releases Report on 'Big Data'

The FTC has released a report on the use of "big data" that highlights the commission's concerns that big data can adversely impact low-income and underserved populations. It also may signal that the commission intends to apply existing laws to limit this impact.

On January 6, 2016, the Federal Trade Commission issued a report titled "Big Data: A Tool for Inclusion or Exclusion," in which it discussed the risks and rewards the use of big data can present, particularly as applied to low-income and underserved populations.[14] Part legal overview, part policy document, the report highlights the commission's focus on the impact of big data practices and provides some guidance on what legal tools the commission may use to reduce their adverse effects.

[14] The report is available online at https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

Scope of the Report

The FTC's report focused solely on the use of big data, not its collection, consolidation, storage or analysis. It described the risks and benefits created by the use of big data, summarized some of the research on this use and suggested some lessons that can be learned from the research. It also provided an overview of the consumer protection and equal opportunity laws applicable to the use of big data, and the commission's role in enforcing those laws.

Benefits and Risks of Big Data

In the report, the commission notes some of the benefits and risks posed by the use of big data, though it focuses more on the latter than the former. As examples of benefits, the report cites how big data helps target educational, credit, health care and employment opportunities to low-income and underserved populations. On the other hand, big data can be prone to unintentional inaccuracies and biases both in how the data is selected and how the resulting analysis is applied. These inaccuracies and biases can lead to detrimental effects for low-income and underserved populations. For example, analysis of a data set based on online buying habits could lead to special offers being made available online that aren't available to those that do not use technology as frequently.

Consumer Protection Laws Applicable to Big Data

In the report, the commission identifies a handful of laws that might apply to the use of big data. Chief among these are the Fair Credit Reporting Act (FCRA) and various equal opportunity laws.

Fair Credit Reporting Act

Under the FCRA, companies that compile and sell consumer reports that are used for credit, employment, insurance, housing or other similar decisions about consumer eligibility for benefits and transactions must (a) implement reasonable procedures to ensure maximum possible accuracy of consumer reports and (b) provide consumers with access to their own information and the ability to correct errors. Classic examples of these types of companies include credit bureaus, employment background screening companies and other specialty companies that provide specialized services. Big data is enabling more companies to use different types of data for these types of purposes, some of which may not even consider themselves subject to the FCRA.

In the report, the commission described an increasing use of predictive analytics for eligibility determinations, some of which are purchased from third parties. These methods take known characteristics about a consumer to make predictions about future behavior. For example, data may predict that consumers that frequently make late payments are not good credit risks.

Companies are increasingly using non-traditional data sets — such as zip codes, social media usage and shopping history — in these analyses. The commission noted that use of these characteristics is subject to the same standards as apply to more traditional methods.

Equal Opportunity Laws

The commission also identified a number of federal equal opportunity laws that might apply to the use of big data. These include the Equal Credit Opportunity Act (ECOA), Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, and the Fair Housing Act. These laws generally prohibit discrimination based on certain protected characteristics, such as race, color, sex, religion and marital status.

In the report, the commission notes that it is responsible for enforcing the ECOA, which prohibits credit discrimination based on characteristics such as race, religion or national origin. Claims may be based on disparate treatment or disparate impact. Disparate treatment occurs when a company treats an applicant differently based on one of these characteristics, even if big data analysis shows conclusively that the company would benefit from that different treatment. For example, even if big data shows that married people are better credit risks than single people, companies cannot offer different rates or benefits based on their marital status.

Disparate impact occurs when use of facially neutral policies nevertheless has a disproportionate adverse impact on a protected class. For example, a policy that offers inferior benefits based on zip codes may, in effect, have a disparate impact on certain ethnic or religious groups that disproportionately live in certain zip codes. There are some situations in which a disparate impact does not violate the law, but companies should think carefully about their practices to assess the risk that they may violate the ECOA.

Research on Big Data

Finally, the report summarized some of the key questions that companies should ask about their data practices and how they may impact certain groups.

- **How representative is your data set?** Companies should consider whether certain groups are under-represented in their data sets. Data collected online, for example, will likely underrepresent groups that are not as engaged with technology, such as the elderly or the poor.
- **Does your data model account for biases?** Some data analytics may incorporate underlying societal inequalities, and companies should try to identify those biases and account for them. For example, an algorithm that only considers applicants from top colleges and universities for hiring decisions may incorporate prior biases in college admissions.
- **How accurate are your predictions based on big data?** The commission noted that, while big data is a useful tool for identifying correlations, it does not provide context or explanations for those correlations. For example, the Google Flu Trends algorithm uses searches for flu-related terms to predict flu outbreaks. However, a spike in searches could be the result of something different than a flu outbreak, such as high-profile news stories about the flu in other countries.
- **Does your reliance on big data raise ethical or fairness concerns?** Companies should examine the factors that go into their analytics models and assess whether they raise fairness concerns. As an example, a company that favors people who live close to the office for employment decisions may unintentionally be incorporating a racial bias into the employment process if different neighborhoods have different racial compositions.

In short, the commission is seeking to encourage companies to evaluate their use of big data and try to identify possible areas where they may be incorporating unintentional biases into their decisions. For its part, the commission will continue to monitor big data practices and whether they violate existing laws.

Key points to note

The FTC's report demonstrates the commission's continuing concerns about the use of big data by businesses. Its detailed discussion of applicable laws and potential violations may well signal a new enforcement initiative as the commission tries to limit the adverse effects the use of big data may have on consumers. From the subtext of the report, however, it is clear that the commission sees limits on its authority to prevent some of the harms that can arise. If its experience in the coming years shows that existing laws are inadequate to prevent what the commission sees as the adverse impacts of big data, it may well push Congress to pass new laws to address these issues.

Return to Table of Contents

FTC Fines Software Provider for Deceptively Advertising Data Security Technology

For the first time in a data security settlement, the FTC has included a monetary penalty in a consent order, seemingly as a result of misleading statements about the encryption offered by the service at issue.

On January 5, 2016, the Federal Trade Commission announced its first data security settlement that included a monetary penalty. In the case, a dental office management software provider agreed to a proposed $250,000 settlement to resolve charges that the provider deceptively claimed its software possessed industry-standard encryption technology, and that clients could rely on such software to satisfy certain regulatory requirements under federal health privacy laws.[15]

Background

The FTC's complaint was based on claims Henry Schein Practice Solutions Inc. (Schein) made in connection with Dentrix G5, a proprietary software product Schein began marketing in 2012. Dentrix G5 is used to perform office tasks that routinely involve collecting and storing sensitive patient information (*e.g.*, entering patient information into the system and processing patient payments). Doctors must satisfy certain regulatory obligations under the Health Insurance Portability and Accountability Act (HIPAA) with respect to protecting sensitive patient information, including, in the event of a data breach, informing patients that their information has been compromised. However, the technology used to protect patient data impacts the steps a doctor must take: If patient data is encrypted using industry-standard technology, consistent with guidance promulgated by the National Institute of Standards and Technology (NIST), doctors have a "safe harbor" and are not obligated to inform patients of the breach.[16]

According to the FTC's complaint, as early as November 2010 Schein's database engine vendor informed Schein that Dentrix G5 used a proprietary algorithm that had not been tested publicly and was "less secure and more vulnerable than widely used, industry-standard encryption algorithms."[17] Nevertheless, Schein, according to the FTC, marketed Dentrix G5 as industry-standard encryption technology that would help doctors satisfy their regulatory requirements.[18] Moreover, Schein subsequently received confirmation that Dentrix G5's data protection capabilities were weak relative to encryption technology. On June 10, 2013, the United States Computer Emergency Readiness Team, a unit of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, issued a vulnerability note describing the Dentrix G5 as a "weak obfuscation algorithm"; three days later, NIST published a corresponding alert.

In response to the government inquiries, the vendor agreed to rebrand its data protection as "Data Camouflage" so as to distinguish it from encryption technology. Schein, however, continued to market Dentrix G5 as offering "encryption" for several months following the vulnerability notices. After a series of media reports highlighted Schein's failure to rectify its encryption claims, Schein conceded in a June 2014 statement that referring to the product's data protection capabilities as "a data masking technique using cryptographic technology" would be "more appropriate" than calling it encryption. Schein then removed references to encryption from its marketing materials and added qualifying language stating that Dentrix G5 does not replace a dentist's own security measures to protect patient data.

FTC's Complaint and Consent Order

The FTC filed a complaint against Schein alleging that it had engaged in unfair or deceptive acts or practices in violation of Section 5(a) of the Federal Trade Commission Act. In particular, the FTC accused Schein of engaging in false or misleading practices in two specific respects: (a) claiming that Dentrix G5 provided industry-standard encryption and (b) claiming that Dentrix G5 helps protect patient data as required by HIPAA.

Under the terms of the proposed consent order Schein will (a) pay $250,000 for consumer relief, (b) refrain from making future misleading statements about the data security strength of its products and (c) take steps to notify customers that, contrary to Schein's advertisements, Dentrix G5 uses less complex technology to protect patient data than the industry standard.

Key Points to Note

The FTC has indicated that the sensitive data at issue rendered Schein's misrepresentations particularly egregious, though it

[15] The FTC has, however, requested damages in relation to data security false advertising claims under other circumstances. On December 17, 2015, Lifelock agreed to pay $100 million to consumers to settle FTC claims that the company violated a 2010 consent order related to Lifelock's alleged deceptive data security advertising. See "Lifelock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order," *available at* https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

[16] See 45 C.F.R. §§ 164.400-414.

[17] The complaint is available online at https://www.ftc.gov/system/files/documents/cases/160105scheincmpt.pdf.

[18] Among other examples, the FTC pointed to a Schein newsletter article that stated its database stores "customer data in an encrypted format. With ever-increasing data protection regulations, Dentrix G5 provides an important line of defense for both patient and practitioner."

did not specifically tie the monetary penalty to that conclusion. "Strong encryption is critical for companies dealing with sensitive health information," said Jessica Rich, director of the FTC's Bureau of Consumer Protection. "If a company promises strong encryption, it should deliver it."[19] The sentiment is in line with the increasingly prominent role the FTC has tried to play in data security regulation as Congress has, in recent years, failed to pass a data breach bill that would set nationwide security standards.

[19] `The FTC statement is available online at https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled.

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

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