



A Retrospective of eDiscovery,  
Information Governance and  
Data Security in 2016

# Welcome,

Warner Norcross & Judd is pleased to share this overview of legal changes, trends and case studies in the 2016 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 Carvo*

**Scott R. Carvo**

*Partner at Warner Norcross & Judd LLP*



*B. Jay Yelton III*

**B. Jay Yelton III**

*Partner at Warner Norcross & Judd LLP*

# Biggest Developments in 2016

## Beware of Boilerplate Objections

The December 1, 2015, amendments to the Federal Rules of Civil Procedure have made it clear that boilerplate objections to Rule 34 document requests are no longer acceptable.

**Case law following the rule amendments shows that courts are quick to reject boilerplate objections and criticize parties using stock, general objections: that the request is overbroad, unduly burdensome and not relevant.**

(See, e.g., *Moser v. Holland*, 2016 WL 426670, at \*1,3 (E.D. Cal. Feb. 3, 2016). Due to defendants' failure to comply with the specificity requirements, the court granted plaintiff's motion to compel, ordered defendants to produce the responsive documents and awarded plaintiff costs as a sanction for having to file the motion.) Litigators should stop using their stock general objections when responding to discovery. Based on the amendments to Rule 34 and the case law interpreting such amendments, specificity is vital to making proportionality and other objections that will limit unnecessary or expensive discovery.

## EU-U.S. Privacy Shield Framework Approved by European Commission

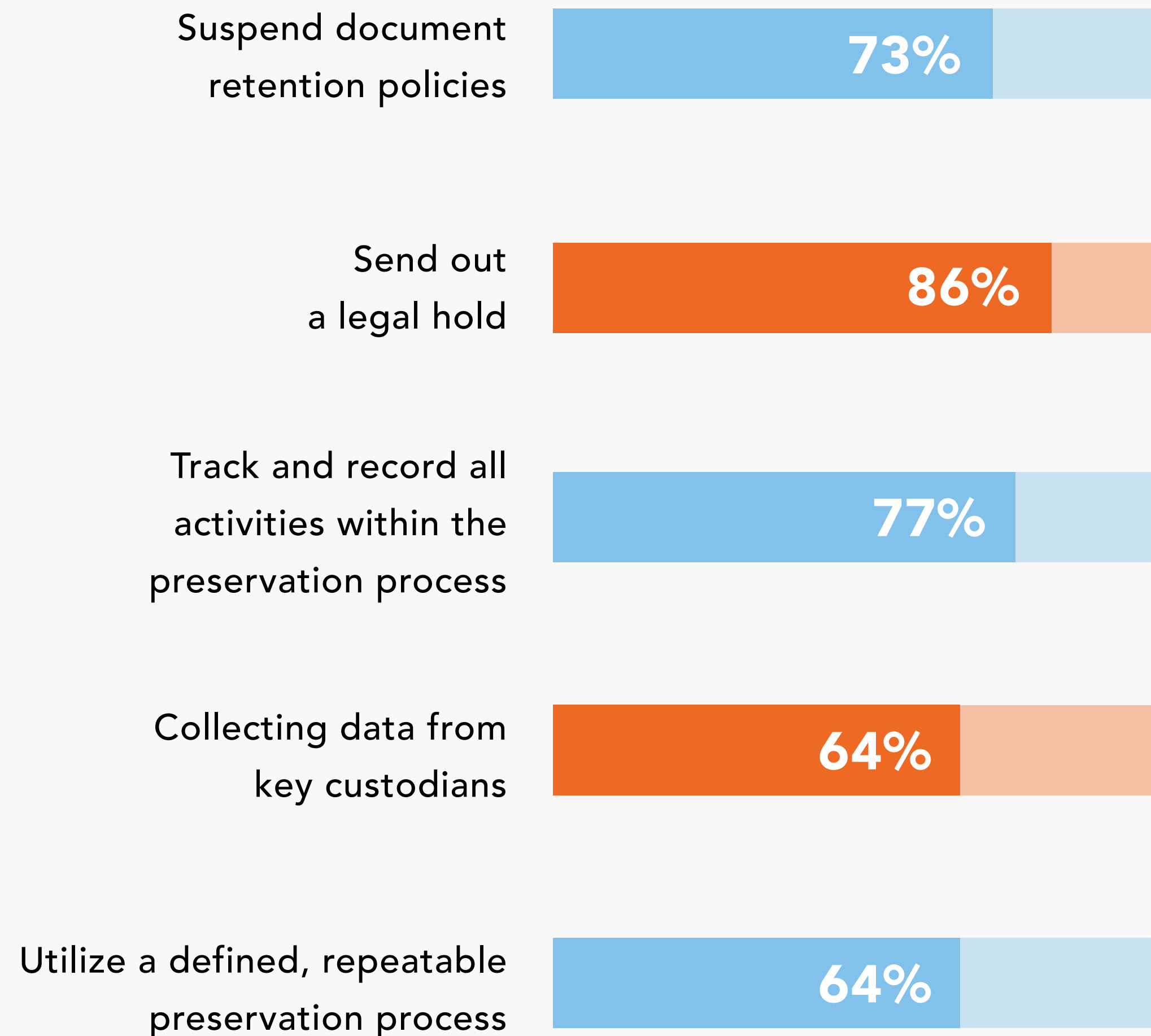
On August 1, 2016, the European Union (EU) — United States (U.S.) Privacy Shield officially went into effect and U.S. companies began certifying to the Privacy Shield. Replacing the invalidated Safe Harbor framework, the Privacy Shield became the latest approved transfer mechanism for companies transferring personal data from the EU to the U.S. Eligible U.S. organizations joining the Privacy Shield must go through a self-certification process and comply with the requirements of the Privacy Shield Principles, which govern the use and treatment of personal data received from the EU under the framework, as well as the access and recourse mechanisms that participants must provide to EU data subjects.



**1,300 organizations  
certified to Privacy Shield**

And, over 1,300 organizations have already certified to the Privacy Shield. Yet, despite its early popularity, recent legal challenges involving the Privacy Shield by privacy advocates in the EU have left organizations concerned about the Privacy Shield's long-term viability.

## WHAT SHOULD A PARTY DO TO DEMONSTRATE "REASONABLE STEPS TO PRESERVE?"



Exterro's 3<sup>rd</sup> Annual Federal Judges Survey: eDiscovery Advice for Becoming a Better Attorney (2017), <http://www.exterro.com/judges-survey-17/>

## Very Risky to Over Rely on Employee Compliance with Data Preservation Obligations

In *GN Netcom, Inc. v. Plantronics, Inc.*, 2016 U.S. Dist. LEXIS 93299 (D. Del. July 12, 2016), an antitrust case, the court ordered \$3,000,000 in sanctions against Plantronics for the deletion of emails subject to a litigation hold by a rogue employee. In this case, Plantronics had implemented a litigation hold, updated the hold and conducted employee training on hold compliance. However, hold compliance was inadequately supervised, and the company did not take steps to preserve data and prevent document deletion. While under litigation hold, a senior vice president and member of the company's executive committee deleted thousands of potentially relevant emails and instructed others to do the same. In its analysis under FRCP 37(e), the court found all conditions satisfied for levying sanctions. Significantly, the court held that because the actions of the employee were intended to protect the company, those actions undertaken in bad faith could be attributed to Plantronics. Similarly, recent allegations of data spoliation against Volkswagen's in-house counsel during the emissions defeat device scandal illustrate the need for vigilant supervision of data preservation efforts under litigation holds. Volkswagen's in-house counsel was indicted on obstruction of justice charges for allegedly encouraging data deletion and delaying the distribution of a litigation hold. Although these companies made efforts to notify their employees of pending litigation and attendant data preservation obligations, they relied too heavily on individual employee compliance. It is increasingly necessary for companies to develop and track data preservation processes that are adequately supervised and do not rely heavily on employee preservation efforts.

## The Rise of DDoS Attacks in the Internet of Things Devices

Although Distributed Denial of Service (DDoS) attacks have been around since the 1990s, these attacks have reached a massive scale in recent years due to the sharp rise of Internet of Things (IoT) devices. 2015 and 2016 both saw record numbers of such IoT-based attacks. Much of the increase can be attributed to poor security on these internet-connected devices, which makes them easy targets for malware, particularly botnets. In fact, hackers are now so highly aware of lax IoT security that many preprogram their malware with commonly used and default passwords.

**While not frequently seen in the past, attacks originating from multiple IoT platforms simultaneously are increasingly common.**

For example, last fall, the largest attack to date brought down many popular internet sites in the U.S. and Europe as a result of a DDoS attack that overloaded servers at domain name system provider Dyn. It was later discovered that the attack originated from Mirai-based botnets, which targeted IoT devices such as digital cameras and DVR players. With the rapid growth of the IoT, it is estimated that DDoS attacks will only continue to increase unless more stringent security measures are adopted.

## Use of Technology-Assisted Review Isn't Required in the United States; at Least Not Yet

Although *Hyles v. New York City*, 2016 WL 4077114 (S.D.N.Y. Aug. 1, 2016) did not create new law; it clarified existing law on technology assisted review. In *Hyles*, the plaintiff wanted to require the defendant (City, i.e., the responding party) to use TAR (technology assisted review, a.k.a. predictive coding), instead of the keyword search method the City preferred.

**As expected, the judge ruled that a party cannot be forced to use predictive coding, even if it is a superior method than what the party wants to use; and, even if the party has not begun using its preferred method.**

However, in *McConnell Dowell Constructors v. Santam*, 2016 VSC 734 (Dec. 2, 2016), an Australian court came to an alternative conclusion in a case involving 1,400,000 documents. When the parties could not agree on a review method, the judge approved TAR as an effective method of document review. The judge held that the court may order discovery by TAR, whether or not both parties consent, where the volume of electronically stored information (ESI) is substantial and the costs of review may not be reasonable and proportionate.

## Hackers Infiltrate the Democratic National Committee's Computer System

During the course of the presidential campaign, the Democratic National Committee's computer system was hacked. The FBI discovered the hack in September of 2015, but when the FBI contacted the DNC to alert it to the problem, the DNC's tech-support contractor didn't seriously investigate the warning as it wasn't sure if the call from the FBI was legitimate or from an imposter. This gave hackers months of unfettered access to the DNC's computer systems, leading to embarrassing revelations during the late months of the campaign.



## Identify and Resolve eDiscovery Issues Early in the Case

According to a recent survey, 95% of federal judges identified "applying principles of cooperation and proportionality at Rule 26(f) conferences" as the area offering the greatest potential for eDiscovery improvement (i.e. reducing costs and risks).

**Serving an immediate Rule 34 request for production of documents is one of the most effective yet least utilized tools for applying principles of cooperation and proportionality at your next Rule 26(c) conference.**

The December 1, 2015, amendment to Federal Rule of Civil Procedure 34 empowers a party to send their initial document requests to the opposing party before the Rule 26(f) conference, which allows the attorneys to leverage their first meet and confer meeting to discuss and identify mutually agreeable eDiscovery terms. If parties take advantage of this, it will get you to the facts of the case sooner and less expensively.

## New Scope of Discovery Under Rule 26(b)(1) Can Reduce Costs

The December 1, 2015, amendments to the Federal Rules of Civil Procedure changed the scope of discovery under Rule 26(b)(1). The test going forward is whether evidence is “relevant to any party’s claim or defense,” not whether it is “reasonably calculated to lead to admissible evidence.” The 2015 amendments also added proportionality as a requirement for permissible discovery.

**Relevancy alone is no longer sufficient — discovery must also be proportional to the needs of the case.**

As the court pointed out in *In re Bard IVC Filters Prods. Liab. Litig.*, 2016 LEXIS 126448 (D. Ariz. Sept. 16, 2016), “the 2015 amendments effectively abrogated cases applying a prior version of Rule 26(b)(1).” So when faced with a motion to compel, remember that the other side may be citing cases that are no longer valid since the rule change. See, e.g., *Fulton v. Livingston Fin. LLC*, 2016 WL 3976558 (W.D. Wash. July 25, 2016) (sanctions imposed for counsel’s misrepresentations of law, including citation to case law analyzing outdated standards under Rule 26(b)(1)).

## WHEN MAKING PROPORTIONALITY ARGUMENTS, WHAT COULD PARTIES DO BETTER?

Use metrics to support  
their arguments

55%

Don’t rely solely on costs  
when making this claim

41%

Try to work more with  
opposing counsel before  
bringing a claim

68%

Suggest alternative  
remedies to court

68%

Exterro’s 3<sup>rd</sup> Annual Federal Judges Survey: eDiscovery Advice for Becoming a Better Attorney (2017), <http://www.exterro.com/judges-survey-17/>





## Government Seeks Back Door into Personal Device

In December 2015, Syed Rizwan Farook and his wife engaged in a mass shooting in San Bernardino, CA. During its investigation, the FBI found Farook's Apple iPhone, but was unable to access the content on the phone.

**After Apple refused to help it unlock the phone, the FBI obtained an order from a federal magistrate judge requiring Apple to unlock the phone.**

Apple opposed the order and it looked like the legal showdown would end up before the U.S. Supreme Court; but the FBI then withdrew its request as it managed to obtain access to the phone's content independently. The case, however, highlights important issues between the government's desire to investigate crimes and the business community's desire to protect the data of their customers.

# Top Ten Data Breaches of 2016

## 1 Yahoo

---

- Data compromised: more than 1 billion user accounts, though initially reported as 500MM
- Current investigation results indicate that the hack was the result of a foreign government.
- Compromised data includes names, e-mail addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers.
- Verizon knocked \$350 million off its offer for Yahoo, bringing the deal down to \$4.48 billion.

## 2 FriendFinder

---

- Data compromised: 412 million users' information
- Compromised data included usernames, passwords, and email addresses. The data includes more than 339 million accounts on AdultFriendFinder.com as well as tens of millions accounts from Penthouse.com and Stripshow.com. Some passwords were cryptographically hashed to protect them, others were unencrypted.

- This hack is nearly 13 times larger than the Ashley Madison breach.

## 3 MySpace

---

- Data compromised: more than 360 million usernames and passwords
- This is the second largest data breach involving a single source (behind Yahoo).
- Information was stored using unsalted SHA-1 hashes, allowing hackers to easily crack the information.
- "Peace," the same organization implicated in hacks of Tumblr and LinkedIn, is assumed responsible for the hack.
- The breach only affected accounts created prior to June of 2013, when MySpace increased its security.

## 4 Unknown Source

---

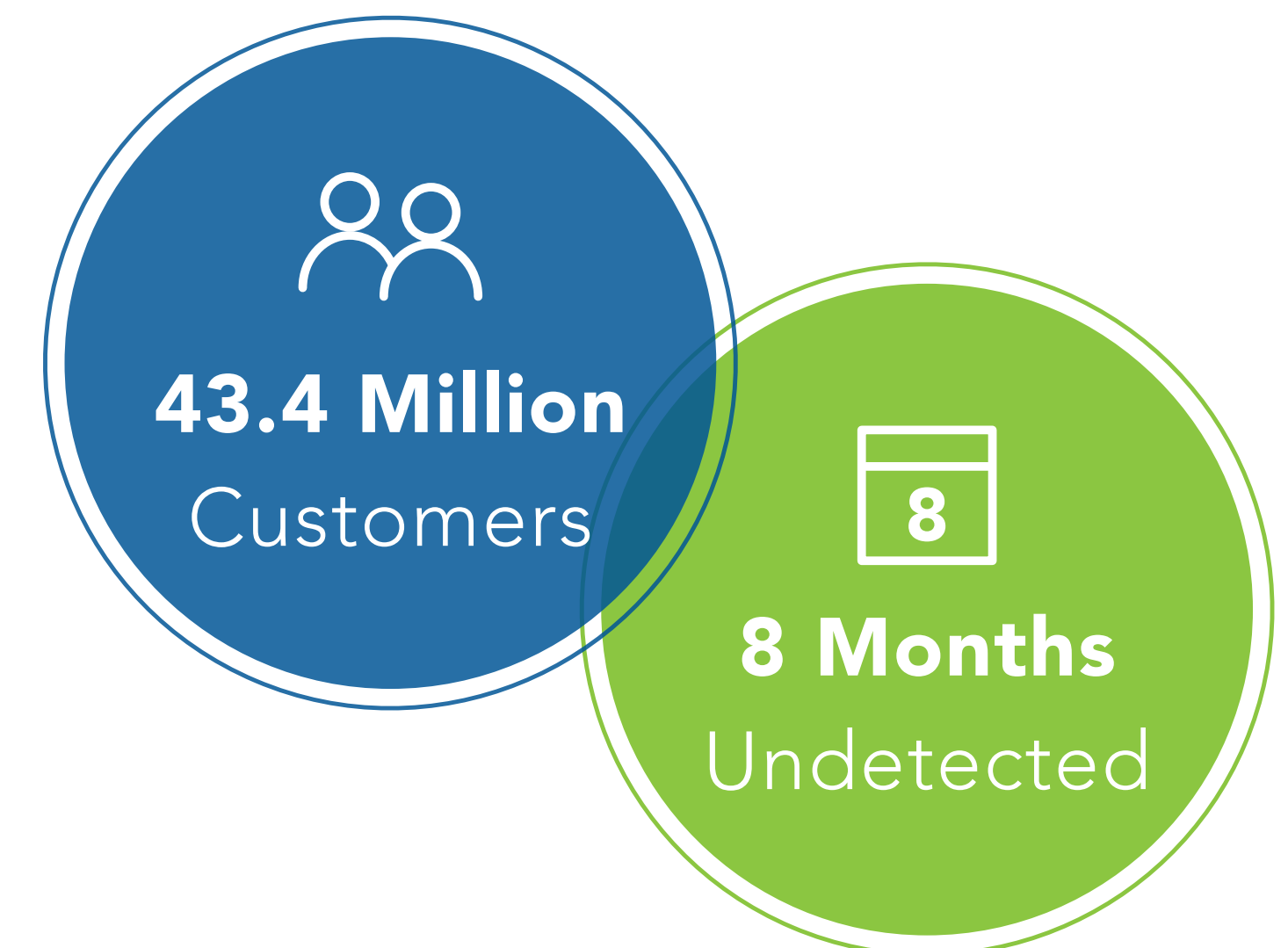
- Data compromised: 191 million voter records
- The information contains voters' names, home addresses, voter IDs, phone numbers and dates of birth, as well as political affiliations and a detailed voting history since 2000.

- The breach was the result of an improperly configured database discovered by a whitehat hacker.

## 5 Weebly

---


- Data compromised: information from more than 43.4 million customers, including email addresses, usernames, IP addresses and passwords
- The root cause of the breach is still unknown.
- The breach went undetected for eight months.
- All passwords were encrypted (bcrypt hashed), which prevented hackers from targeting customer websites hosted on the Weebly platform.



## 6 Twitter

---

- Data compromised: more than 32 million users
- Passwords were stolen from users and not through an internal system.
- According to LeakedSource, user credentials were being traded on the Dark Web for about 10 bitcoin or a little under \$6,000.
- Twitter remains adamant that its systems were not breached.

 User credentials were being traded for a little under \$6,000

## 7 Foursquare

---

- Data compromised: more than 22.5 million customer accounts, including email addresses, usernames, and Twitter and Facebook IDs
- Reported by LeakedSource, which claims to have received the account information allegedly stolen from Foursquare in December 2013.

- After conducting an internal investigation, Foursquare denied that it was hacked, claiming that the email addresses were simply cross-referenced with publicly available data from Foursquare.

## 8 U.S. Department of Health and Human Services

---

- Data compromised: nearly 5 million names and Social Security numbers
- Personal laptop and hard drives were stolen from a federal building in Washington State.
- Intruders used a copy of a building key kept by a former building employee who was fired for stealing.
- It was unclear whether information on the hard drives was encrypted.
- HHS officials waited almost two months to notify Congress.

## 9 21st Century Oncology

---

- Data compromised: 2.2 million patient records including patient names, Social Security numbers, diagnoses and treatments provided

- The breach involved patients in all 50 states and several foreign countries.
- Patients affected filed federal class-action lawsuits.
- This breach went undetected for more than five months.

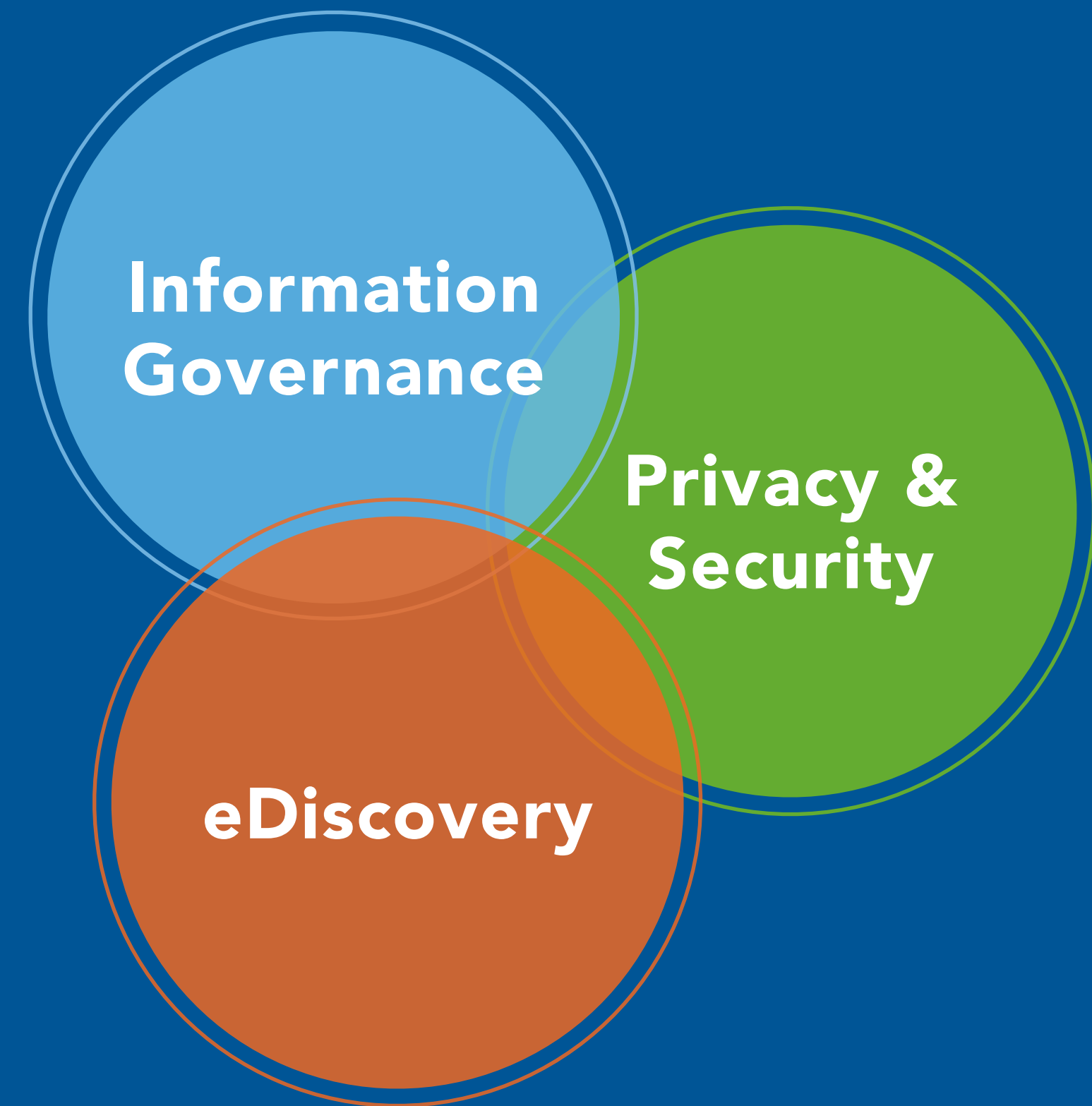
## 10 Washington Department of Fish and Wildlife

---

- Data compromised: 1.7 million people who bought Washington hunting and fishing licenses before mid-2006
- Customers' personal information included their names; addresses; birthdates; driver's license numbers (customers had the option of providing this information) and related details such as height, weight and eye/hair color; and the last four digits of Social Security numbers (the other five Social Security numbers were encrypted).
- Breach occurred with Washington State's vendor that manages the license system, a vendor Washington was trying to part ways with for several years.

# 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](mailto:jyelton@wnj.com) or 269-276-8130) or Scott R. Carvo ([scarvo@wnj.com](mailto:scarvo@wnj.com) or 616-752-2759).





**A BETTER PARTNERSHIP<sup>®</sup>**

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

Thank you!  
Please visit [WNJ.com](http://WNJ.com).