WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

Data Privacy & Security Watch

Spring 2015

Letter from the Chair of the Communications, Media & Privacy Department

As data privacy and cybersecurity matters continue to increase in frequency and prominence in the news, in regulatory enforcement offices, in Congress and the White House, and in corporate boardrooms, it has become essential for in-house counsel to remain fully informed of the key issues in this space that affect their businesses. Multiple high-profile cyber attacks launched against major retailers, insurance companies, financial institutions, and others – many backed by organized crime syndicates or even sovereign nation states – have captured headlines, highlighting the enormous legal, regulatory, and reputational risks faced by companies. Hundreds of millions of people have seen their sensitive personal information stolen and misused, leading federal and state regulators to focus a glaring spotlight on the data security practices of American companies of every size and in every industry sector.

For some time, the business and legal risks associated with data privacy and security issues have been frustratingly abstract and opaque, with the relatively few clear rules making it difficult for companies to assess potential liabilities, enforcement risk, and the possibility of future regulations. We anticipate that 2015 will be a year of rapid change as those risks start to be clarified and, in some cases, amplified. It has become more important than ever for companies to understand the data privacy and security issues relevant to their businesses and incorporate a rigorous assessment of these issues into their overall corporate risk management strategies.

The attorneys in Willkie Farr & Gallagher's Data Privacy & Security Practice Group regularly monitor and counsel clients regarding developments across the privacy world – both domestic and international. This publication uses that deep expertise to cover a broad spectrum of what we see as the most significant recent and ongoing data privacy and security developments to help our clients be better positioned to protect their businesses. We hope you find it useful.

Francis M. Buono

Francis M. Buono is the Chair of the Communications, Media & Privacy Department at Willkie Farr & Gallagher LLP. He specializes in data privacy law and FCC regulatory and policy work for a variety of domestic and multinational clients.

Contents

Consumer Privacy

KEY DEVELOPMENTS

The White House has released comprehensive online privacy legislation that could dramatically change the way companies collect and use consumer personal data collected online. The draft legislation marks a significant shift toward "EU-style" privacy regulation, although the bill has been criticized by businesses, consumer advocates, and the Federal Trade Commission, and is viewed as highly unlikely to pass in the current Congress or in the near future.

An FTC staff report on the "Internet of Things" stresses the need for strong consumer privacy protections as more devices automatically connect to the Internet and to each other, but resists calls for additional legislation.

As regulators and advocates continue to press companies to give consumers more choices in how personal data is collected online, AT&T announces plans to offer pay-for-privacy Internet service and Verizon permits subscribers to opt out of its "super cookies," setting up a potential shift away from advertising-based revenue models.

White House Releases Draft Online Privacy Bill

President Obama recently released draft legislation that would impose sweeping rules on how U.S. companies, particularly Internet and technology firms like Facebook and Google, can collect and use consumer personal data, including requiring explicit consent and enhanced consumer notice under many circumstances.[1] The legislation, entitled the "Consumer Privacy Bill of Rights Act," could have a significant impact on the online economy, including advertisers, app developers, cloud providers, and others throughout the Internet ecosystem. It would also give the Federal Trade Commission (FTC) new enforcement powers, further solidifying the agency's position as the de facto U.S. federal privacy regulator. FTC Chairwoman Edith Ramirez and Consumer Protection Bureau chair Jessica Rich sharply criticized the draft, arguing that the proposal fails to offer concrete consumer protections and lacks sufficient enforceability.[2]

Federal Courts Find That Unique Device IDs are Not Personal Information

Continuing a trend, two federal courts recently held that anonymous but unique identifiers associated with a particular device do not qualify as "personally identifiable information" (PII) under the Video Privacy Protection Act (VPPA). Courts in New Jersey and Georgia dismissed claims against Viacom and Dow Jones that the companies shared unique device identifiers and other similar information with third-party analytics and advertising firms to serve tailored advertisements on the device users. Both courts held that information must itself identify an actual person to be considered PII for purposes of VPPA claims. Although the rulings are limited to VPPA claims (and certain other laws specifically identify unique identifiers as PII), they nevertheless lend incremental support to companies' ability to use consumer data that does not specifically identify individuals for advertising and other purposes.[3]

FTC Issues Report on the Internet of Things; Calls for Consumer Privacy Protections in Connected Device World

The FTC recently issued a staff report discussing the privacy implications of the "Internet of Things," the world of increasingly interconnected machines and devices used by consumers that can send and receive data automatically. The report acknowledges that the Internet of Things will continue to offer myriad consumer benefits but calls on companies to implement best practices to ensure that devices offer reasonable privacy protections. Specifically, the report urges companies to adopt reasonable and appropriate security measures, to minimize the amount and nature of data collected and processed by devices, and to ensure that consumers have sufficient notice and choice. Although the report repeats the FTC's previous calls for legislation strengthening the agency's data security regulatory powers and implementing a national data breach notification standard, the report resists calls from some consumer groups for legislation specifically regulating the Internet of Things.[4]

AT&T Offers Pay-for-Privacy Broadband Service

As part of its GigaPower gigabit-speed broadband Internet service, AT&T is offering consumers an option to prevent AT&T from collecting vast amounts of data about its users' browsing habits for advertising and other purposes. The privacy surcharge of $29 per month – nearly $350 per year – is a model that many consumer-facing edge providers like Facebook and Google have thus far resisted, choosing instead to continue offering their services for "free" while relying on their troves of user data to generate advertising revenue. Commentators have suggested that the model could be one way for retailers and Internet companies to address concerns about potential misuse of consumer data without European-style data protection regulation.[5]

FCC Net Neutrality Rules May Let Broadband Providers Avoid FTC Privacy Jurisdiction

The Federal Communications Commission (FCC) recently issued long-awaited rules governing net neutrality that, among other things, reclassify broadband Internet access service providers as "common carriers" subject to utility-like regulation under the Communications Act.[6] Although the FTC has not opposed the rules in general, FTC Bureau of Consumer Protection Director Jessica Rich pointed out that reclassification means that the FTC can no longer enforce its privacy and data security rules against broadband providers, since the FTC's jurisdiction does not extend to common carriers. Rich and other FTC officials have urged Congress to ensure that the FTC retains jurisdiction over broadband companies regardless of what happens to the FCC's net neutrality rules, which are expected to be challenged in court.[7]

Key Senate Democrats Introduce Data Broker Accountability Legislation

Legislation introduced on March 9 by Senators Ed Markey (D-MA), Richard Blumenthal (D-CT), Al Franken (D-MN), and Sheldon Whitehouse (D-RI) would require accountability and transparency from data brokers that sell certain personal data of consumers, potentially giving consumers the right to demand that brokers stop selling their data altogether for marketing purposes. The Data Broker Accountability and Transparency Act would give the FTC enforcement and rulemaking authority, with penalties ranging up to $16,000 per violation.[8]

Microsoft First to Adopt ISO Cloud Computing Privacy Standard

Microsoft has become the first major company to adopt ISO/IEC 27018, a standard developed by the International Organization for Standardization to protect personal data held in public cloud computing environments. The standard ensures that data owners have transparent visibility into and control over how their data is stored, accessed, and protected around the world. Microsoft has achieved the standard with respect to its Azure, Office 365, and Dynamics CRM Online cloud-based software.[9]

Visa to Use Smartphone Geolocation Data to Combat Fraud

Visa has announced plans to allow cardholders to use the geolocation features on smartphones to alert their financial institutions automatically when they travel outside their home area or internationally. Privacy advocates have offered tentative support for the company's plans, saying that the feature could significantly cut down on credit card fraud, but have also warned that consumers must be given adequate notice of how the technology will work and the option to deactivate the feature.[10]

Senator Criticizes Connected Car Privacy Safeguards

After soliciting information from 16 automakers, Senator Ed Markey (D-MA) has released a report alleging that emerging connected car technologies using wireless communications do not adequately protect consumer data from hackers. The report published by Sen. Markey, a senior Democratic member of the Senate Commerce Committee, finds that security measures employed by car companies are "inconsistent and haphazard" and that consumers are often not made aware of the vast amounts of data harvested by the technologies and, in some cases, shared with third parties. Sen. Markey calls on the National Highway Traffic Safety Administration (NHTSA) to work with the FTC to develop and promulgate new regulations restricting the types of data that can be collected and the ways in which such data can be used and shared.[11]

White House Targets Online Retailers' Use of Consumer Data to Price Discriminate

Coming nearly one year after the White House's initial report on big data, President Obama's Council of Economic Advisers (CEA) has released a follow-up report focusing on the use of consumer data collected online to charge different prices to consumers. CEA Chairman Jason Furman said that the report, which does not propose any additional legislation or regulation, does not claim that price differentiation is inherently harmful; the report concludes that the practice "seems most likely to be harmful when implemented through complex or opaque pricing schemes designed to screen out unsophisticated buyers."[12]

Verizon Allows Subscribers to Opt Out of "Super Cookies"

Following months of criticism from consumer and privacy advocates, Verizon recently announced that it would allow subscribers to opt out of its so-called "super cookies," a unique device identifier that the carrier uses to track user behavior and help target advertisements. The move comes after several Democratic senators wrote to Verizon chairman Lowell McAdam to complain about the use of the identifier to track mobile browsing records even after subscribers deleted the records from their devices. AT&T had previously announced in November 2014 that it would stop using a similar identifier as part of its wireless service.[13]

Financial Privacy

KEY DEVELOPMENTS

Version 3.0 of the Payment Card Industry Data Security Standard was released on January 1, 2015. The new standard, which includes more than 100 new controls to bring the total number of controls up to nearly 300, comes as Verizon's annual PCI compliance report indicates that four out of every five organizations are not in full compliance with existing PCI-DSS standards. As pressure mounts on businesses to avoid additional payment card network data breaches, PCI compliance efforts are expected to increase significantly in 2015.

The Federal Financial Institutions Examination Council (FFIEC) plans to update its cybersecurity guidance based on assessments of various institutions during 2014. The FFIEC guidelines are widely relied upon by U.S. financial institutions to protect financial information, including data entrusted to service providers. The FFIEC also encouraged institutions to participate in the Financial Services Information Sharing and Analysis Center to improve industry-wide security.

The New York Department of Financial Services announced a new cybersecurity preparedness assessment process, which will become part of the agency's examination process of regulated financial institutions. The guidance encourages financial institutions to ensure that cybersecurity is included as a core part of their risk management strategy.

PCI DSS Version 3.0 Goes Into Effect

On January 1, 2015, the latest version of the Payment Card Industry Data Security Standard (PCI-DSS), Version 3.0, which was announced in November 2013, replaced Version 2.0. After December 31, 2014, covered entities must use Version 3.0 for their attestation and internal compliance purposes. Version 3.0 clarifies and updates existing requirements and introduces over 100 new requirements, bringing the total number of required controls to 287. Examples of key new requirements include the following:

- Requirement 12.8.5 requires organizations to maintain information about which entity (the organization or one of its service providers) manages each PCI-DSS requirement.
- Requirement 12.9, which becomes effective July 1, 2015, requires service providers to acknowledge in writing to their customers that they are responsible for the security of cardholder data possessed or otherwise stored, processed, or transmitted by the service provider on behalf of the customer, recognizing the extent to which service providers can impact the security of the customer's cardholder data environment.
- Requirement 11.3, which also goes into effect July 1, 2015, imposes a new methodology for penetration testing.
- Several new requirements impose new physical access controls and payment device protection measures.

Verizon's annual PCI-DSS compliance report, issued on March 19, 2015, indicates that although compliance is improving, more than four out of every five organizations are not in full compliance with existing standards, with regular system testing being identified as a particular weak point for many companies.[14]

Consumer Financial Protection Bureau Finalizes Annual Privacy Notice Proposed Rules

In October 2014, the Consumer Financial Protection Bureau (CFPB) finalized a proposed rule that would alleviate reporting burdens under the Gramm-Leach-Bliley Act (GLBA). The rule eliminates the need for certain financial institutions regulated by the CFPB to mail annual privacy notices to their customers, so long as the institutions comply with certain practices. To avoid the notification requirement, a financial institution must (1) use the federal GLBA model privacy form; (2) refrain from engaging in information sharing that triggers customer opt-out rights under GLBA or the Federal Credit Reporting Act (FCRA); and (3) conspicuously publish its privacy notice online and provide customers with an annual disclosure that includes the URL at which the privacy notice can be found, a telephone number for customers to request a mailed notice, and a statement that the privacy policy remains unchanged from the previous notice. However, an institution that has changed its privacy practices must use standard delivery methods for annual notices.

FFIEC to Update Cybersecurity Guidance Based on Recent Cybersecurity Assessments

On November 3, 2014, the Federal Financial Institutions Examination Council (FFIEC) released a report on its observations from cybersecurity assessments it conducted during summer 2014 at 500 community financial institutions. The report summarizes findings from the assessments and provides suggested questions for institutions to ask when assessing cybersecurity preparedness. The FFIEC announced that it will review and update current FFIEC cybersecurity guidance based on these assessments. The FFIEC also recommended that financial institutions of all sizes participate in the Financial Services Information Sharing and Analysis Center as part of their cybersecurity assessment process. The center develops methods for obtaining, monitoring, sharing, and responding to threat and vulnerability information.

New York Department of Financial Services Introduces New Cybersecurity Preparedness Assessment Process for Banks

On December 10, 2014, the New York Department of Financial Services (DFS) issued an industry guidance letter to all of its regulated banking institutions introducing a new cybersecurity preparedness assessment process, which will become a regular part of the Department's IT examination process.[15] The letter encourages institutions to "view cybersecurity as an integral aspect of their overall risk management strategy." It also provides a nonexclusive list of the topics the examination will address, including corporate governance, integrating information security into core business functions, risks posed by sharing infrastructure, information management and security, and incident detection and response. The letter also lists a dozen information requests to which it will seek responses as part of its comprehensive risk assessment of each institution.

New York DFS Announces Cybersecurity Assessments for Insurance Companies

The New York DFS published a report in February 2015 on the state of cybersecurity preparedness in the insurance industry and announced plans for regular, targeted assessments of insurance companies. Among the findings of the 14-page report, DFS found that only 14 percent of insurance company CEOs receive monthly briefings on the state of their companies' cybersecurity, despite multiple recent high-profile data breaches affecting financial institutions.[16]

Eleventh Circuit Reverses District Court's Budget Rent A Car FACTA Decision

On January 12, 2015, the Eleventh Circuit reversed a lower court's holding that two insurance companies, Travelers Property Casualty Company of America and Saint Paul Fire and Marine Insurance Company, have no duty to defend an insured Budget Rent A Car licensee over its alleged violation of the Fair and Accurate Credit Transactions Act (FACTA).[17] The underlying suit against the Budget Rent A Car licensee alleges the licensee failed to redact credit card numbers and expiration dates on receipts. The insurance companies initially won a motion for summary judgment in the district court, which declared that because the underlying complaint alleged only knowing violations of FACTA, which were excluded from coverage, the companies were not required to defend the insured licensee under the terms of the licensee's policy. However, the Eleventh Circuit panel disagreed, holding that the plaintiffs could proceed on the theory that the insured licensee violated FACTA with reckless disregard, a violation which is not excluded from the licensee's coverage.

President Obama Signs Executive Order Enhancing Government-Issued Payment Card Security

As part of a broader industry effort to improve the security of consumer financial transactions, President Obama issued an executive order on October 17, 2014 requiring government-issued payment cards and payment processing terminals to employ "enhanced security features."[18] Starting January 1, 2015, government agencies began issuing new cards and payment terminals with enhanced security features and replacing existing cards. This Order comes in anticipation of a shift in liability for fraudulent transactions from card issuers to retailers who fail to support EMV technology, which will occur in October 2015. The Order also provides measures to reduce identity theft burdens faced by victims and ensure that agencies use appropriate authentication and identity proofing processes for digital applications allowing citizens access to personal information.

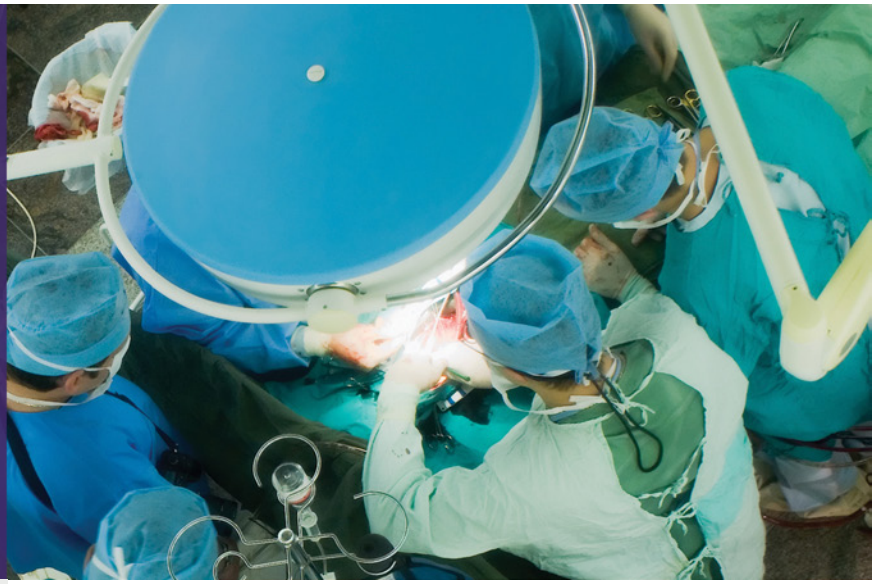
Multiple Employers Sued for Failing to Clearly Disclose Background Check Authorizations in Job Applications

In the last few months, numerous putative class action lawsuits have been filed in federal courts alleging that major U.S. employers have failed to comply with the Federal Credit Reporting Act (FCRA) by conducting background checks on prospective employees without proper disclosure. Suits have been filed against Paramount Pictures Corp.,[19] Whole Foods,[20] and Michaels Stores Inc.,[21] alleging that these entities failed to provide prospective employees with clear and conspicuous disclosures that the prospective employee would be subject to a background check, as required by the FCRA. A similar suit filed against Publix Super Markets Inc. settled in November for approximately $6.8 million.[22]

Supreme Court Deciding Whether to Hear Spokeo's FCRA Challenge

A petition for certiorari pending before the U.S. Supreme Court may have broad implications for establishing the injury-in-fact requirement under Article III of the U.S. Constitution in privacy cases if accepted by the Court. In May 2014, Spokeo filed a petition with the Court seeking review of a Ninth Circuit Court of Appeals decision allowing a class action to proceed and determining that allegations that Spokeo compiled false information into reports sold to its subscribers were sufficient to establish an injury-in-fact under the FCRA.[23] Opponents of this ruling argue that allowing the ruling to stand would make it easier for plaintiffs to file "no-injury" class action suits under a variety of federal privacy statutes.

Health Privacy



KEY DEVELOPMENTS

A recent HIPAA enforcement action by the Department of Health and Human Services resulting in a $150,000 fine has highlighted the need for covered entities and business associates to ensure that all software involved in storing and processing protected health information is up-to-date and fully patched.

HIPAA audits of covered entities and business associates are expected to continue throughout 2015 and 2016 in several phases. The President recently announced that the federal office charged with conducting the audits would receive a budget increase of $4 million, signaling that the audits are a priority for the Administration.

A key Senate committee is considering imposing mandatory encryption of protected health information following the Anthem breach of unencrypted protected health information. HIPAA strongly encourages but does not strictly require the use of encryption and many businesses have resisted incorporating it throughout their systems to avoid losses in efficiency and functionality.

HHS Inspector General Audit Finds Health Insurance Marketplace Security Flaws

The Department of Health and Human Services (HHS) Office of the Inspector General (OIG) has continued to demonstrate its attention to data security matters in the realm of health-related personal information, recently finding multiple flaws in the security controls implemented by the federal Healthcare.gov health insurance marketplace website along with the similar websites operated by state-run exchanges in Kentucky and New Mexico.[24] The OIG's report found that while all three exchanges generally protected consumer personal information in line with federal standards, there was much room for improvement, particularly with respect to implementing robust access controls and developing tools to quickly detect and defend against intrusion attempts and other cyber attacks. The OIG's audit, which it indicates will be one of many, suggests that ensuring the security of health-related personal information will continue to be a priority for the agency.

Healthcare Provider Pays $150,000 for Ignoring Policies and Using Outdated Software

In December 2014, the HHS Office of Civil Rights (OCR) announced a $150,000 settlement with Anchorage Community Mental Health Services (ACMHS), a healthcare provider in Anchorage, Alaska, following a breach of protected health information (PHI) that affected 2,743 individuals.[25] The immediate cause of the breach – malware that allowed hackers to access ACMHS's network – was directly attributed to ACMHS's failure to follow the HIPAA policies it adopted and to update the software used to store PHI with available patches, thereby allowing known vulnerabilities to remain exposed. In addition to the monetary penalty, ACMHS has agreed to implement a corrective action plan and report on its status to OCR for two years.[26]

HIPAA Audits Expected for Covered Entities and Business Associates in 2015

The HHS OCR is expected to begin a second round of intensive HIPAA compliance audits in 2015 that will target approximately 350 covered entities and 50 business associates.[27] The covered entity audits will focus on a range of areas, including security risk analysis and management, breach notification protocols, privacy notices, access to PHI, device and media controls, PHI transmission security, and employee training. Audits of business associates are expected to focus on security risk analysis and management and breach reporting to covered entities. OCR projects additional audits in 2016 focused on encryption and decryption, physical facility access controls, breach reporting, and high-risk areas identified in the current round of audits. Privacy and compliance officers at covered entities and business associates should evaluate their organizations' preparedness for these audits, including by ensuring that they have performed and documented a comprehensive risk assessment. The HHS security risk assessment tool released in early 2014, freely available on the OCR website, provides a good starting point for this process.[28] The President's FY 2016 budget requests an additional $4 million earmarked for OCR's HIPAA audits, indicating that the Administration sees the audits as a priority.[29]

Senate to Consider Mandatory PHI Encryption

The Senate Health, Education, Labor, and Pensions Committee is currently planning a bipartisan review of health information security and has confirmed in the wake of the data breach affecting Anthem that it is considering reforming HIPAA to require that all protected health information (PHI) held by covered entities be encrypted at all times. Although HIPAA does not strictly require encryption, it strongly encourages it and covered entities and business associates that fail to use it should be prepared to defend their security practices. Businesses accessing large amounts of PHI on a regular basis have generally been reluctant to implement encryption across their systems due to the loss of functionality and efficiency that often results.[30]

HIPAA Audit Subjects

2015 | ROUND 1 (BUSINESS ASSOCIATES)

- Risk Analysis and Risk Managementt
- Breach Reporting to Covered Entities

2015 | ROUND 2 (COVERED ENTITIES)

- Device and Media Controls
- Transmission Security
- Privacy Safeguards
- Employee and Vendor Training

2016

- Encryption and Decryption
- Facility Access Control
- Breach Reporting and Complaint Processing
- Other High-Risk Areas

Student and Children's Privacy

KEY DEVELOPMENTS

President Obama has announced a new initiative to protect student privacy. The initiative is expected to include new federal legislation meant to ensure that student data collected in classrooms is used only for educational purposes. The President also endorsed a voluntary student privacy pledge created by the Future of Privacy Forum and Software and Information Industry Association that commits companies to 12 specific privacy practices.

California's new privacy law granting minors additional online protections went into effect January 1, 2015. The law enables minors to request removal of certain content and information from online and mobile platforms.

An FTC staff letter issued to China-based software developer Baby Bus clarifies the extraterritorial applicability of COPPA and highlights the risks for non-U.S. companies offering services targeting children in the United States. The letter also reminds companies subject to COPPA that the FTC considers geolocation data highly sensitive and subject to close scrutiny.

Chinese Company Faces FTC Inquiry for Collecting Geolocation Data from Children's Apps

On December 22, 2014, the Federal Trade Commission (FTC) notified Baby Bus (Fujian) Network Technology Co., Ltd. that it appeared to be in violation of the Children's Online Privacy Protection Act (COPPA) for collecting information through its apps directed at children in the United States.[31] Although the company is based in Fujian, China, it advertises multiple apps on various mobile platforms for purchase in the United States. These apps use cartoon characters to teach young children basic skills and also appear to collect precise geolocation information that is then transmitted to third-party advertisers and analytics companies. In its letter, the FTC informed the company that COPPA applies to foreign-based websites and online services that are involved in commerce in the United States and recommended that the company review all of its apps in light of COPPA's requirement, noting that the FTC would follow up on the violations. The agency also published a blog post reminding all COPPA-covered businesses that geolocation data remains highly sensitive, especially when connected to children.[32]

Yelp and TinyCo Enter Settlements with FTC Over COPPA Violations

The FTC settled two complaints in September 2014 against mobile app providers, Yelp and TinyCo., Inc., for violating COPPA by improperly collecting children's information. Yelp allegedly failed to prevent children under 13 from registering for its service, and TinyCo allegedly collected email addresses from children through its app without following COPPA's procedural collection steps. Under the terms of the settlements, each company agreed to pay a civil penalty – $450,000 for Yelp and $300,000 for TinyCo – and is required to delete the information it collected from users under the age of 13.

President Obama Announces Student Privacy Initiative

On January 12, 2015, President Obama announced a new initiative to protect the privacy of students. As part of this initiative, the President is expected to propose new federal legislation, the Student Digital Privacy Act. The proposed legislation is meant to ensure that data collected in the classroom will be used only for educational purposes. Although the White House has not released details, the legislation will likely be modeled on a California law passed last year, which prevents companies from targeting students with advertising based on data collected at school or selling such data for non-educational purposes. As part of this initiative, President Obama also endorsed the Future of Privacy Forum and The Software & Information Industry Association's voluntary student privacy pledge, encouraging companies to sign on to the joint initiative.[33] Signatories of the privacy pledge commit to 12 practices, including abstaining from selling student information, engaging in targeted behavioral advertising, and changing privacy policies without notice or choice. The pledge has been criticized, however, for failing to ensure adequate security of student information.[34]

Department of Education Issues Student Privacy Compliance Guidance

The Department of Education (DOE) has issued guidance and model terms of service for schools to use in evaluating whether online educational tools and mobile applications comply with student privacy laws. The guidance consists of a publication entitled *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service*,[35] which provides advice on evaluating common privacy provisions found in application terms of service, and also includes a training video about the privacy obligations schools must abide by when using online educational services.[36]

California's Privacy Law for Minors Went into Effect January 1, 2015

The California Rights for Minors in the Digital World Act went into effect on January 1, 2015.[37] The law gives Californians under the age of 18 the right to remove or request removal of content and information from online and mobile app postings on platforms that are either directed to minors or directed to a general audience but for which the company has knowledge that minors use the website or application. Covered companies must also notify minors that the removal service is available and provide instructions on how to use the service. Although the law's protection is limited to California minors, its requirements may extend to companies operating from outside California as well if they handle personal information of California minors.

Children's Web Privacy Suit Dismissed Against Google and Viacom

On January 21, 2015, a federal district court dismissed a nationwide suit against Google and Viacom under the Video Privacy Protection Act and a New Jersey anti-hacking law for allegedly tracking the Internet activity of children visiting Nick.com for advertising purposes.[38] The companies allegedly placed cookies on children's computers to gather information after Viacom secretly tracked children under the age of 13 who used the site and shared the information it collected with Google. The suit was dismissed when the court determined that no evidence had been offered to prove that Google and Viacom could individually identify the particular children using the service.

Data Breach

KEY DEVELOPMENTS

Multiple large-scale data breaches affecting Sony Pictures, Anthem, JPMorgan, Home Depot, the U.S. Postal Service, and others have affected hundreds of millions of Americans in the last few months, exposing millions of records containing sensitive health, financial, and other personal information across multiple industries and sectors.

These large-scale breaches, which can cost companies over $100 million, more than doubled the adoption rate of corporate cyber insurance policies from 10 percent in 2013 to 26 percent in 2014.

President Obama renewed calls for Congress to pass stalled data security and privacy proposals, including a proposed national data breach notification law. The proposal would set a national standard with a 30-day deadline for informing affected individuals in the event of a breach but is seen as potentially preempting stronger state laws.

California and Wyoming passed amendments to their data breach notification statutes. California now requires all offers of identity theft protection services to be for at least 12 months of services, while Wyoming has broadened the scope of notice-triggering personal information and added to the required content of breach notices sent to Wyoming residents.

Obama Calls on Congress to Pass Data Breach Notification Law Proposal

In January 2015, President Obama renewed calls for Congress to pass stalled data security and privacy proposals, including a national data breach notification law proposal. The President's data breach notification proposal would set a national standard with a 30-day deadline for informing affected individuals in the event of a breach. It contains a risk of harm standard that would exempt companies from providing notice to individuals if an assessment concluded that no reasonable risk exists that the breach harmed or will harm the individuals whose information was affected, although companies would have to notify the Federal Trade Commission (FTC) in order to take advantage of the exemption. The FTC and state attorneys general would have enforcement authority over the law. Notably, the proposed standard uses a different and broader definition of personal information than the definition found in many state breach notification statutes, which could significantly increase the number and types of breaches for which companies would be required to notify individuals.[39]

Cyber Insurance Plans See Major Increase in Popularity

A recent report published by the Ponemon Institute on data breach preparedness found that cyber insurance policies have become an increasingly important component of companies' data breach preparedness plans, with the adoption rate more than doubling from 10 percent in 2013 to 26 percent in 2014. In the study, 43 percent of risk management professionals reported that their companies had experienced a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the prior two years. In addition, 67 percent of respondents stated that their organizations do not understand what needs to be done following a material data breach to prevent the loss of customers' and business partners' trust and confidence.[40]

Recent Data Breaches Announced

Anthem, a U.S. health insurer, announced on February 5, 2015 that hackers obtained data on tens of millions of current and former customers, employees, and non-customers who have used Blue Cross or Blue Shield insurance in states where Anthem operates partnerships in a sophisticated attack that has led to an FBI probe. The information compromised includes names, dates of birth, Social Security numbers, street and email addresses and employee data such as income. The company has said that it will notify customers who were affected and provide credit and identity-theft monitoring services free of charge. Seven members of the National Association of Insurance Commissioners will lead the multistate investigation of the breach, which is ultimately expected to cost over $100 million.

Staples announced on December 19, 2014 that the payment cards of approximately 1.2 million customers were compromised by a previously announced breach that affected 115 of the company's retail stores. Staples is offering affected customers free credit monitoring, identity theft insurance, and a free credit report.

On November 25, 2014, **Sony Pictures Entertainment** announced it had discovered a cyber attack that gave perpetrators access to huge troves of confidential employee information, including executive salaries, personal emails, and other highly sensitive data, along with unreleased films set to open in theaters, which the hackers then posted on file-sharing sites. The attack, which has been tied to North Korea, occurred in the month prior to the scheduled release of "The Interview," a comedy about an assassination plot against North Korean leader Kim Jong-un, and resulted in many large theaters' refusal to carry the film.

In an October 2014 Form 8-K SEC filing, **JPMorgan Chase & Co.** reported that contact information (including name, address, phone number, and email address) for about 76 million households and seven million small businesses was compromised in the data breach that began in June 2014. In addition to contact information, hackers tapped into internal data containing information such as whether customers are clients of the bank, or its mortgage, auto, or credit card divisions. The breach is being probed by attorneys general in several states, including Connecticut, Illinois, and Rhode Island.

In November 2014, **Home Depot** announced that 53 million email addresses were taken by hackers during the breach it suffered in 2014, in addition to the previously disclosed 56 million payment cards. Home Depot said that the hackers used a third-party vendor's user name and password to reach the perimeter of its network and subsequently to gain additional rights to navigate the company's systems. Home Depot reported that it spent $33 million responding to the data breach in 2014 in a Form 8-K filing.

The **United States Postal Service** issued a statement in November 2014 indicating that personal information of 800,000 employees, including names, dates of birth, and Social Security numbers, was affected by a hacking incident. Personal information of customers who called or emailed the Postal Service Customer Care Center was also compromised. In the wake of the announcement, the American Postal Workers Union announced that it had filed an unfair labor practice charge with the National Labor Relations Board regarding the Postal Service's failure to bargain over the impact of the breach.

Wyoming Amends Breach Notification Requirements

On March 2, 2015, the governor of Wyoming signed a law that adds elements to the definition of personally identifiable information triggering notification of a data breach. The definition now includes taxpayer identification number, birth or marriage certificates, biometric data, medical history, and health insurance information. A separate law specifies additional information required to be included in breach notices. Both laws go into effect in July 2015.[41]

California Updates Data Breach Notification Law

California Governor Jerry Brown recently signed a bill to update California's data breach notification law. The new law requires notifications sent to individuals affected by a security breach that include an offer to provide identity protection services to offer such services at no cost for at least 12 months (although it does not require the services to be offered in the first place), and expands the requirements for maintaining reasonable security practices and procedures for businesses that maintain personal information of California residents. The law also prohibits the sale, advertisement for sale, or offer to sell an individual's Social Security number.[42]

Parties Reach Settlement in Target Data Breach Litigation

On March 18, 2015, a federal district court in Minnesota approved a settlement in class action litigation related to Target's December 2013 data breach affecting payment card and other personal information of as many as 70 million customers. Target has agreed to pay $10 million plus attorney's fees and costs, and has also agreed to implement various data security measures, including: (1) appointing a high level executive as Chief Information Security Officer; (2) maintaining a written information security program; (3) maintaining a process to monitor information for security events and to respond to any threats; and (4) providing security training to Target employees.[43] The settlement comes after the court held in December 2014 that the plaintiffs had alleged injury sufficient to establish standing, stemming from "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."[44]

Zappos and Attorneys General Sign Compliance Agreement

Zappos and nine states signed a no-fault assurance of voluntary compliance on January 5, 2015 related to a data breach the company suffered in 2011. Under the agreement, Zappos will pay $106,000 to the attorneys general of Arizona, Connecticut, Florida, Kentucky, Maryland, Massachusetts, North Carolina, Ohio and Pennsylvania. The company also agreed to a number of other obligations, including data security improvements, new oversight and reporting requirements, and employee information security training.[45]

Data Security

KEY DEVELOPMENTS

President Obama proposed legislation to encourage sharing cyber threat information between the public and private sectors. Among other things, the legislation would offer targeted liability protection for companies that choose to share information. Similar legislation is already working its way through Congress and was recently passed by the Senate Intelligence Committee.

The Eleventh Circuit affirmed a lower court ruling dismissing LabMD's challenge against the Federal Trade Commission's authority to regulate data security. Meanwhile, the Third Circuit heard oral argument in Wyndham's similar challenge, and a ruling is expected in the coming months.

The Federal Communications Commission imposed a $10 million fine in its first data security enforcement action. The agency claims that two companies placed personal information of up to 305,000 consumers – including Social Security numbers, names, addresses, and driver's license numbers – on unprotected Internet servers that could be accessed by anyone without security credentials in violation of the Communications Act.

White House Announces Cybersecurity Legislative Proposals

On January 13, 2015, President Obama proposed legislation that would encourage the private sector to share cyber threat information with the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC).[46] NCCIC would then disseminate the cyber threat information in near real time to relevant federal agencies and potentially impacted industry stakeholders. The President's proposal provides targeted liability protection for companies that share cyber threat information. As part of the proposal, shared cyber threat information could not be used in an enforcement action and would not be subject to dissemination under the Freedom of Information Act, although law enforcement would have limited access to the information. The proposal also encourages the private sector to form Information Sharing and Analysis Organizations (ISAOs) to assist with sharing cyber threat information. The proposal comes a month after Congress passed, and the President signed into law, a bill that codified NCCIC as an entity charged with facilitating cyber threat information sharing.[47] Congress has also proposed its own cyber threat data sharing legislation; a bill introduced by Senators Richard Burr (R-NC) and Dianne Feinstein (D-CA) was recently approved by the Senate Intelligence Committee on a 14-1 vote, although it has been heavily criticized by privacy advocates.[48]

White House Holds Cybersecurity Summit

The White House hosted the Summit on Cybersecurity and Consumer Protection on February 13, 2015, at Stanford University to foster coordination on public and private sector efforts to protect Americans from cyber attacks. As part of the Summit, President Obama signed an executive order intended to promote cyber threat information sharing between the private sector and the federal government.[49] The executive order builds on the legislative proposal discussed above by asking private sector entities to develop ISAOs to serve as collection points for data exchanges. The executive order also directs DHS to create and fund a non-profit organization tasked with developing voluntary standards for ISAOs.

LabMD's Complaint Dismissal Affirmed by Federal Appeals Courts

On January 20, 2015, the U.S. Court of Appeals for the Eleventh Circuit affirmed a lower court ruling dismissing on procedural grounds LabMD's claim that the FTC lacks authority to charge it with violating the FTC Act for failing to provide adequate data security.[50] The Court held that the FTC's refusal to dismiss the administrative complaint filed with the agency was not a final agency action and, as such, was not ripe for court review. The FTC's authority to regulate data security under the FTC Act is also the subject of a challenge pending before the Third Circuit in *FTC v. Wyndham Worldwide Corp.*, discussed below.

Oral Argument Heard in *Wyndham* Challenge to FTC Data Security Authority

On March 3, 2015, the FTC and Wyndham made their oral arguments before the U.S. Court of Appeals for the Third Circuit in Wyndham's challenge to the FTC's jurisdiction over regulating data security. The case has attracted considerable interest and a number of amicus briefs have been filed on behalf of either side.[51] The FTC argued, in its brief filed in November,[52] for the Third Circuit to affirm a lower court's ruling rejecting Wyndham's motion to dismiss on the grounds that the FTC does not have authority to regulate data security under Section 5 of the FTC Act. Wyndham asked the Third Circuit in its October and December-filed briefs to overturn the lower court's ruling.[53] Specifically, Wyndham argued that its actions in failing to protect consumers' payment information were negligent, and that negligence is neither necessary nor sufficient to establish an unfair business practice under Section 5 of the FTC Act. A decision in the case is expected within the next few months.

FCC Imposes First Data Security Fine

A divided Federal Communications Commission (FCC) made its first foray into data security regulation, issuing a Notice of Apparent Liability on October 24, 2014 against two telecommunications carriers, YourTel America, Inc. and Terracom, Inc., for $10 million for failing to adequately protect consumers' personal information.[54] The FCC alleges that the companies placed up to 305,000 consumers' personal information – including Social Security numbers, names, addresses, driver's license numbers, and other personal information – on unprotected Internet servers that could be accessed by anyone without security credentials. The FCC claims that YourTel and Terracom violated Section 201(b) of the Communications Act, which requires all practices in connection with interstate or foreign communication service to be just and reasonable, by failing to employ basic and readily available data security features, by misrepresenting their security practices to consumers, and by failing to notify all affected consumers. The FCC further claims that the companies violated Section 222(a) of the Communications Act by failing to protect consumers' "proprietary network information," which the FCC interpreted to include personal data that consumers expect carriers to keep private. Two of the five FCC commissioners – Ajit Pai and Michael O'Rielly – dissented, arguing that the FCC had failed to provide fair notice of "novel legal interpretations and never-adopted rules" before imposing a significant financial penalty.

Employee Privacy

KEY DEVELOPMENTS

The NLRB ruled that employees have a right to use company email systems for certain protected activities, including self-organization and other statutorily protected communications. According to the ruling, employers can generally prevent employees from using company email for such purposes by issuing a total ban on non-work use of the system.

NLRB Finds Employee Right to Use Email for Protected Activities

The National Labor Relations Board (NLRB), in a 3-2 ruling on December 11, 2014, found that employees who have been given access to an employer's email system must presumptively be allowed to use the email system for statutorily protected communications, including self-organization and other communications.[55] The NLRB ruling in *Purple Communications* overturned a 2007 decision – in *Register Guard* – which held that employees had no statutory right to use their employer's email systems for statutorily protected communications. The NLRB overturned its prior decision on the grounds that it was too focused on employers' property rights and that it placed too little importance on email as the dominant means of workplace communication. The NLRB's ruling explicitly limits its applicability to employees who have already been granted access to the employer's email system in the course of their work. The ruling also permits employers to justify a total ban on non-work use of email by demonstrating that special circumstances make the ban necessary to maintain production or discipline. Absent a total ban on non-work use of email, employers are allowed to apply uniform and consistently enforced controls over their email systems to the extent that such controls are necessary to maintain production and discipline.

NLRB Ruling in *Purple Communications*

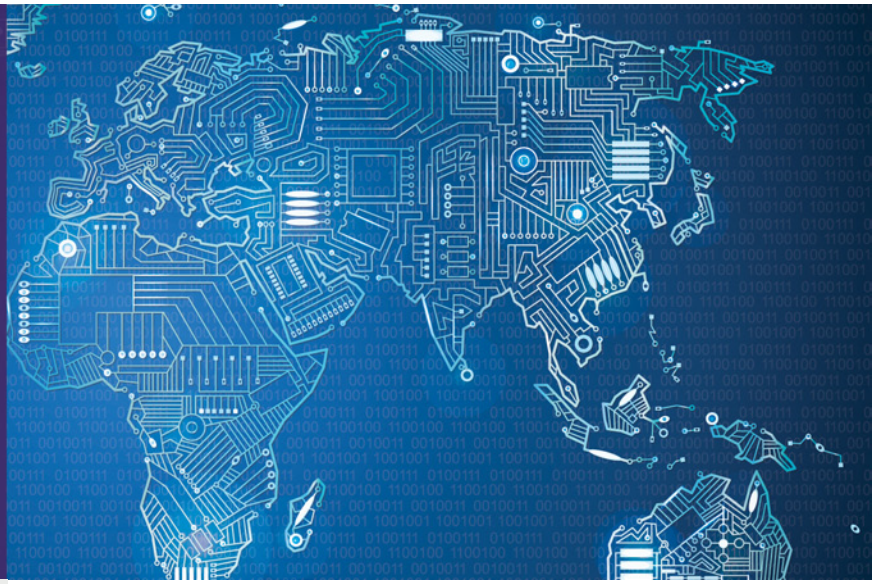
Applies to employees who have been granted access to an employer's email system, but does not require employers to provide email access to employees.

If access is granted, employees must generally be permitted to use the system for protected communications absent special circumstances.

Workplace Medical Records Privacy Ruling Limits Employer Compliance Risk

The Occupational Safety and Health Review Commission (OSHRC) issued a ruling resolving a potential conflict between employers' confidentiality obligations under the Family and Medical Leave Act (FMLA) and reporting obligations under Occupational Safety & Health Administration (OSHA) regulations.[56] OSHRC ruled on September 29, 2014 that FMLA administrators are not required to report certain medical conditions where such reporting would violate FMLA confidentiality requirements. OSHRC reversed a lower decision that would have required logging FMLA injuries and illnesses on OSHA logs despite FMLA confidentiality protections. OSHRC's decision only applies where there is a clear separation between the FMLA administrator and the persons conducting OSHA recordkeeping.

International Privacy



KEY DEVELOPMENTS

The EU's Article 29 Working Party adopted guidelines on the implementation of the "Right to be Forgotten" as it pertains to search engines, providing a glimpse of how regulators may interpret the European Court of Justice's landmark ruling establishing the right. In January 2015, the Working Party indicated that search engines should apply Right to be Forgotten requests globally, including to searches that take place on non-EU domains.

Work on the controversial and long-delayed EU data protection regulation continues, with ratification currently expected by early 2016. EU ministers agreed in October on several key provisions of the draft regulation, including the need to conduct data protection impact assessments, and requiring non-EU data controllers to appoint an EU representative. The Council of the European Union is expected to approve the draft bill text by mid-2015.

Russia's new data localization law, which generally requires database operators to store all personal data of Russian citizens in databases located within Russia, is now scheduled to take effect on September 1, 2015, a year earlier than previously planned.

Canada

Alberta Amends Provincial Privacy Statute After Deadline Extended

After receiving a six-month extension from the Supreme Court of Canada to revise the Personal Information Protection Act (PIPA),[57] the Alberta legislature passed Bill 3, which amends the law to remove the requirement that unions obtain consent to collect or process personal information during labor disputes, which had caused the Supreme Court to invalidate the entire law as unconstitutional in 2013.

First Major Anti-Spam Penalty Issued

The Canadian Radio-television and Telecommunications Commission (CRTC) announced earlier this month that it has issued the first penalty under Canada's robust Anti-Spam Law (CASL), fining Quebec-based Compu-Finder CAD $1.1 million for "flagrant" violations of CASL, including failure to obtain adequate consent and failure to provide functioning opt-out links within commercial electronic messages. With the CRTC indicating that it "take[s] violations to the law very seriously," the Compu-Finder penalty could be a sign of continuing, robust enforcement efforts.[58]

Regulator Publishes Guidance on CASL

The CRTC published guidance in November 2014 on how it will enforce the computer program provisions of CASL, including its consent and disclosure requirements.[59] The guidance clarifies that CASL prohibits the installation of computer programs on another person's computing device during the course of commercial activity without the express consent of the device's owner prior to installation, and applies to programs installed on desktops, laptops, smartphones, gaming consoles, and other connected devices. Separate consent is required for updates or upgrades of installed software. The computer program consent provisions went into effect in January 2015.

OPC Examines Privacy Practices of Microsoft and Google

In two enforcement reports issued in December 2014, the Office of the Privacy Commissioner of Canada (OPC) examined the privacy practices of Microsoft and Google. OPC specifically criticized Microsoft for gaps in its privacy accountability framework in dealing with users' complaints, although it was satisfied by the company's "fulsome response" in resolving the complainant's original issue during the investigation. OPC found in favor of Google on a complaint alleging that Google forced a user to consent to permissions that would lead to the collection of personal information, but encouraged Google to improve the clarity of the permissions process.

European Union

EU Ministers Agree on Data Protection Regulation Provisions Related to Data Processors and Controllers

In October 2014, EU justice ministers agreed on several provisions of the draft EU data protection regulation relating to requirements for data controllers and processors. Ministers agreed that "high risk" processing that could infringe on the rights of data subjects by, for example, exposing them to the risk of identity theft, fraud, or reputational damage, should trigger a data protection impact assessment. Ministers also agreed that controllers should be required to consult with their data protection supervisor on the measures to be taken to mitigate the risk of infringement. They agreed that non-EU data controllers should be required to nominate an EU representative except for data processing that is unlikely to result in a risk for data subjects. Regarding the obligations of data controllers and processors, such as maintaining records of operations and making records available to supervisors, the EU ministers endorsed an exemption for companies with fewer than 250 employees that do not carry out high risk data processing.

Article 29 Working Party Says User Consent Requirements Apply to Device Fingerprints

In November 2014, the Article 29 Working Party released an opinion stating that the user consent requirements of the EU's e-Privacy Directive apply to "device fingerprints," or sets of data that can be used to identify specific Internet-connected devices (such as computers, smart meters, or other objects in the "Internet of Things"). This means that any company or organization that wants to use device fingerprints to identify connected devices in the EU must first obtain the device user's valid consent.[60]

Article 29 Working Party Issues Guidance on Right to be Forgotten

The Article 29 Working Party adopted guidelines in November 2014 on the implementation of the European Court of Justice's May 2014 decision, which ruled that Google was a data controller and as such was obligated to comply with EU data protection laws, including the Right to be Forgotten.[61] The recommendations set out criteria to determine under which circumstances search results should be de-indexed, noting that as a general rule, the rights of individuals to suppress search results prevail over other interests. The privacy regulators also criticized the practice of notifying website operators when search results linking to their sites are delisted. On January 16, 2015, the Article 29 Working Party sent letters to Microsoft, Qwant, and Yahoo! stating that the Internet search engines should apply right to be forgotten requests globally (including to searches that take place on .com domains), and not just to results returned from searches carried out on European Union domains. Google appointed an advisory council, which issued a report on February 6, 2015 concluding that the Right to be Forgotten should apply only to EU domains.[62]

France – DPA Plans to Conduct Audits for Compliance With Cookie Recommendations

France's data protection authority (CNIL) announced in October 2014 that it will use online audits to verify compliance with French laws and recommendations on the use of cookies and other mechanisms that track users' browsing histories. The CNIL plans to audit the number

and types of cookies that sites install on users' machines; information given to site users about cookies used; the quality and relevance of that information; and the process used to obtain users' consent for cookies.

France – CNIL Expands Trust Seal Program

In December 2014, CNIL's governing board decided to expand its voluntary data protection trust seal program to include a data governance seal, which allows companies to certify that their internal data processing complies with French privacy law. In order to obtain the seal, companies and organizations must take a number of steps, including designating a data protection officer that is tasked with overseeing data governance procedures and establishing a regularly updated report of all data processing within the company.

Italy – Google to Submit to Italian DPA Audits on U.S. Soil

The Italian DPA has announced that it will perform monitoring and audits of Google's operations, including spot checks at Google's Mountain View, California headquarters, to ensure Google's compliance with Italian data protection law. Google reportedly agreed to the Italian assessments, which are believed to be the first conducted of a U.S. company.[63]

Italy – DPA Publishes Biometric Rules

In December 2014, the Italian DPA published rules governing the use of biometric data, making it easier for companies and other private entities to use certain data without prior consent from regulators. The new rules also require that data breaches compromising biometric information be reported within 24 hours and establish safeguards that companies must implement in order to use biometric data. The safeguards require companies to take steps such as deleting biometric data when no longer needed, restricting copying of data, and submitting oversight reports to the DPA.

Netherlands – DPA Issues Cease and Desist Order to Google

The Dutch Data Protection Authority (CBP) issued a cease and desist order to Google, threatening a fine of €60,000 per day, up to €15 million total, for breaching the Dutch Data Protection Act. The CBP said that Google breaches Dutch law by collecting the personal data of Internet users without sufficient consent and by combining personal data across its services. The order required Google to amend its privacy practices to make clear to users that Google is the owner of YouTube, seek the unambiguous consent of users for combining their data across services, and to revise its privacy policy to clarify what data Google collects and how such data is used.

Russia – Regulator Clarifies New Law Will Not Block Cross-Border Online Services

The Russian federal data protection regulator has stated that the new Russian data localization law, which requires data operators to store all personal data of citizens of the Russian Federation in databases located inside Russia by September 1, 2015, a year earlier than previously announced, will not block cross-border online services. The new law will, however, prohibit Russian data transfers without consent to jurisdictions where there is no adequate protection of personal data.

Spain – DPA Issues Privacy Guidance

In October 2014, the Spanish Data Protection Agency issued guidance to companies on how to identify and avoid privacy risks. The guidance aims to introduce new approaches to data protection, such as privacy by design, and recommends a privacy impact assessment where a company uses certain technologies such as geolocation, data mining, and biometric analysis.[64]

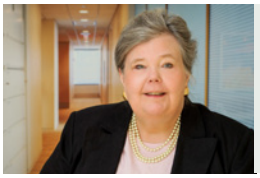
Turkey – President Signs New E-Commerce Privacy Law

In November 2014, Turkey's president signed an e-commerce law requiring transparency for e-commerce transactions. The law bans sending email spam and making unsolicited telemarketing calls, texts, and faxes. The law also requires all service operators to protect personal data collected and stored as part of online transactions and prohibits them from transmitting data to third parties or using the information without consent for purposes other than that for which it was collected.

Contributors

Francis M. Buono

Partner, Chair, Communications, Media & Privacy Department
Washington
202 303 1104 | fbuono@willkie.com

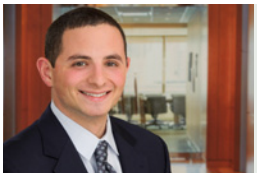


Barbara Block

Senior Associate
Washington
202 303 1178 | bblock@willkie.com

Melanie A. Medina

Associate
Washington
202 303 1191 | mamedina@willkie.com



Joshua S. Parker, CIPP/US, CIPP/E

Associate
Washington
202 303 1234 | jparker@willkie.com.

Daniel R. Bumpus

Associate
Washington
202 303 1226 | dbumpus@willkie.com

Brenna A. Sparks

Associate
Washington
202 303 1145 | bsparks@willkie.com

Stephanie B. Power

Associate
Washington
202 303 1249 | spower@willkie.com

If you need assistance with particular data privacy or data security matters, please contact Frank Buono at fbuono@willkie.com or the attorney with whom you regularly work.

End Notes

[1] Consumer Privacy Bill of Rights Act, Administration Discussion Draft (Feb. 27, 2015), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[2] Elizabeth Dwoskin, Digits Blog, *Consumer Protection Official Blasts White House Privacy Proposal*, Wall St. J. (Mar. 9, 2015), http://blogs.wsj.com/digits/2015/03/09/federal-consumer-protection-official-blasts-white-house-privacy-proposal/.

[3] *See Locklear v. Dow Jones & Co.*, No. 14-cv-744 (N.D. Ga. Jan. 23, 2015) (order granting motion to dismiss), *available at* http://www.privsecblog.com/files/2015/01/Locklear-v.-Dow-Jones.pdf; *In re Nickelodeon Consumer Privacy Litig.*, No. 13-cv-3729 (D.N.J. Jan. 20, 2015) (same), *available at* http://www.bloomberglaw.com/public/document/IN_RE_NICKELODEON_CONSUMER_PRIVACY_LITIGATION_No_2443_SRC_2015_BL.

[4] *See* Federal Trade Commission, Staff Report, Internet of Things: Privacy and Security in a Connected World (Jan. 2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[5] Jeff John Roberts, *AT&T charges $29 for privacy. Time for others to do the same*, Gigaom (Feb. 17, 2015, 7:41 AM), https://gigaom.com/2015/02/17/att-charges-29-for-privacy-time-for-others-to-do-the-same/.

[6] *In re Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24, GN Docket No. 14-28 (rel. Mar. 12, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.

[7] Brendan Sasso, *Net Neutrality Has Sparked an Interagency Squabble Over Internet Privacy*, National Journal (Mar. 9, 2015), http://www.nationaljournal.com/tech/the-future-of-broadband/net-neutrality-has-sparked-an-interagency-squabble-over-internet-privacy-20150309.

[8] Emily Field, *Senate Dems Look To Make Data Brokers More Accountable*, Law360 (Mar. 9, 2016), http://www.law360.com/privacy/articles/629200?nl_pk=1da41084-ebb2-476f-b68f-b8c2fdb79647&utm_source=newsletter&utm_medium=email&utm_campaign=privacy.

[9] Adrienne Hall, *Microsoft achieves globally recognized ISO/IEC 27018 privacy standard*, Microsoft Cyber Trust Blog (Feb. 16, 2015), http://blogs.microsoft.com/cybertrust/2015/02/16/microsoft-achieves-globally-recognized-isoiec-27018-privacy-standard/.

[10] Ken Sweet, *To fight fraud, Visa wants to track your smartphone*, Denver Post (Feb. 14, 2015), http://www.denverpost.com/business/ci_27525296/fight-fraud-visa-wants-track-your-smartphone.

[11] *See* Sen. Ed Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (Feb. 2015), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[12] Executive Office of the President, Big Data and Differential Pricing (Feb. 2015), http://www.whitehouse.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf.

[13] Brian X. Chen and Natasha Singer, *Verizon Wireless to Allow Complete Opt Out of Mobile 'Supercookies'*, N.Y. Times (Jan. 30, 2015 11:31 AM), http://bits.blogs.nytimes.com/2015/01/30/verizon-wireless-to-allow-complete-opt-out-of-mobile-supercookies/?_r=0.

[14] Eric Parizo, *Verizon 2015 PCI report: More achieve PCI compliance, but fail to keep it*, TechTarget (Mar. 11, 2015), http://searchsecurity.techtarget.com/news/2240242119/Verizon-2015-PCI-report-More-achieving-PCI-compliance-but-failing-to-keep-it.

[15] Press Release, New York Department of Financial Services, NYDFS Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments (Dec. 10, 2014), *available at* http://www.dfs.ny.gov/about/press2014/pr1412101.htm.

[16] New York State Department of Financial Services, Report on Cyber Security in the Insurance Sector (Feb. 2015), http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf; *see also* Press Release, New York State Department of Financial Services, NYDFS Announces New, Targeted Cyber Security Assessments for Insurance Companies (Feb. 8, 2015), http://www.dfs.ny.gov/about/press2015/pr1502081.htm.

[17] *Travelers Property Casualty Co., et al. v. The Kansas City Landsmen, L.L.C., et al.*, No. 14-11006 (11th Cir. Jan. 12, 2015).

[18] Exec. Order No. 13,681, 79 Fed. Reg. 63,489 (Oct. 17, 2014).

[19] *Peikoff v. Paramount Pictures Corp.*, No. 3:15-cv-00068 (N.D. Cal. Jan. 7, 2015).

[20] *Speer v. Whole Foods Market Group., Inc.*, No. 8:14-cv-03035 (M.D. Fla. Dec. 4, 2014).

[21] *Burnside v. Michaels Stores Inc.*, No. 6:15-cv-0310 (W.D. Mo. Jan. 9, 2015).

[22] *Knights v. Publix Super Markets, Inc.*, No. 3:14-cv-0020 (M.D. Tenn, Oct. 28, 2014).

[23] *Spokeo, Inc. v. Robins*, No. 13-1339 (Oct. 6, 2014).

[24] *See* Daniel R. Levinson, Inspector General, Office of Inspector General, Dep't of Health & Human Servs., Health Insurance Marketplaces Generally Protected Personally Identifiable Information but Could Improve Certain Information Security Controls, Report No. A-18-14-30011 (Sept. 2014), https://oig.hhs.gov/oas/reports/region1/181430011.pdf.

[25] Office of Civil Rights, Dep't of Health & Human Servs., Bulletin: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software (Dec. 2014), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf.

[26] Resolution Agreement between Anchorage Community Mental Health Services and Office of Civil Rights (Dec. 2, 2014), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf.

[27] Presentation at HCCA Compliance Institute, Office for Civil Rights, Dep't of Health & Human Servs., OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2 (Mar. 31, 2014), http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2.pdf; *see also* Daniel Solove, The Most Alarming Fact About HIPAA Audits (Part 5), SafeGov.org (Oct. 23, 2014), http://safegov.org/2014/10/23/the-most-alarming-fact-about-hipaa-audits-(part-5).

[28] *See* http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.

[29] *See* Elizabeth Snell, *OCR HIPAA Audit Program Part of 2016 Budget Plan*, HealthIT Security (Feb. 6, 2015), http://healthitsecurity.com/2015/02/06/ocr-hipaa-audit-program-part-of-2016-budget-plan/.

[30] *See* Susan D. Hall, *Lawmakers to rethink requiring encryption in HIPAA*, FeirceHealthIT (Feb. 9, 2015), http://www.fiercehealthit.com/story/lawmakers-rethink-requiring-encryption-hipaa/2015-02-09.

[31] Letter from Maneesha Mithal, Associate Director, Federal Trade Commission, To BabyBus(Fujian) Network Technology Co., Ltd. (Dec. 22, 2014) *available at* http://www.ftc.gov/public-statements/2014/12/letter-maneesha-mithal-associate-director-babybus-fujian-network.

[32] Lesley Fair, FTC Business Blog, *Who's covered by COPPA? FTC staff letter outlines the ABCs* (Dec. 22, 2014), https://www.ftc.gov/news-events/blogs/business-blog/2014/12/whos-covered-coppa-ftc-staff-letter-outlines-abcs.

[33] Press Release, Future of Privacy Forum & Software & Information Industry Association, President Obama Endorses the Student Privacy Pledge (Jan. 12, 2015), *available at* http://studentprivacypledge.org/?page_id=662.

[34] *See* Natasha Singer, Bits Blog, *Data Security Gaps in an Industry Student Privacy Pledge*, N.Y. Times (Feb. 11, 2015), http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge.

End Notes

[35] Department of Education, Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service* (January 2015), *available at* http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf.

[36] YouTube Video: Protecting Student Privacy While Using Online Educational Services, U.S. Department of Education (Feb. 26, 2015), https://www.youtube.com/watch?v=deo2F19DK_o.

[37] Calif. Bus. & Prof. Code §§ 22580-22582.

[38] *In re Nickelodeon Consumer Privacy Litig.*, MDL 2443 (D.N.J. Jan. 21, 2015).

[39] The White House, Personal Data Notification and Protection Act, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (last visited Mar. 16, 2015).

[40] Ponemon Institute, Is Your Company Ready for a Big Data Breach? (2012), *available at* http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

[41] Tripp Baltz, *Wyoming Governor Mead Signs Breach Notice Amendment Bills*, BNA (Mar. 6, 2015), http://www.bna.com/wyoming-governor-mead-n17179923753/.

[42] A.B. 1710 (Ca. 2014), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710.

[43] Consumer Plaintiffs' Memorandum in Support of Motion for Certification of a Settlement Class and Preliminary Approval of Class Action Settlement, *In re Target Corp. Customer Data Security Breach Litig.*, No. 14-md-2522 (D. Minn. Mar. 18, 2015).

[44] Megan Guess, Judge Rules That Banks Can Sue Target for 2013 Credit Card Hack, Arstechnica (Dec. 4, 2014), *available at* http://arstechnica.com/tech-policy/2014/12/judge-rules-that-banks-can-sue-target-for-2013-credit-card-hack/.

[45] Zappos, Assurance of Voluntary Compliance (Jan. 5, 2015), *available at* http://www.ncdoj.gov/getattachment/41014ef1-2b17-411d-a821-78454e04beb7/Zappo-Assurance-of-Voluntary-Compliance-(2).aspx.

[46] *Updated Cybersecurity Information Sharing Proposal*, WhiteHouse.gov (Jan. 13, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.

[47] *See* National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282 (2014).

[48] *See* Alexei Alexis, *Senate Panel Advances Bill to Provide Immunity for Cyberthreat Data Sharing*, BNA (Mar. 12, 2015).

[49] Executive Order – Promoting Private Sector Cybersecurity Information Sharing, http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[50] *LabMD, Inc. v. FTC*, No. 14-12144 (11th Cir. Jan. 20, 2015), *available at* http://www.ftc.gov/system/files/documents/cases/d09351labmdappealorder_0.pdf.

[51] *See, e.g.*, Brief of Amici Curiae Center for Democracy & Tech. and Elec. Frontier Found. Supporting Plaintiff-Appellee, *FTC v. Wyndham Hotels & Resorts, LLC*, No. 14-3514 (3d Cir. filed Nov. 12, 2014), *available at* http://epic.org/amicus/ftc/wyndham/Amicus-EFF-Berkeley-CDT.pdf; Brief of Amicus Curiae Elec. Privacy Info. Ctr. (EPIC) and Thirty-Three Technical Experts and Legal Scholars in Support of Plaintiff-Appellee, *FTC v. Wyndham Hotels & Resorts, LLC*, No. 14-3514 (3d Cir. filed Nov. 12, 2014), *available at* http://epic.org/amicus/ftc/wyndham/Wyndham-Amicus-EPIC.pdf; Brief of Amici Curiae Chamber of Commerce of the U.S., Am. Hotel & Lodging Ass'n, and Nat'l Fed'n of Indep. Bus. in Support of Appellant, *FTC v. Wyndham Hotels & Resorts, LLC*, No. 14-3514 (3d Cir. filed Oct. 14, 2014), *available at* http://epic.org/amicus/ftc/wyndham/Amicus-Chamber-Commerce.pdf.

[52] Brief for Plaintiff-Appellee, *FTC v. Wyndham Hotels & Resorts, LLC*, No. 14-3514 (3d Cir. filed Nov. 5, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141105wyndham_3cir_ftcbrief.pdf.

[53] Brief for Defendant-Appellant, *FTC v. Wyndham Hotels & Resorts, LLC*, no. 14-3514 (3d Cir. filed Oct. 6, 2014), *available at* https://epic.org/amicus/ftc/wyndham/Wyndham-Opening-Appellate-Brief.pdf; Reply Brief for Defendant-Appellant, *FTC v. Wyndham Hotels & Resorts, LLC*, no. 14-3514 (3d Cir. filed Dec. 8, 2014), *available at* https://epic.org/amicus/ftc/wyndham/Wyndham-Reply.pdf.

[54] TerraCom, Inc. and YourTel American, Inc. Apparent Liability for Forfeiture, *Notice of Apparent Liability for Forfeiture*, 29 FCC Rcd. 13325 (Oct. 24, 2014).

[55] Purple Communications, Inc. and Communications Workers of America, AFL-CIO, Decision and Order Remanding, 361 N.L.R.B. No. 126 (Dec. 11, 2014), *available at* http://apps.nlrb.gov/link/document.aspx/09031d45819e22c9.

[56] U.S. Postal Service, Decision, OSHRC Docket No. 08-1547 (Sept. 29, 2014), *available at* http://www.oshrc.gov/decisions/pdf_2014/08-1547.pdf.

[57] Decision on Miscellaneous Motion, *Information and Privacy Commissioner v. United Food and Commercial Workers, Local 401*, No. 34890 (Can. Oct. 30, 2014), *available at* http://www.scc-csc.gc.ca/case-dossier/info/dock-regi-eng.aspx?cas=34890.

[58] Press Release, Canadian Radio-television and Telecommunications Commission, CRTC Chief Compliance and Enforcement Officer issues $1.1 million penalty to Compu-Finder for spamming Canadians (Mar. 5, 2015), *available at* http://news.gc.ca/web/article-en.do?nid=944159.

[59] Canadian Radio-television and Telecommunications Commission, Canada's Anti-Spam Legislation Requirements for Installing Computer Programs, http://www.crtc.gc.ca/eng/info_sht/i2.htm last updated Jan. 1, 2015).

[60] Article 29 Data Protection Working Party, Opinion 9/2014 on the application of Directive 2002/58/EC to Device Fingerprinting (Nov. 25, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf.

[61] Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on the "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez" C-131/12 (Nov. 26, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

[62] The Advisory Council to Google on the Right to be Forgotten (Feb. 6, 2015), https://drive.google.com/a/google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1.

[63] Alistair Barr and Sam Schechner, Digits Blog, *Google Agress to Spot Checks by Italian Privacy Regulators*, Wall St. J. (Feb. 20, 2015), http://blogs.wsj.com/digits/2015/02/20/google-agrees-to-spot-checks-by-italian-privacy-regulators/.

[64] Agencia Española de Protección de Datos, Guía para una Evaluacion de Impacto en la Protección de Datos Personales, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf (Oct. 2014) (in Spanish).