Warner Norcross&Judd® LLP
ATTORNEYS AT LAW

A Retrospective of eDiscovery, Information Governance and Data Security in 2015

Welcome,

Warner Norcross & Judd is pleased to share this overview of legal changes, trends and case studies in the 2015 calendar year. In this paper we'll review:

- Specific law changes, amendments and ethical obligations
- Updates to regulations and unique cases that have fueled these updates
- Data breach case studies

As the amount of data that companies collect and generate continues to increase, the risks associated with that data also increase, from the risk of data breaches to the risk of expensive disclosures in litigation. This information is meant to provide you with a deeper look into these trends in order to benefit your organization.

Scott R. Carvo

Partner at Warner Norcross & Judd LLP

B. Jay Yelton III

Partner at Warner Norcross & Judd LLP

Biggest Developments in 2015

EU Court of Justice Invalidates the U.S. —EU Safe Harbor Program

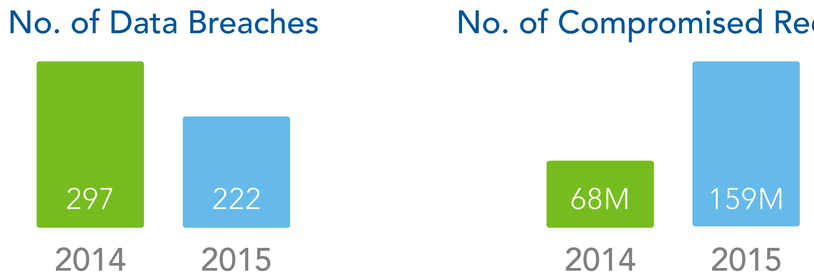
In October, the European Union Court of Justice invalidated the 15-year-old data transfer Safe Harbor agreement between the U.S. and EU. The Safe Harbor allowed U.S. companies to self-certify compliance with EU data protection laws so that personal data could be transferred from the EU to the U.S. under EU laws. With the Safe Harbor removed, European privacy regulators have stated that tougher oversight of data transfers, including issuing fines and banning overseas data transfers, is on the horizon if a new Safe Harbor agreement cannot be reached. In the meantime, the EU Commission has indicated that the only viable way currently to transfer data from the EU to the U.S. is either through certain Binding Corporate Rules (BCRs) or the use of Standard Contractual Clauses (SCCs).

BCRs can take significant time to set up and receive approval from the EU data protection agency in each EU country, so the most practical short-term solution is to utilize SCCs.

Companies that have relied on the Safe Harbor program to date should review their current contracts and update them with these SCCs as necessary.

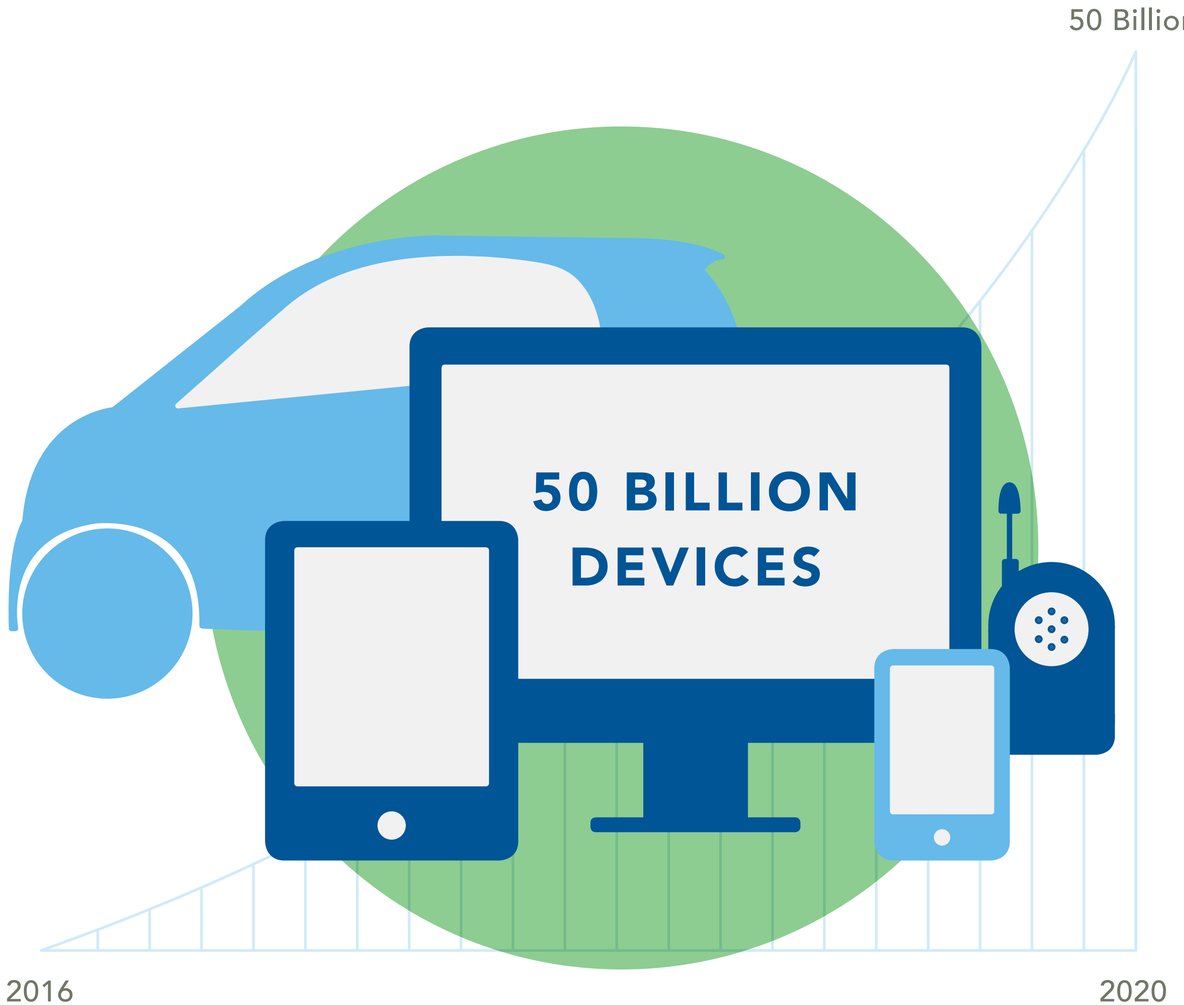
2015: The Year in Data Breaches

Early analysis of data breaches in the United States for 2015 paint a good news/bad news picture when compared with the previous year. According to one clearinghouse, the total number of data breaches was down by nearly 25%, decreasing from 297 to 222 publically reported breaches. The number of records involved in the breaches, however, jumped significantly, a steadily increasing trend. For those breaches where the number of compromised records is known, 159 million records were compromised in 2015.



Compare this with almost 68 million in 2014 and companies have good reason to be concerned about the ongoing threats to their data. The average number of records compromised per breach in 2015 was about 718,000. Businesses involved in the financial and insurance industries experienced the highest per breach average, with 3.3 million records accessed per breach. Those businesses involved in industries other than retail, health care and the financial industry experienced the greatest number of breaches—85 in 2015—though the breaches themselves tended to be smaller, averaging only 27,000 records per breach.[1]

[1]*Source: http://www.privacyrights.org/data-breach*



Internet of Things Vulnerabilities Exposed

Experts estimate that by 2020 there will be 50 billion devices connected to the Internet.[1] The proliferation of the "Internet of things"—the network of connected objects with the ability to communicate with each other and with people—brings both untold potential benefits to businesses and consumers, as well as security and privacy risks.

2015 saw the exposure of security vulnerabilities in several connected devices including automobiles, baby monitors, medical devices, thermostats and even firearms.

Vulnerabilities in some of these devices—those capable of collecting, transmitting or even storing personal information—can be exploited to allow hackers to access and misuse personal information, often without the device's end-user even being aware of the intrusion. Potential reasons for the vulnerabilities are many, including a lack of ability or desire to patch known security risks and a lack of experience in security for companies manufacturing Internet-enabled devices for the first time. Ultimately, whether most consumers will buy such devices may hinge on whether they trust the devices to keep their information secure.

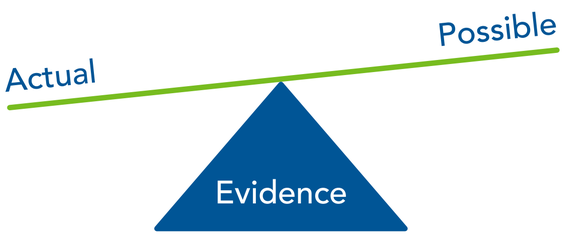
[1] *DHL Trend Report Internet of Things 2015*

FTC's Mixed Bag of Results in Data Security Enforcement Litigation

In the last 15 years, the Federal Trade Commission has taken a lead role in privacy enforcement, settling over 50 cases involving information security practices relating to consumer data. But in recent litigation, Wyndham Worldwide Corp. challenged the FTC's enforcement authority in this arena.

In August 2015, the Third Circuit Court of Appeals found that the FTC's authority over unfair trade practices does indeed extend to cybersecurity.

But in November 2015, an administrative law judge dismissed the FTC's complaint against LabMD, ruling that the FTC failed to present adequate proof that LabMD's cybersecurity practices were likely to result in harm to consumers. The judge found, in the absence of actual injury to consumers, that the FTC had to prove more than a mere possibility of harm; rather, the FTC had to present specific proof about the level of risk or the probability that a data breach would occur. While these court decisions help confirm the FTC's enforcement authority, they also demonstrate the uphill battle the FTC faces if there is no evidence of actual harm to consumers.



EU Creates Unified Data Protection Regulations

The European Commission has revealed a draft of its General Data Protection Regulation (GDPR), expected to be approved by the EU Parliament this spring. The aim of the GDPR is to harmonize the current data protection laws in place across EU member states that regulate processing of personal data and the transfer of data to countries outside of the EU.

The fact that it is a "regulation" instead of a "directive" means it will be directly applicable to all EU member states without a need for national implementing legislation.

While most of the GDPR's provisions merely reinforce what is already included in the Directive, the GDPR provides for significantly greater penalties for failure to comply with the Regulation, up to four percent of a company's global annual revenue. Additionally, the GDPR is slated to apply to all companies that collect data on EU data subjects, rather than requiring the data controller to be established in the EU. If passed, the Regulation will not be in effect for at least two years.

Amendments to Federal Rules of Civil Procedure

The 2015 amendments to the Federal Rules of Civil Procedure became effective on 12/1/15, after five years of intense study, debate and drafting to address the most serious impediments to just, speedy and efficient resolution of civil disputes.

In his 2015 Year-End Report on the Federal Judiciary, U.S. Supreme Court Chief Justice John Roberts explained that "the amendments may not look like a big deal at first glance, but they are."

To watch a video on how these amendments will likely play out in a litigation scenario from the perspectives of a plaintiff, a defendant and from the bench, go to wnj.com/frcp-video.

Litigator's Ethical Obligation with Respect to eDiscovery

The State Bar of California Standing Committee on Professional Responsibility and Conduct issued Formal Opinion No. 2015-193 on an attorney's ethical duties in the handling of electronically stored information. The Committee explained that because electronic document creation and electronic communications have become commonplace in modern life, and discovery of electronically stored information (ESI) is now a frequent part of almost any litigated matter, litigation attorneys may not ignore the requirements and obligations of eDiscovery. The Committee noted that a lack of technological knowledge in handling eDiscovery may render an attorney ethically incompetent to handle certain cases, even where the attorney may otherwise be highly experienced. Several courts have subsequently cited to this Opinion in sanctioning attorneys for their eDiscovery missteps.

Identifying Data Preservation Triggering Events

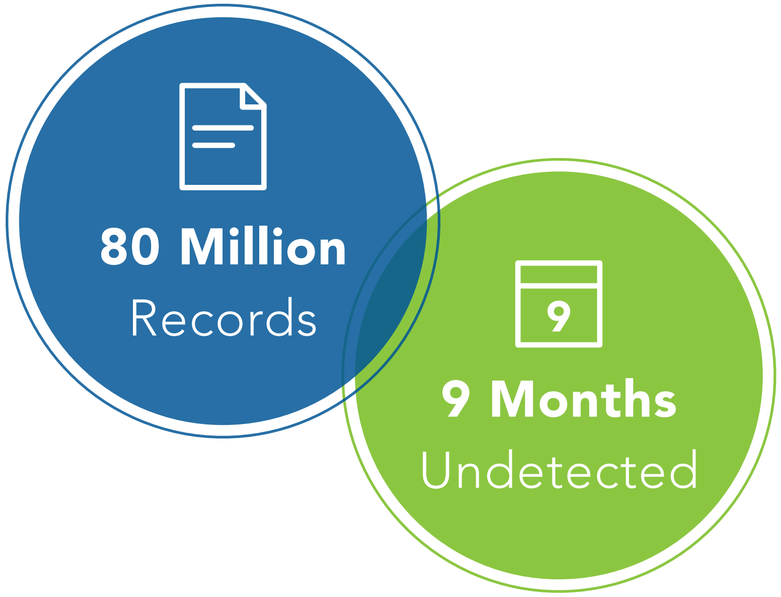
Clear-View Technologies, Inc. v. Rasnick, 2015 WL 2251005 (N.D. Cal. 2015) further proves that one's duty to preserve data almost always occurs before the lawsuit is filed.

The court explained that the duty to preserve evidence begins when litigation is "reasonably foreseeable."

This is an objective standard, asking not whether the party in fact reasonably foresaw litigation, but whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation. Based upon that standard, the court found that a text message threatening a lawsuit clearly triggered the duty to preserve, despite the fact that the lawsuit was not filed for two years thereafter. Defendant received an adverse jury instruction and $212,320 in penalties for failing to preserve data on a timely basis.

Top Ten
Data Breaches of 2015

1 Anthem Blue Cross



- Data compromised: as many as 80 million current and former customer records
- Customer database was breached by possibly hijacking legitimate websites to push malware to its users, yielding a compromised administrator password
- Stolen data included names, addresses, dates of birth, Social Security numbers and employment histories
- Breach went undetected for nine months
- This breach resulted in the largest number of records compromised in a health care network and bore the fingerprints of Deep Panda, a group known for breaking into technology, aerospace and energy firms, as well as another health insurer, Premera
- A class action lawsuit was filed against Anthem following the breach, but has not yet been resolved

2 Ashley Madison

- Data compromised: 37 million customer records including millions of account passwords
- Attackers posted personal information of customers seeking extramarital affairs with other married persons, which led to embarrassment, and in two cases, possible suicides
- This was arguably the most publicized hack of the year
- More than a dozen lawsuits were filed following this data breach; one suit seeks $578 million in damages

3 Office of Personnel Management

- Data compromised: personnel records on 22 million current and former federal employees
- The hackers breached the system by using a contractor's stolen credentials to plant a malware backdoor in the network
- The breach went undetected for 343 days, almost a full year
- This breach appeared to be a data mining operation—seeking data on individuals for intelligence purposes—as opposed to data to be exploited for cash
- The stolen personnel records included those for workers with classified employees holding sensitive jobs in law enforcement and intelligence, and also included their fingerprints
- Several lawsuits were filed following this breach—one class action suit was filed on behalf of 21 million federal employees whose personal information was exposed

4 Experian/T-Mobile

- Data compromised: 15 million personal records, including names, addresses, dates of birth and encrypted Social Security numbers and other ID numbers
- Breach went undetected for 15 days
- The unauthorized access was in an isolated incident over a limited period of time. It included access to a server that contained personal information for consumers who applied for T-Mobile USA postpaid services or products that required a credit check from Sept. 1, 2013, through September 16, 2015
- An undisclosed number of class action lawsuits were filed against Experian as a result of this breach and Experian reported that costs incurred by responding to the breach amounted to over $20 million

5 Premera Blue Cross

- Data compromised: names, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical claims information and financial information for 11 million customers
- It is believed that this breach occurred by using phishing to lure employees to typo domain sites that downloaded malware
- Breach went undetected for almost a year—from May 5, 2014, to January 29, 2015
- This was the largest breach of medical records, and the methods used in the attack are similar to those used against Anthem and likely used by the same attack group. Both attacks were discovered the same day

6 LastPass

- Data compromised: 7 million users
- This cyberattack compromised email addresses, password reminders, server per user salts and authentication hashes
- This was a relevant and important hack because of the nature of the service—a password management service like LastPass is probably the last account you would want to be hacked

7 VTech

- Data compromised: personal information of 6.4 million children
- This marked the first breach to directly affect children

- In November 2015, an unauthorized party obtained customer data from the Learning Lodge app store and Kid Connect servers, exposing the data of more than 6 million children and nearly 5 million parent accounts
- As part of the hack, the company's Learning Lodge app store and Kid Connect messaging system were breached. According to VTech, information about children's names, gender and birth dates were accessed

- Data was also stolen about many of the children's parents, including names, mailing addresses, encrypted passwords and secret questions and answers for password retrieval

8 CareFirst Blue Cross Blue Shield

- Data compromised: 1.1 million records
- Names, birth dates, email addresses and subscriber information compromised, but member password encryption prevented cybercriminals from gaining access to Social Security numbers, medical claims, employment, credit card and financial data
- CareFirst discovered the breach as part of a Mandiant-led security review that found hackers had gained access to a database that members use to get access to the company's website and services

9 Hacking Team

- Data compromised: 1 million emails
- The Hacking Team develops spy tools for government agencies, including those that can go around traditional anti-virus solutions

Spy tools were used to expose 1 million emails

- This breach published more than 1 million emails from the Italian surveillance company, revealing its involvement with oppressive governments, as well as multiple Flash zero-day vulnerabilities and Adobe exploits
- A full list of Hacking Team's customers

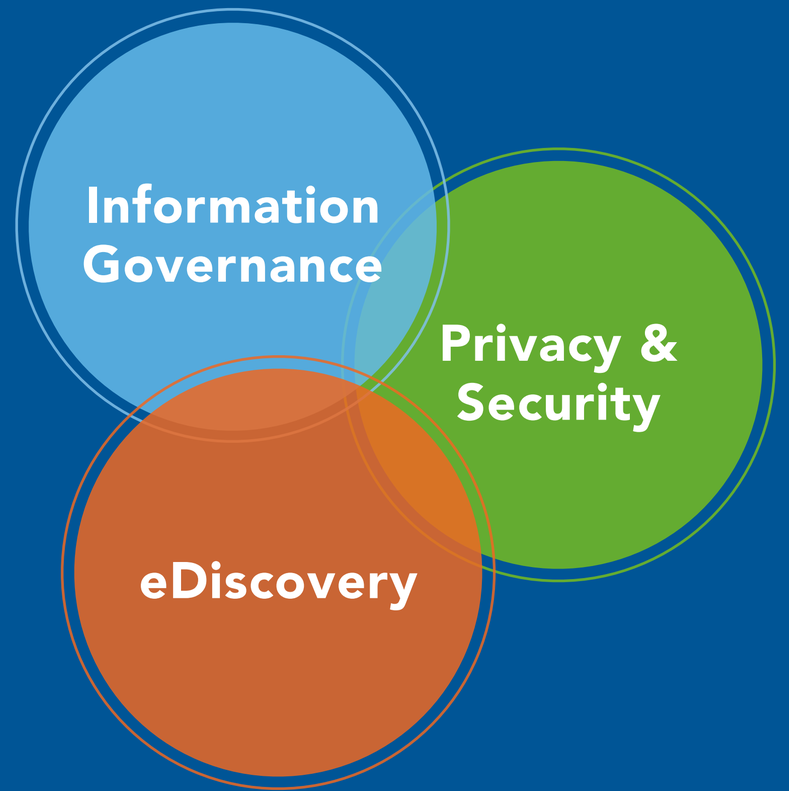
was leaked in the 2015 breach that included mostly military, police, federal and provincial governments

10 IRS

- Data compromised: tax records for 330,000 taxpayers used to collect bogus refunds
- This breach occurred through stolen credentials and knowledge-based authentication information obtained through the IRS filing and refund systems
- Attackers were discovered because they sent so many requests for old tax returns that the IRS IT team thought it was a DDoS attack and investigated
- The thieves collected tens of millions of dollars in fraudulent refunds, as well as all the data included on the tax forms they scammed from the IRS

About

By providing discerning and proactive legal advice, Warner Norcross & Judd LLP builds a better partnership with its clients. Warner Norcross provides full life-cycle support for business data, from data creation to disposition and everything in between, including eDiscovery and data privacy solutions. As a premiere corporate law firm, Warner Norcross attorneys have the business acumen and legal expertise to confront any issue throughout an organization's data life-cycle and provide legally defensible counsel. Warner Norcross is a corporate law firm with 230 attorneys practicing in eight offices. For more information on policies, best practices and litigation, contact the Data Solutions co-chairs: B. Jay Yelton III (jyelton@wnj.com or 269-276-8130) or Dawn Garcia Ward (dward@wnj.com or 616-396-3039).



Warner Norcross&Judd® LLP
ATTORNEYS AT LAW

A BETTER PARTNERSHIP®

By providing discerning and proactive legal advice, we build a better partnership with clients.

Thank you!
Please visit WNJ.com.