Worldwide ERC®
Data Privacy and Security Task Force
Summary of Resources
October 9, 2015

Recognizing the increasing importance to its members of compliance with laws and regulations concerning the protection of personally identifiable information, Worldwide ERC® appointed a Task Force in 2015 to address the myriad of issues that arise. The Data Privacy and Security Task Force undertook a detailed study focused on identifying resources that it believed would be helpful to Worldwide ERC® members in seeking to comply with such laws and regulations, and its report is provided here. The Task Force report contains an extensive collection of important and useful links to sources of detailed information on data privacy and security. It will enable Worldwide ERC® members to find information they need to understand the laws and regulations that apply across the world, and to create a strong culture protecting personally identifiable information of transferees and others. Worldwide ERC® intends that this material will be updated regularly, and will be available to all members.

The following is a summary of what we believe are some of the best sources of current, dependable, and accessible information regarding data privacy and security issues for members of Worldwide ERC®.

I. GENERAL DATA PRIVACY AND SECURITY RESOURCES

A. Maximizing the Value of a Data Protection Program.

This Ernst & Young publication was the June 2014 edition of the Insights on Governance, Risk and Compliance series. It provides a succinct yet comprehensive outline for developing a highly effective data protection program that can be tailored to the unique needs of any business in any industry. This publication also provides helpful strategies for successful implementation of a data protection program, as well as insight into proper maintenance for achieving long-term results. This publication can be used as a blueprint for members of Worldwide ERC as they begin the process of increasing the protection of their clients' sensitive data, as well as their own. The report can be found at http://www.ey.com/Publication/vwLUAssets/EY__Maximizing_the_value_of_a_data_protection_program/$FILE/EY-insights-on-grc-data-protection.pdf.

B. Privacy & Data Security Law Resource Center.

Created and owned by Bloomberg's Bureau of National Affairs ("Bloomberg BNA"), this web-based platform provides authoritative, in-depth privacy and security law resources for lawyers and businesses alike. The Resource Center provides information on a wide range of topics in the area of data privacy and security, which can be individually customized to fit each customer's specific needs. It contains resources such as industry-leading news and commentary which includes comprehensive daily coverage of the latest developments, legal analysis from expert practitioners and Bloomberg BNA treatises, a comprehensive collection of U.S. domestic (federal and state) and international laws and regulations, and other relevant Bloomberg BNA insights. This is an essential resource for members to stay on top of data privacy and security issues. The Resource Center is a subscription-based service available at http://www.bna.com/privacy-data-security-p17179869769/.

C. Privacy Trends.

This is an annual edition of Ernst & Young's Governance, Risk and Compliance series that examines the external factors which have a significant impact on the ability to effectively manage private information in the context of a constantly evolving environment. Previous topics have covered (a) the utilization of high internal compliance standards and enforcement strategies by organizations and industries seeking to avert governmental expansion of more costly regulation, (b) the need for accountability to maintain strong compliance standards in the face of a changing environment (such as the emphasis on maintaining digital records of sensitive information), and (c) the strategies for containing the constant threat presented by a technology sector that innovates and evolves too quickly for regulation and counter-technologies to provide adequate protection alone. These

articles identify both hostile and helpful trends so that members can utilize or prepare for the potential impact on their private data. The report can be found at http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf.

D. Verizon Data Breach Investigations Report.

This is an annual publication from Verizon that examines the most recent and relevant data breaches and extracts the pertinent information that can help industries and organizations improve their efforts to keep their private and sensitive data secure. The Data Breach Investigation Report has examined 100,000+ data and security breaches over the last decade and, through its analysis, has identified nine distinct attack patterns that comprise 92% of all data and security attacks. The publication continually expands upon these patterns to keep information on their development current. This publication can be very helpful for members of Worldwide ERC as it will allow their security programs to anticipate and quickly identify future attacks. The report can be found at http://www.verizonenterprise.com/DBIR/2015/.

E. Information Security and Privacy: A Guide to Federal and State Law and Compliance; A Guide to International Law and Compliance.

This resource comprises two comprehensive volumes on United States federal and state privacy and security laws, as well as a volume on international privacy and security laws. It provides an in-depth look at data laws and regulations and communicates effective compliance with them. This resource is essential for any organization seeking to remain in compliance with U.S. domestic and foreign privacy and security laws. This publication is authored by Andrew B. Serwin and is published by Thomson Reuters, ISBN 978-0-314-61076-8.

F. Electronic Privacy Information Center ("EPIC") Online Guide to Practical Privacy Tools.

A web-based platform from EPIC, this website is a comprehensive collection of resources that can aid any organization looking for technology tools to further secure its sensitive data. It includes, among many others, links to sites with information on snoop-proof e-mail, anonymous remailers, html filters, cookie busters, encryption services for many forms of electronic data, and many additional privacy resources. The website can be found at https://www.epic.org/privacy/tools.html.

G. Data Breach Incidents & Responses.

This survey by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association provides a look at the prevalence, causes, and consequences of data breaches. The survey analyzes the leading factors that result in data breaches. Specifically, the survey provides a breakdown of the sources of data breaches, how the breaches were discovered, and the cost of data breaches. The survey is important because it highlights the fact that, for all of the concerns over digital breaches, simple things such as lost documents and memory devices present the greatest threat of data breaches. This is an important reminder to members of Worldwide ERC that strict adherence to strong policies regarding sensitive documents and memory devices is imperative to preventing the loss of private data. The survey can be found at http://www.corporatecompliance.org/Resources/View/ArticleId/881/Data-Breach-Incidents-Responses-1.aspx.

H. National Association of Corporate Directors.

The NACD has bundled their most recent guidance on cyber issues into the NACD Cyber-Risk Oversight Toolkit, available through membership on the NACD website. The toolkit offers access to several publications, tools, and educational materials to help corporate leaders stay on top of the threats facing their private and sensitive data. The NACD Cyber-Risk Oversight Toolkit can be found at http://blog.nacdonline.org/2015/08/cyber-risk-oversight-toolkit/.

I. World Economic Forum Website.

The World Economic Forum Website can serve as an additional resource when members of Worldwide ERC have questions that may not be answerable by the aforementioned resources. They can search this site for current reports on data privacy and security developments. The site will provide links to articles and resources that members of Worldwide ERC can use to familiarize themselves with the topic to determine their next steps in regard to the specific matter, whether that means they need not take further action or they need to update their current privacy and security program. The website can be found at http://www.weforum.org/reports.

J. Chronicle of Data Protection.

Maintained by the law firm Hogan Lovell, the Chronicle of Data Protection is a blog dedicated entirely to privacy and information security news and trends. The website publishes articles, webinars, and other media on global topics and developments in the data privacy and security field as it pertains to all industries. This is a great resource providing the most important and current information on data privacy, and can be found at http://www.hldataprotection.com/.

K. Skadden, Arps, Slate, Meagher & Flom Privacy & Cybersecurity Updates.

This is a monthly update from the international law firm Skadden Arps that contains relevant and useful information on the legal developments of data privacy and security laws as they are enacted through legislation, assessed, and put into practical use. These updates would be beneficial to members of Worldwide ERC as they provide insight into the practical application of data privacy laws, allowing, among other things, members to assess how they might engage similar situations in the context of their own legal strategies. These updates can be found at https://www.skadden.com/insights.

L. DLA Piper Insights on Cybersecurity and Data Privacy.

The international law firm DLA Piper, with headquarters in both London, England and Chicago, Illinois, publishes numerous articles and events (in the form of webinars) that address the recent trends, challenges, and developments in cybersecurity and data privacy. These reports focus on all major global topics and issues, though there is focus on developments within the EU. These publications can be found at https://www.dlapiper.com/pl/uk/.

M. Linklaters Technology, Media & Telecommunication Publications.

These are publications from the UK-based international law firm Linklaters that analyzes, among other things, technological and legal developments and their impact on information management and security. The publications can be larger, more official editions as well as individual articles that contain developments pertaining to EU and EU country-specific as well as global events. The publications can be found at. http://www.linklaters.com/insights/pages/publicationsearchresults.aspx?name=&practice=Information%20Management%20and%20Data%20Protection&location=All&quals=All.

N. Getting Your Cybersecurity Breach-ready.

A six part series from Shamoil T. Shipchandler and Rachel M. Riley of the law firm Bracewell & Giuliani, the series focuses on preparing your cybersecurity program for the inevitable breach. Each part in the series provides insight into a crucial component of the overall framework required for an effectively responsive data security program. It also includes links to other resources that are helpful for a further understanding of each part's focus. Part six of the series (with links to the previous 5) can be found at http://www.insidecounsel.com/2015/08/17/getting-your-cybersecurity-breach-ready-part-6-han?t=cybersecurity-privacy.

O. National Institute of Standards and Technology: Guidelines on Security and Privacy in Public Cloud Computing.

This publication from the United States Department of Commerce provides an overview of the security and privacy challenges pertinent to public cloud computing. The publication highlights considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment. Although published at the end of 2011, it still provides a good summary of the risks of using public cloud storage and computing and the security and privacy of using the cloud. The publication can be found at http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

P. American Institute of CPAs ("AICPA"): Privacy Risk Assessment Questionnaire.

Published on May 26, 2015 by the AICPA, this article presents key questions businesses should ask about privacy risk, implementing sound privacy policies and practices, managing privacy risk, and obtaining privacy assurance. Members can run through the questions presented in this article to give themselves a quick assessment of their understanding of privacy risk. The article can be found at https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/Pages/Privacy%20Risk%20Assessment%20Questionnaire.aspx.

Q. Data Protection Global Guide.

This is a collection of overviews of data protection legislation of many prominent jurisdictions. The pages are authored by lawyers specializing in data protection law at leading law firms in their jurisdictions. Importantly, each page presents the rules governing the transfer of private data outside of the jurisdiction. Each page also provides an overview of the law of the jurisdiction and its application, a discussion of the rights of data subjects, and a breakdown of the enforcement mechanisms and penalties for non-compliance. The article can be found on Practical Law, a subscription service available at http://us.practicallaw.com/us/resources/global-guides/dataprotection-guide.

R. Future-proofing Privacy: a Guide to Preparing for the EU Data Protection Regulation.

Published by the law firm Hogan Lovell, this work provides a comprehensive discussion of the new EU Data Protection Regulation which introduces greater accountability obligations, stronger rights for data subjects, and ongoing restrictions on international data flows. The publication offers guidance on the best methods for adapting to and navigating the new regulation. The publication can be found at http://www.hoganlovells.com/files/Publication/cee0104e-9625-4a3c-9d57-dc7c810da2fe/Presentation/PublicationAttachment/7f46bf34-5f15-4aeb-9ec6-e79f28981d95/100273_CM3_Data%20Privacy_BRO_E_link.pdf.

II. CYBER INSURANCE RESOURCES

A. NetDiligence Cyber Claims Study 2014.

This is an annual study from NetDiligence that uses cyber liability insurance reported claims to demonstrate the real costs of incidents from an insurer's perspective. The study looked at claims in order to get a better picture of the types of data exposed, the cause of loss, the business sector in which the incident occurred, and the size of the organization. From our members' perspective, it can provide insight into not only the need for cyber insurance for data breaches and costs associated with data breaches, but also the most common types of data exposures and causes of the loss. The study can be found at http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf.

B. Cyber Insurance for Data Breaches.

This article discusses cyber insurance coverage for data breach incidents. Particularly, it addresses the need for coverage, typical coverage, key considerations in selecting coverage, and the application process. The article can be found on Practical Law, a subscription service available at http://us.practicallaw.com/us-homepage.

C. Views on Corporate Cybersecurity Insurance Option.

This article is presented as a Q&A session between Bloomberg BNA and Thomas H. Bentz, Jr., of the law firm Holland & Knight. In his answers to Bloomberg BNA's questions, Mr. Bentz addresses many topics regarding cybersecurity insurance. These topics include, among others: (a) the importance of cybersecurity insurance in the wake of legislative actions and case law decisions increasing the vulnerability of organizations to lawsuits after experiencing data breaches, (b) the scope of coverage organizations should obtain, and (c) guidance for ensuring organizations get the most out of a policy from their insurer. The article can be found at http://www.hklaw.com/files/Publication/fee5740f-9d04-47e0-ab24-3a92b3762d1f/Presentation/PublicationAttachment/776272f3-f366-4e91-bd60-b12ab89fee3a/0817CorporateCybersecurity.pdf.

D. Cyber Risk Management: New Threats, New Approaches.

This publication from September 2015 was created by Marsh LLC and provides an overview of the cyber threats that organizations face, the role and accountability of organization members, and strategies for combating the risks presented by cyber threats. This article offers a unique perspective since the information presented is from the perspective of an insurance broker, an organization that would have extensive knowledge of the most common types of threats and breaches. The purpose of the publication is to present what Marsh appears to consider an inconvenient truth – that "even an unlimited budget for information security will not eliminate your cyber risk," reminding organizations of the need for cyber insurance. The publication can be found at https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20NROR%20Cyber%20September%202015.pdf.

E. Cyber Risk Insurance.

This webpage from Marsh LLC contains many publications under their Insights on important news and events on the topic of cyber risk insurance. The goal of the page is to address organizations risk management and insurance needs by assessing not only at the technological aspect of organizations, but by assessing the organization as a whole. The page, which offers a registration service to access the entire volume of its content, can be found at https://www.marsh.com/us/services/cyber-risk.html.

III. INTERNATIONAL DATA PRIVACY AND SECURITY RESOURCES

A. ISO/IEC 27001: 2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements.

This ISO publication covers information security system requirements for many types of organizations (e.g. commercial enterprises, government agencies, and not-for-profit organizations). ISO/IEC 27001:20013 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system within the context of the organization's overall business risks. This publication is available for purchase at http://www.iso.org/iso/home/store/catalogue_detail_ics.htm?csnumber=54534.

B. ISO 31000: 2009, Risk Management – Principles and Guidelines.

This ISO publication provides principles, framework, and a process for overall enterprise risk management. It can be used by any organization regardless of its size, activity, or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment. This publication is available for purchase at http://www.iso.org/iso/catalogue_detail?csnumber=43170.

C. Privacy & Security Law Report: Privacy Laws in Africa and the Middle East.

From a series in the Privacy & Security Law Report from Bloomberg BNA by Cynthia Rich of the law firm Morrison & Foerster, this article covers the status of data protection laws in Africa and the Middle East. The article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments, such as the June 2014 adoption of the African Union Convention on cybersecurity and data protection, which could see the amount of countries in the region with comprehensive data privacy frameworks increase substantially from the current number of 18. The article also discusses the legislation under development in some countries and contains a breakdown of the laws of specific countries with established data privacy frameworks. The article can be found at http://www.insidecounsel.com/resources/4734f9732b4258c1a45058e62a66bfda.

D. Privacy & Security Law Report: Privacy Laws in Asia.

From a series in the Privacy & Security Law Report from Bloomberg BNA by Cynthia Rich of the law firm Morrison & Foerster, this article covers the status of data protection laws in Asia. Similar to above, this article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments, such as China's slow, piece-meal, and sectoral move towards a comprehensive privacy regime, and Thailand's reported steps towards enacting privacy legislation. The article also discusses the legislation under development in some countries and contains a breakdown of the laws of specific countries with established data privacy frameworks. The article can be found at http://www.insidecounsel.com/resources/76f6f067672916becc871a76d509db50.

E. Privacy & Security Law Report: Privacy Law in Latin America and the Caribbean.

From a series in the Privacy & Security Law Report from Bloomberg BNA by Cynthia Rich of the law firm Morrison & Foerster, this article covers the status of data protection laws in Latin America and the Caribbean. Similar to above, this article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments. The article can be found at http://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/PVRC/Privacy_Laws_Latin_America.pdf?elqTrackId=B1BE04049403C22ADB6A7C7541A0EC97&elqaid=168&elqat=2.

F. Global Data Privacy Directory.

From the London, England-based international law firm Norton Rose Fulbright, the Global Data Privacy Directory is a comprehensive directory of data privacy and security laws from around the world. It is designed to give businesses an overview of the data legislation applicable in key jurisdictions as well as the restrictions on the transfer of personal data in those jurisdictions. The directory can be found at http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf.

G. American Institute of CPAs ("AICPA"): Comparison of International Privacy Concepts.

Published by the AICPA, this article presents a table that offers a comparison of privacy concepts from Australia, Canada, EU, and the Organization for Economic Cooperation with the AICPA's generally accepted privacy principles. The article can be found at http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/InternationalPrivacyConcepts.aspx.

IV. UNITED STATES DATA PRIVACY AND SECURITY RESOURCES

A. Best Practices for Victim Response and Reporting of Cyber Incidents.

The United States Department of Justice ("DOJ") has issued guidance on the best practices for responding to breaches of private and sensitive data. The purpose of the guidance is to provide the "best practices for victims and potential victims to address the risk of data breaches, before, during and after cyber attacks and intrusions." The premise of the best practices outlined by the DOJ emphasizes organizations conduct their own risk assessments, the results of which should be incorporated into incident response plans. These best practices can be found at http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

B. Framework for Improving Critical Infrastructure Cybersecurity.

The United States government has released a new cybersecurity framework aimed at helping operators of critical infrastructure develop their cybersecurity programs. The framework is voluntary and is designed to create a consensus on what a good cybersecurity framework looks like. The framework can be found at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

C. White House Cybersecurity Rules for Contractors.

The United States government has released draft guidelines for government contractors that handle private data to follow baseline security and reporting requirements. The new requirements come in the wake of several high-profile and damaging security breaches of government agencies and contractors. It will be crucial for members of Worldwide ERC which have government contracts to be sure to adhere to these new requirements, especially considering the damage that would be caused if a large data breach were to occur in the relocation management industry. A brief overview of the proposed guidelines can be found at http://thehill.com/policy/cybersecurity/250869-white-house-issues-cybersecurity-rules-for-contractors.

D. Improving Cybersecurity Protections in Federal Acquisitions.

The purpose of this proposed memorandum from the Federal Chief Information Officers Council and the Chief Acquisition Officers Council is to provide guidance to federal agencies on implementing strengthened cybersecurity protections in acquisitions for products or services that in any way touch sensitive information on behalf of the federal government. Specifically, the proposed memorandum advocates focus on the areas of (a) incident reporting and notification, (b) information system assessments, and (c) information security continuous monitoring. While these best practices may be intended for government agencies, they can be utilized by any organization seeking to improve their handling of sensitive data. The proposed memorandum can be found at https://policy.cio.gov/.

E. American Institute of CPAs ("AICPA"): Generally Accepted Privacy Principles.

Published in August 2009 by the AICPA and the Canadian Institute of Chartered Accountants ("CICA") Privacy Task Force, this article presents the principles this group views as governing privacy of data, customers, and stakeholders. It was designed to assist management in creating an effective privacy program that addresses privacy obligations, risks, and business opportunities. The article can be found at http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx.

V. EUROPEAN UNION DATA PRIVACY AND SECURITY RESOURCES

A. European Union Data Privacy Directive.

European Union data privacy and security laws can be found in the summary of legislation on the European Union website. This website contains the Data Privacy Directive which currently governs European Union data privacy. Additionally, the European Union has recently voted on a new framework for a comprehensive reform of the Data Privacy Directive. Once this framework has been adopted and put into legislation, it will also be available in the summary of legislation on the European Union Website. The text of the legislation and a summary of the key points can be found at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.

B. Model Contract Clauses.

Based on the eight principles of the Data Protection Act of 1998, which was enacted to bring British law into compliance with the EU Data Privacy Directive, the model contract clauses govern international transfers of personal data. The purpose of the model contract clauses is to ensure that foreign companies are providing adequate protection of personal data to the same standard required by the Data Protection Act of 1998, and by extension, EU law. The model contract clauses achieve this by establishing the foreign organization's privacy obligations for a transfer. Although the model contract clauses are a creation of British law, they can be used by organizations in other EU countries seeking to do business with organizations not governed by EU law to ensure the non-EU organizations are adequately protecting personal data to the standard required by EU law. Further information on the model contract clauses can be found with the UK's Information Commissioner's Office at https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf.

C. Binding Corporate Rules.

BCRs are designed to allow organizations to transfer personal data to affiliates or other related organizations located outside of the EU while maintaining compliance with the EU Data Privacy Directive. The purpose of BCRs is to save organizations time and money by allowing them to avoid having to approach each data protection authority separately. Rather, organizations can submit their BCRs to a select lead data protection authority based on criteria such as the location of an organization's EU headquarters (described in the Working Party papers and the various instruction and application forms needed to obtain BCRs). If the lead data protection authority is satisfied with the level of data protection described in the application, it will distribute the BCRs to the other data protection agencies in Europe. Essentially, the lead data protection authority facilitates the authorization process for the transfer of personal data within a defined controlled group of companies. BCRs can provide for a variety of intra-group data transfers that an organization may require while also allowing for the accommodation of changes in organization structure and data flow. Further information on BCRs can be found at https://ico.org.uk/for-organisations/binding-corporate-rules/.

VI. CANADIAN DATA PRIVACY AND SECURITY RESOURCES

A. Canadian Data Privacy Laws.

Canadian data privacy and security laws can be found on the website of the Office of the Privacy Commissioner of Canada. This website includes data privacy laws at both the federal and provincial levels, as well as brief explanations of how they are applied. The website can be found at https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp.

B. Canadian Data Privacy Toolkit.

The Office of the Privacy Commissioner of Canada has prepared this guide to help organizations fulfill their responsibilities under the Personal Information Protection and Electronic Documents Act ("PIPEDA"). This publication highlights, among other things, how PIPEDA applies, the responsibilities of organizations under PIPEDA, and strategies and resources for effective compliance with PIPEDA as well as for effective data privacy and security in general. The website can be found at https://www.priv.gc.ca/information/pub/guide_org_e.asp.

C. Miller Thomas LLP, Business Laws of Canada, 2014-2015 Edition.

This book is authored by Kathryn Frelick, a partner and leader of the privacy practice at the Toronto-based law firm Miller Thomson. The book covers business laws of Canada, but in particular, chapter 9 addresses many of the pertinent privacy laws in Canada and their affect on businesses in their dealings with consumers. Additionally, chapter 22 takes a closer look at privacy laws of Canada in general, which also contains a breakdown of provincial-specific laws. It is available for purchase at http://legalsolutions.thomsonreuters.com/law-products/Treatises/Business-Laws-of-Canada-2014-2015-ed/p/100385075.

D. McCarthy Tétrault Cybersecurity, Privacy and Data Protection Blog.

The Toronto, Canada based law firm McCarthy Tétrault has recently launched a new blog with a focus on cybersecurity and data privacy. The blog, called CyberLex, which is updated regularly, features trends and developments in cybersecurity, privacy, and data protection law in Canada and internationally. It offers practical suggestions and insights on how these issues affect companies in a wide variety of industries and provides guidance on how to address the challenges and opportunities created by developments in these areas. The blog can be found at http://www.canadiancybersecuritylaw.com/.

VII. RECENT DEVELOPMENTS

A. Healthcare Security Breaches (March 2015).

Two major healthcare organizations, Premera Blue Cross and Anthem, Inc., were the subjects of hacking incidents that together affected the private information of nearly 100 million individuals. These incidents are part of a growing trend of hackers targeting health information. Hackers have targeted protected health information (ex. medical histories), personally identifiable information (ex. social security numbers), as well as intellectual property (ex. medical device and equipment development data). This trend appears to be due to several factors such as the expanding number of access points to health information and the longer term value of health information (as opposed to credit card information which may only be valuable to a hacker for a few days) which makes the healthcare industry a vulnerable and attractive target for cybercriminals. The U.S. Health and Human Resources Department publishes a "shame list" that includes all healthcare providers that reported a breach of healthcare information. That list can be found at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

B. Target Corporation (April 2015).

In its February 2015 Form 8-k filing to the U.S. Securities and Exchange Commission, Target reported that the costs related to its 2013 data breach have exceeded $252 million. On April 15, 2015, Target announced that it reached a settlement to reimburse MasterCard International Incorporated up to $19 million for losses related to the data breach. On September 15, 2015, five financial institutions which have not settled recently won class action status going forward in their suit against Target. In granting the status, U.S. District Court Judge Paul A. Magnuson ruled that an action does not need to be legally mandated to establish injury or causation, rejecting an argument made by Target which would have narrowed the liability for organizations that have been breached.

C. United States Office of Personnel Management (June 2015).

The Office of Personnel Management ("OPM") announced that it had experienced a data breach ultimately affecting almost 22 million people. The breach not only exposed the sensitive personal information of current and former government employees, but it exposed the personal information of their friends and families as well. The breach has been extremely damaging to the United States' intelligence networks and the individuals whose information was exposed. It is believed that the hackers gained access to the data using legitimate credentials obtained via social

engineering. This is an effective method for gaining access to secure information because it allows those perpetrating the breach to sidestep even the most advanced security measures, and it highlights the necessity for any organization to focus not only on the technical side of data security but also on the human element as well. On September 23, 2015, the OPM announced that the breach had resulted in the theft of 5.6 million fingerprints, five times the 1.1 million figure that was given in the original announcement.

D. Ashley Madison (July 2015).

The extramarital affair website Ashley Madison suffered a data breach at the hands of a group calling itself the "Impact Team," which bills itself as hacker activists ("hacktivists"). Due to the nature of the service Ashley Madison provides, secrecy and data security were essential elements to its operation. The breach exposed the personal data and information of Ashley Madison clientele, leaving those affected open to blackmail and public ridicule. Further, the clientele filed a $567 million class-action lawsuit against Avid Life Media, the owner of Ashley Madison. The consequences have been significant, and it is unlikely Ashley Madison will ever recover, regardless of the outcome of the lawsuit. Furthermore, it is possible that this data breach will have a negative impact across the entire spectrum of internet dating sites, as users of more reputable dating sites may fear the industry in general, and by extension their sensitive data, is vulnerable to future breaches. This breach highlights the financial and reputational impact data breaches can have on an organization as well as an entire industry, demonstrating the need for dialogue and cooperation among industry participants to ensure all are taking the necessary measures to protect consumer data.

E. Hilary Remijas v. Neiman Marcus Group, LLC, 794 F.3d688 (7th Cir. 2015).

This article from the Junto Blog is presented as a Q&A with Ben Barnow of Barnow Associates regarding the implications of the decision of the Seventh Circuit Court of Appeals in the Neiman Marcus case. The decision established the legal standard for liability in data breach cases of "likely future fraud or injury," which is a significant reduction from the previous standard of "impending certainty." Such a reduction in the standard should force organizations to take necessary measures to ensure their sensitive date is secure, otherwise they will almost certainly face litigation before an unfriendly court. The article can be found at http://juntoblog.net/what-does-the-neiman-marcus-ruling-mean-for-data-security-law/.

F. Proposed Federal Cybersecurity Legislation.

This article was authored by Erin Fonté and Jacqueline Allen of the law firm Dykema Gossett and discusses the following two potential federal data privacy and security laws. The article can be found at http://www.insidecounsel.com/2015/09/08/proposed-federal-cybersecurity-legislation.

1. H.R.1770. A federal data breach notification law proposed by the House of Representatives, it would preempt the various state laws that currently define what a data breach is in those individual jurisdictions. Additionally, the law would impose a 30-day period in which companies must notify consumers affected by a data breach. The law would not preempt other federal notification laws such as the Gramm-Leach-Bliley Act. H.R. 1770 also expands the definition of "personal information" to include additional data fields not typically covered under state laws such as biometric data and consumer unique account identifiers. Importantly, it excludes encrypted information from the definition, providing a safe harbor for organizations that take advanced steps to protect data.
2. S. 754. The Cybersecurity Information Sharing Act of 2015 ("CISA") is currently pending in the Senate and would enhance cybersecurity information sharing between private and government entities. CISA would permit private entities to exchange information about certain cyber threat indicators with the federal government in an effort to prevent future cyberattacks. Companies that choose to share information with the government in accordance with CISA would be protected from liability for doing so.

G. Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, [2015] (October 2015).

On October 6, 2015, the European Court of Justice invalidated the Safe Harbor agreement established on July 26, 2000, by [European] Commission Decision 2000/520/EC using the principles found in Article 25(2) of [EU] Directive 95/46/EC by ruling that the Safe Harbor agreement did not eliminate the need for local privacy watchdogs to check U.S. organizations were taking adequate data protection measures. Going forward, EU organizations seeking to export personal data to U.S. organizations must undertake greater measures, such as utilizing model contract clauses, to ensure data protection. The impact of this decision will be an increase in the costs of doing business between EU and U.S. organizations. Further information on the decision can be found at http://www.bbc.com/news/technology-34442618.