Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

INTERNATIONAL EDITION

MAY 2015

IN THIS ISSUE

Locke Lord LLP

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of data security. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:

Natasha Ahmed
Associate
London
+44 (0) 20 7861 9048
nahmed@lockelord.com

David L. Anderson
Counsel
Los Angeles
310-860-8710
david.anderson@lockelord.com

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

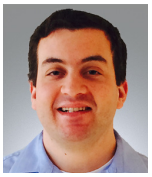
Michael Bennett
Partner
Chicago
312-201-2679
michael.bennett@lockelord.com

Karen L. Booth
Associate
Hartford
860-541-7714
karen.booth@lockelord.com

Wing Cheung
Partner
Hong Kong
+852 3465 0688
wcheung@lockelord.com

Laura Ferguson
Associate
Houston
713-226-1590
lferguson@lockelord.com

Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com



Aaron Igdalsky
Associate
Hartford
860-541-7766
aaron.igdalsky@lockelord.com

Sean Kilian
Associate
Dallas
214-740-8560
skilian@lockelord.com

John Kloecker
Of Counsel
Chicago
312-443-0235
jkloecker@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Alan Meneghetti
Partner
London
+44 (0) 20 7861 9024
ameneghetti@lockelord.com

Charles E. Phipps
Partner
Dallas
214-740-8441
cphipps@lockelord.com

Charles M. Salmon
Associate
Austin
512-305-4722
csalmon@lockelord.com

Stephen R. Ucci
Counsel
Providence
401-276-6426
stephen.ucci@lockelord.com

Tammy Ward Woffenden
Partner
Austin
512-305-4776
twoffenden@lockelord.com

Vita Zeltser
Senior Counsel
Atlanta
404-870-4666
vzeltser@lockelord.com

Privacy and Other Issues Presented by Body Cameras

Body cameras are becoming part of the uniform for certain professionals including police officers and service personnel. These cameras are more than an extension of dashboard cameras for law enforcement; they are more versatile and more likely to present privacy and intellectual property issues. Thus, any organization using or considering the use of such cameras should consider these issues, establish appropriate contractual covenants, establish internal policies governing the use of the cameras and the handling of the recordings, and train employees appropriately.

For law enforcement applications, in addition to important privacy concerns, there are concerns over public access rights to the recordings. Body cameras come in various forms, and may be worn or attached at various places on the body. In the extreme, they represent the surveillance state – the government can watch public and private spaces through the eyes of the police. With the assistance of facial recognition technology, police could even scan the public for those who have warrants outstanding or who are suspected of crimes. The concept may not sit well with those who are leery of government use of technology for widespread surveillance of the public.

On the other side of the coin, the cameras can certainly offer valuable evidence in connection with the crimes to which law enforcement responds. In addition, police officers are less likely to be falsely accused of excessive or improper force and are more likely to be reprimanded when excessive or improper force is used. Even better, police and those with whom they interact are more likely to behave better when they know they are being recorded. Still, the presence of a recording device would almost certainly undermine trust and the willingness of witnesses, victims, suspects, and informants to share information with the police. Police officers themselves may resent being monitored while they work. And the police often venture into private homes and must sometimes deal with violent situations and unclothed individuals, the video from which may be inappropriate for public review but attractive to the press.

Thus, the debate. At a minimum, police forces must evaluate risks and concerns and implement appropriate guidance and policies. Laws governing access to public information may need to be amended. In one survey, nearly a third of the law enforcement respondents indicated that they do not have a written policy in place for appropriate usage of body cameras. The International Association of Chiefs of Police has published sample policies for its membership. The U.S. Department of Justice's "Implementing a Body-Worn Camera Program—Recommendations and Lessons Learned" provides guidance on topics such as: when to record, whether recording should be discretionary or mandatory, consent issues (including as pertinent to state laws requiring two-party consent for audio recording), sensitive environments or situations, public access to recordings, and retention considerations.

Body cameras, like dashboard and highway cameras, location tracking technologies, and even Internet tracking capabilities, raise privacy issues in a manner not contemplated by traditional privacy law. As stated by Justice Sotomayor in her concurrence in U.S. v. Jones (a case about GPS tracking): "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."

Outside of the law enforcement realm, in commercial applications of body cameras, there are concerns over the protections of confidential documents or meetings being recorded by these cameras. For example, body cameras may be worn by delivery personnel or service personnel, and a company may want to consider prohibiting or restricting the use of such cameras in the workplace by non-employees. And body cameras worn by employees could bring their own issues – in addition to privacy and data security concerns, issues like rights of publicity and copyright ownership could be blurred if the employee captures images outside the scope of employment (such as a celebrity sighting). And use of body cameras by employees of state or federal employees could implicate open-records laws.

From a personal perspective, would an employee have a right to wear a body camera to work for his or her own sense of protection? Would employees be entitled to overtime pay and benefits if they use company-issued body cameras after normal working hours?

Body cameras offer the potential to collect an unprecedented volume of detailed data and that data can itself create needle-in-the-haystack problems. What if a body camera collects information which shows that a dangerous condition exists at a manufacturing facility? Would the wearer recognize that condition? If there is a subsequent accident, would the company even be aware it has that information when served with a subpoena? If the body camera is worn by a third-party service provider, when do they have a duty to disclose the recorded dangerous situation?

These any many other issues will unfold as a result of the increase use of body cameras. A proactive approach to addressing these significant legal issues is advisable.

There is plenty of room for careful thought and analysis in this area. In a world where we have the technology to record everything, and to store all those recordings, should everything be recorded? The analysis will undoubtedly lead to a balancing of interests, but the balancers should keep in mind that compelling interests arise all over the place, beyond the area of law enforcement and commercial applications. Presumably, some parents (and claim-wary teachers) wouldn't mind cameras in the classroom, and some patients (and claim-wary surgeons) wouldn't mind cameras in the operating room. Is there a line, and where should it be drawn? Companies will need to formulate pro-active policies to address these issues against a backdrop of rapidly changing public opinion and policy.

Rapid Developments in State Student Privacy Laws

In 2014, at least 16 states enacted laws regulating the privacy of student information. The trend is continuing in 2015, as at least 165 state student privacy bills have been introduced thus far, six of which have already been enacted in Virginia and Utah. As new state laws continue to be layered upon existing federal obligations such as the Family Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA"), schools, districts, ed tech companies, and other service providers face an increasingly complex regulatory regime.

The new state requirements vary, in some cases restricting the type of information that may be collected from students, while in other cases strictly limiting the ways in which student data may be used or disclosed, or requiring transparency regarding data collection, use, and disclosure practices, notification to parents in the event of a data breach, certain levels of security for student information, vendor contract terms imposing such requirements, or some combination of these and other requirements. Many but

not all of the new laws apply only to data stored in the statewide longitudinal data system ("SLDS").

In most cases, the new requirements apply to schools and school districts. However, many laws also require that schools and school districts include specific privacy and data protection terms in their contracts with ed tech companies and other service providers that may have access to student data. In addition, California's Student Online Personal Information Protection Act, which was enacted in 2014 and becomes effective January 1, 2016, extends directly to operators of websites, online services, or online or mobile applications with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. The California Act restricts such operators from knowingly engaging in targeted advertising, amassing a profile about a K-12 student except in furtherance of K-12 school purposes, selling a student's information, or disclosing student information other than for certain specified purposes.

Schools, districts, ed tech companies, and other service providers should monitor the new requirements, as well as relevant contractual obligations, to ensure that their privacy and data protection policies, procedures, and practices comply with the increasingly complex statutory and regulatory requirements applicable to student data.

Facebook Class Action Lawsuit in Austria

A class action against Facebook has been filed in Vienna by privacy campaigner and Austrian law graduate Max Schrems, along with 25,000 other users of the social network site. The lawsuit alleges breaches of EU privacy law and mass surveillance.

The case was filed on 9 April this year against Facebook's European HQ in Dublin, which handles accounts outside the U.S. and Canada, accounting for approximately 80% of Facebook's 1.35 billion users. The alleged breach of European privacy laws relates to the way that Facebook monitors its users' activation of its "Like" buttons.

Currently, the 25,000 users are claiming €500 (£392) each in damages for the "illegal" tracking of their data under EU law, amounting to over €10 million if the charges against Facebook are proved in this case. A further 55,000 users have registered to join the procedures at a later stage.

Schrems is reported in the Guardian as commenting: "Basically we are asking Facebook to stop mass surveillance, to (have) a proper privacy policy that people can understand, but also to stop collecting data of people that are not even Facebook users."

Facebook has raised procedural objections, asking for the case to be dismissed. The Vienna court will rule in several weeks or so whether it has jurisdiction to hear the class action in Austria.

Economic Impact from a Company's Data Breach – No Big Deal? Not So Fast!

Recent data breaches have prompted worries about economic damage to the infiltrated companies. Analyses in fact show minimal effects on stock prices or revenues of the hacked companies. But that may be only temporary comfort as commentators urge a longer-term view.

A recent article in the *Harvard Business Review* found that "even the most significant recent breaches had very little impact on the company's stock price." Similarly, "actual expenses … amount to less than 1% of each company's annual revenues. After reimbursement from insurance and minus tax deductions, the losses are even less," according to a new analysis from a fellow at the Columbia School of International and Public Affairs.

Good news? To an investor looking solely at publicly disclosed costs of data breaches by large retailers, one takeaway may be that sophisticated companies have done a decent job of preparing for, responding to, and insuring against large data breaches. Another question, however, is whether the costs are merely shifted to consumers, who as a group bear the brunt of the inconvenience and anxiety associated with a data breach, even where monetary loss is minimal. And if a large company does not feel the pain in its bottom line, does it have adequate incentive to invest in cybersecurity measures to protect consumers? And without market incentives, will that prompt more government intervention and regulatory fines?

What about the longer term? It is not clear to what extent corporate data breach victims incur damages that are not subject to data breach notification laws – *e.g.*, losses from competitor or state-sponsored theft of intellectual property, customer lists, business plans, and other proprietary data that, while sensitive and valuable to the owner, may not contain personal identifying information. The incentives to protect access to this data may outweigh any notion that the costs of consumer data breaches are too low to justify additional investment in cybersecurity.

The publicly disclosed costs also do not factor in reputational interests, customer loyalty, distraction to senior management, and other less easily quantified costs. All stakeholders will continue to wrestle with efforts to quantify all of the hard and soft costs of data breaches of all kinds, short and long-term, so that risks can be better assessed and managed through the private and public sectors.

Delays Continue for OCR's 2015 HIPAA Audits

The Department of Health and Human Services Office for Civil Rights ("OCR") continues to delay implementation of Phase 2 of its HIPAA Audit Program ("Phase 2"), which will build on OCR's pilot audit program that concluded in 2012. In January, OCR Director Jocelyn Samuels reportedly stated that Phase 2 would be "implemented expeditiously." However, during an April 15 session at the HIMSS 2015 Conference in Chicago, a regional official from OCR reportedly communicated that the audit program is still "under development."

The 2015 audits will target both HIPAA-covered entities and their business associates. When originally announced, the Phase 2 audits were expected to be desk audits, though now it appears that OCR may also perform some audits onsite. The audits will

focus on areas of heightened risk identified by OCR during its pilot program, which include compliance with the HIPAA Security Rule's requirement to conduct security risk assessments.

OCR is also expected to issue new guidance for the Phase 2 audits, which may include updating its audit program protocol currently on the OCR's website for covered entities and issuing new business associate protocols. Until additional guidance is issued, to prepare for a potential audit, covered entities and business associates should continue to monitor their HIPAA compliance and implementation efforts and consider the current OCR audit program protocol, which addresses elements of privacy, security, and breach notification. Topics of review are: (1) notice of privacy practices for HIPAA Protected Health Information ("PHI"), (2) individuals' rights to request privacy protection for PHI, (3) individuals' access to their own PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.

The current protocol also covers Security Rule requirements for administrative, physical, and technical safeguards and requirements for the Breach Notification Rule. Thus, in addition to monitoring general HIPAA compliance, both covered entities and business associates should conduct regular security risk assessments and address potential HIPAA risks identified in such assessments.

In addition to its Phase 2 HIPAA audits, OCR will continue investigating complaints alleging violations of the HIPAA Privacy and Security Rules and may also investigate reports of high profile breaches. So far in 2015, OCR has not announced any settlements with covered entities or business associates.

Entertainment Industry Agent Rightscorp Seeks Personally Identifiable Information of Thousands of Internet Users

In the past two years, Rightscorp, Inc. has sought the identity of thousands of Internet subscribers across the country, in order to obtain settlements for alleged violations of its clients' copyrights. In its campaign, Rightscorp primarily relies upon subpoenas issued pursuant to 17 U.S.C. § 512(h) of the Digital Millennium Copyright Act ("DMCA"). Section 512(h) allows a copyright holder, or a person authorized to act on its behalf, to request that a subpoena be issued to a "service provider" to identify an "alleged infringer." The request is made in a "miscellaneous case" in federal district court, and the subpoenas are issued by the Clerk of the Court, not a District Judge. Rightscorp has filed approximately 150 Section 512(h) actions in 2014 and 2015.

Rightscorp's approach is inconsistent with decisions of the U.S. Courts of Appeal from the Eighth and District of Columbia Circuits, which state that an Internet service provider ("ISP") acting as a conduit (i.e., simply providing Internet service) is not subject to the provisions of Section 512(h). When challenged based on these authorities, Rightscorp has either withdrawn or lost.

By virtue of the large scale, Rightscorp has had some success in obtaining names and sending out demands. But other problems have surfaced, including two now-pending federal class action lawsuits in California and Georgia alleging violations of federal debt collection and communications laws by Rightscorp in connection with its pursuit of settlements from individuals.

Despite judicial disapproval of a key element of Rightscorp's business model (i.e., the use of Section 512(h)) and class action lawsuits, two of the copyright holders that rely on Rightscorp's services are suing an ISP. The suit alleges that the ISP (which refused to provide Rightscorp with personally identifiable information about subscribers) cannot rely on DMCA immunity and should be liable for contributory and vicarious copyright infringement.

Although no one would seriously disagree that something should be done about online copyright piracy, the existence of a problem is not an excuse to circumvent the law or to disregard appropriate procedures for obtaining personal information of Internet subscribers. Accusations by a private entity of copyright infringement are just that. Adjudications are still appropriately left to the courts.

NAIC Planning to Require Cybersecurity Insurance Data Submission

The National Association of Insurance Commissioners' ("NAIC's") Cybersecurity Task Force and Property and Casualty Insurance Committee are jointly considering whether to require a cybersecurity insurance coverage supplement in addition to the already-required Property and Casualty Annual Statement. The supplement, which would be due April 1 annually, would be required of every reporting carrier writing a stand-alone cybersecurity insurance policy or including such coverage in a commercial multi-peril package policy.

According to the NAIC, the idea behind requiring the additional report is to gain a better understanding of the cybersecurity insurance market, including what carriers are dominating the market, how much premium is being collected, and the amount and nature of the claims being submitted. The NAIC's Cybersecurity Task Force is also in the process of finalizing its "Principles for Effective Cybersecurity Insurance Regulatory Guidelines," for which the comment period concluded on April 10, 2015. The Principles are the subject of a separate article in this newsletter.

The latest draft of the proposed cybersecurity insurance coverage supplement and associated guidelines were discussed at the Spring 2015 NAIC meetings in Phoenix. The supplement is just another example of how important regulators view the role of cyber insurance in managing cyber risks, both from a preemptive risk prevention perspective, as well as from a reactive financial exposure mitigation perspective. Along those lines, meetings between state insurance regulators and federal officials regarding best practices for cybersecurity in the insurance sector took place in late April at the Treasury Department.

Cyber insurance is attracting the interest of others besides regulatory agencies. Lawmakers themselves have taken an interest in the subject. The Senate Commerce Committee's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security held what Senator Jerry Moran declared to be the first ever congressional hearing on cyber insurance on March 19. At the hearing, Senator Moran expressed interest in learning more about how cyber insurance may prove to be "a market-led approach to help businesses improve their cybersecurity posture by tying policy eligibility or lower premiums to better cybersecurity practices." More information about the hearing can be found here.

Insurance Regulatory Bellwether: NAIC Adopts 12 Principles for Effective Cybersecurity for Regulators

The National Association of Insurance Commissioners ("NAIC") is all over cybersecurity. On April 16, 2015, as a part of its aggressive work plan to help the insurance sector come up with an effective cybersecurity framework in the face of a tidal wave of data security breaches that pose a significant threat to consumer financial and health information, the NAIC's Cybersecurity Task Force adopted 12 principles for effective cybersecurity insurance regulatory guidance.

The principles are general policy statements identifying areas of concern to the NAIC and are intended to guide insurance regulators in creating specific regulations protecting the information of insurance consumers, and the information infrastructure of the insurance industry. The 12 principles address security safeguards for confidential and personally identifiable consumer information, incident response planning and consumer security breach notifications, incorporating cybersecurity risks into a company's internal risk management process, employee training and vendor management, and similar topics. Principle 4 clarifies that "Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework."

The guidelines are a bellwether of regulations to come, and insurance industry participants and their vendors should familiarize themselves with the 12 principles and consider engaging with regulators in order to anticipate and potentially help shape the future standards, requirements, and practices. Of course, they should also update and maintain appropriate data management policies and practices.

Drone Privacy Implications Following the FAA's Proposed Regulations

As Amazon recently stated in a letter to the FAA, "One day, seeing Amazon Prime Air will be as normal as seeing mail trucks on the road today." Most people are aware that drones are well on their way towards full integration in our society. In fact, on April 8, 2015, the Federal Aviation Administration (FAA) approved Amazon's bid to test its "Prime Air" package delivery drones outdoors. Drone technology is advancing so quickly that, according to Amazon, the FAA approvals issued are already obsolete.

The law is reacting to advances in drone technology, albeit at a more measured pace. In February, the FAA's proposed regulations for a limited class of commercial drone use garnered much public interest. The regulations, which are expected to become effective by 2017, are designed to provide for safe drone operation with the national airspace system. Clearly, if drones become as ubiquitous as mail trucks, they must be as safe, but what about privacy? Justice Brandeis famously asked in 1890, how can the law protect against "mechanical devices" that take "instantaneous photographs," and "threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops?" If a delivery drone can drop a package,

can it pick one up? If it navigates by camera, what else can it see? Certainly much more than a Polaroid camera on the ground.

If you are looking for guidance on the privacy implications of drone operations, you won't find it in the FAA's proposed regulations. Except for the storage of information collected during the operator certification process, privacy is explicitly outside the scope of the proposed regulations. Indeed, with the exception of privacy concerns related to drone operations at commercial test sites, the FAA has avoided regulating drone privacy in general.

Currently, there is limited legal protection from the unique privacy risks posed by commercial drones, with only a few state privacy laws specifically aimed at drones. One such law is the Texas Privacy Act, which prevents private drone use with the intent to conduct surveillance, and specifies certain private uses to which the law does not apply. For example, the law does not apply to certain uses by electric and gas utilities, licensed real estate brokers, or owners and operators of pipelines. Bills introduced in Congress have not been enacted, and the drone privacy legislation currently in committee focuses mostly on governmental use. However, in conjunction with the FAA's proposed regulations, the White House released a memorandum directing government agencies to update their privacy policies, and directing the National Telecommunications and Information Administration (NITA) to work with private stakeholders to develop a privacy framework for commercial and private drone use.

In NITA's words, its framework will address the unique privacy issues caused by the fact that drones "enable aerial data collection that is more sustained, pervasive, and invasive than manned flight." It accepted public comment through April 20, 2015. Questions posed by NITA include, Do drone-based aerial photography services pose unique privacy risks as compared to non-drone based services? Other questions are:

- Should drones maintain a certain distance from people, homes, businesses, or vehicles?
- Should the types of cameras or microphones used be regulated?
- Should drones deliver prescription medicine, or handle medical information? Serve legal process? Read electric and gas meters? Should they coach third base?

Compliance with NITA's best practices will be voluntary, and enforcement is limited. Until Congress acts, or until best practices are widely adopted, protection for privacy from commercial drones will likewise remain limited.

Guidance on CCTV Surveillance and the Responsible Use of Drones in Hong Kong

Owing to the increased popularity of unmanned aircraft systems, Hong Kong's Privacy Commissioner for Personal Data (PCPD) has issued a Guidance Note for Hong Kong on CCTV Surveillance and Use of Drones.

The Privacy Commissioner for Personal Data, Allan Chiang, said, "While the privacy implications of surveillance tools such as CCTV are fairly well understood, drones when fitted with cameras could add a new dimension to these privacy concerns by virtue of their unique attributes. To eliminate or reduce the privacy intrusiveness of the use of drones as a persistent, surreptitious, agile and efficient surveillance tool, users of drones should be particularly mindful of the need to respect people's privacy. Public perception and the reasonable privacy expectations of affected individuals should be ascertained. The alternative use of less privacy intrusive means of collection and use of personal data should be seriously considered. The intrusion on privacy can only be justified if it is proportional to the benefit to be derived."

The Guidance Note, issued on March 31, 2015, offers advice to data users (both organisational and individual data users) on determining whether CCTV should be used in given circumstances and how to use CCTV responsibly. Privacy impact assessments are expected, and special considerations apply for workforce implementations. With respect to drones, the Note explains that the same considerations and protections should apply; however, drones can be even more intrusive and more difficult from a notice perspective. At bottom, the Note is a good example of important thinking about privacy that will need to evolve along with the technology.

UK's Serious Fraud Office Fined £180,000 for Disclosure of Confidential Documents from High-Profile Investigation

On 30 March 2015, the UK's Information Commissioner's Office ("ICO") announced that it has fined the Serious Fraud Office ("SFO") £180,000 after sensitive evidence relating to 64 people involved in the BAE Systems ("BAE") bribery investigation was accidently sent to the wrong witness, and subsequently leaked to the press.

The SFO's corruption and bribery investigation concerned a BAE arms deal with Saudi Arabia. The allegations were that a BAE executive received payments, including two properties worth over £6 million, as part of BAE's sale of tens of billions of pounds' worth of arms to Saudi Arabia, from the 1980s to 2006. The case was closed in February 2010 on the grounds of public interest and concerns that relations with Saudi Arabia were being harmed.

After the bribery investigation concluded, the SFO began returning the evidentiary documentation to third parties involved in the case. Numerous bags containing sensitive personal data about third parties – including bank statements, hospital invoices, DVLA documents, and passport details – were sent to the wrong witness between November 2011 and February 2013. The witness then disclosed the confidential personal data to The Sunday Times, which published multiple articles based on this evidence.

The ICO found that the confidential evidence was wrongly sent to the witness by "a temporary worker who had received minimal training and had no direct supervision."

ICO Deputy Commissioner David Smith, reporting on the fine for the data breach, said:

> Given how high-profile this case was, and how sensitive the evidence being returned to witnesses potentially was, it is astounding that the SFO got this wrong. This was an easily preventable breach that does not reflect well on the organisation. All law enforcement agencies should see this penalty as a warning that their legal obligations to look after people's information continue even after their investigation has concluded.

The ICO took into account various mitigating steps taken by the SFO in determining the extent of the fine, including that:

1. the SFO made immediate efforts to recover the information from the witness,
2. 98% of the information in bags was recovered with their seals intact,
3. the SFO voluntarily reported the case to the ICO, and
4. the ICO is not aware of similar previous security breach.

North Dakota Broadens Reach for Breach Notification

North Dakota recently enacted an amendment that will again tighten its existing breach notification law. The current law, North Dakota Century Code Section 51-30 et. seq., has evolved over time, having been previously amended in 2013 to add health information to the definition of "personal information" that could trigger a notification if breached. This new amendment may be a result of recent large data breaches and a concern that existing law did not require notification of the Attorney General or notification to residents if a company was not "conducting business" in North Dakota.

The amendment broadens the reach of the existing breach notification law by requiring a company to notify affected North Dakota residents regardless of whether the company operates in North Dakota. And for large breaches that impact more than 250 individuals, the Attorney General must now be notified by mail or e-mail. The definition of "personal information" has been updated again – this time to add an employer's identification number assigned to an individual in combination with any required security code, access code, or password. The amendment will take effect on August 1, 2015.

FTC Actions Highlight Pitfalls for Failing to Comply with the International Safe Harbor Privacy Frameworks

The Federal Trade Commission recently agreed to settle claims against two companies alleging that the companies were not abiding by the U.S.-EU Safe Harbor international privacy framework. While the U.S.-EU Safe Harbor permits companies to self-certify compliance and transfer data from the EU to the U.S. in compliance with EU law, these latest cases highlight the importance of making sure the certifications are accurate and up to date.

The FTC has stressed that these cases "send an important message that businesses must not deceive consumers about whether they hold these certifications, and by extension, the ways in which they protect consumers."

As outlined in the Department of Commerce's FAQ on Safe Harbor Self-Certification, in order to self-certify an entity must submit to the U.S. Department of Commerce a letter signed by a corporate officer that includes a description of the activities of the organization with respect to personal information and a description of the organization's privacy policy. With respect to the privacy policy, the company must include its effective date, contact information, the specific statutory body that has jurisdiction to hear any claims against the organization, and an independent recourse mechanism to resolve unresolved complaints.

The Department of Commerce offers some helpful hints on self-certifying. Among them, self-certifying organizations may choose to use a private sector dispute resolution program, or they may choose to cooperate with and comply with the EU data protection authorities. The BBB EU Safe Harbor Program, TRUSTe, Direct Marketing Association, the Entertainment Software Rating Board, JAMS, and the American Arbitration Association all offer programs in compliance with the Safe Harbor's Enforcement Principle.

However, as illustrated in the latest FTC cases, an organization should pay close attention to selecting and correctly identifying its independent recourse mechanism, because a selection of one dispute resolution program in certification documents while displaying another form of dispute resolution on an organization's website may be deceptive to consumers.

In addition, organizations that self-certify compliance must remember that certification must be renewed on an annual basis. Claiming certification in a posted privacy policy after failing to renew can also be viewed as deceptive to consumers.

A company that self-certifies should be sure it understands the Safe Harbor Privacy Principles and that its privacy policy is readily accessible and conforms to the Principles. Before submitting for certification, the company should designate a contact regarding the Safe Harbor, establish a procedure to verify compliance, and be clear and consistent as to the independent recourse mechanism the company is going to use.

Cyber Bills Gain Momentum as DOJ Issues Cyber Guidance

While the U.S. Congress has been faulted for failing to find common ground on many issues, one exception seems to be cybersecurity and data sharing. Three bills are in Congress that address the reporting and sharing of private sector cyber issues, shielding private entities from liability arising from cyber mitigation efforts, as well as coordinating efforts between government agencies. The U.S. Department of Justice has also issued its Best Practices for Victim Response and Reporting of Cyber Incidents, which is another example of the importance Congress and the Executive Branch are placing on cyber awareness and information sharing.

Senate bill 754, the Cybersecurity Information Sharing Act of 2015, permits private entities to detect, prevent, mitigate, and employ defensive measures against cyber threats. The bill essentially codifies the current U.S. DOJ antitrust exemption for the sharing of threat data and mitigation techniques amongst private entities. It requires the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Department of Justice to promulgate procedures to share classified and declassified cyber threat indicators with non-governmental entities. In addition, it reinforces the need to examine policies to ensure that civil liberties and privacy rights are not abridged. The bill also shields private entities from civil liability for entities acting in accordance with the bill. It has been passed by the Senate Intelligence committee and is awaiting a vote on the Senate floor.

House bill 1560, the Protecting Cyber Networks Act, and House bill 1731, the National Cybersecurity Protection Advancement Act, passed the House overwhelmingly. These two bills are similar to the Senate bill in that they encourage the sharing of threat data while shielding the sharing entities from civil liability. The bills also require changes to federal agency coordination and enact the antitrust-like data sharing exemption as in the Senate bill. H.R. 1751 expands the role of the department of Homeland Security National Cybersecurity and Communications Integration and Intelligence Center (NCCIC) to include private and non-federal governmental entities.

These bills would not require the reporting of cyber threats to any federal agency. They are written to permit the voluntary sharing of threats and mitigation techniques in an attempt to strength U.S. cyber defense. The limitation of liability for information sharing, as well as the codification of the anti-trust exemption, are important for the successful coordination of cyber threat mitigation. Congress and the Administration appear to be in agreement that the coordination and sharing of threat data is paramount to the mitigation of cyber threats.