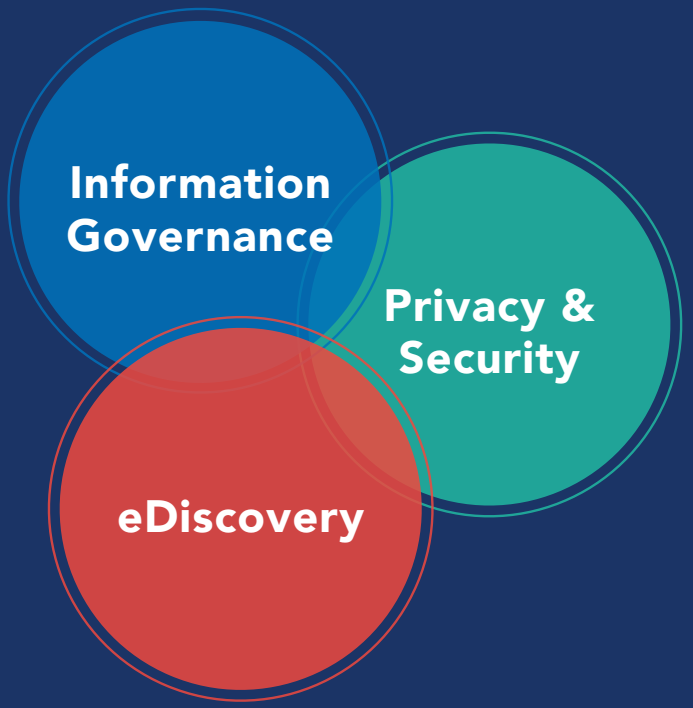
Warner Norcross + Judd

A Retrospective of eDiscovery, Information Governance and Data Security in 2017

3rd Annual Data Solutions Whitepaper



Welcome,

Warner Norcross + Judd is pleased to share this overview of legal changes, trends and case studies in the 2017 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

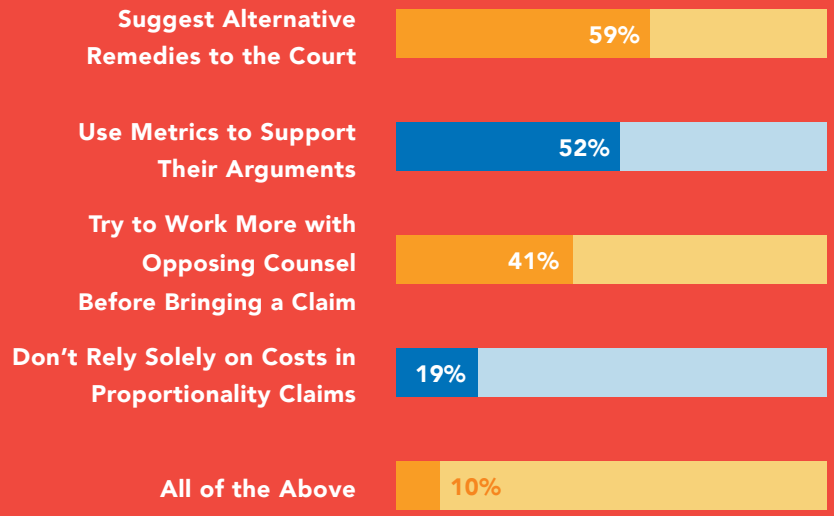
Biggest Developments
in 2017

Leveraging Proportionality is Essential

When asked to evaluate how attorneys were leveraging proportionality to improve eDiscovery outcomes, recently surveyed judges found that more parties were making proportionality claims, averaging a 3.9 on a scale of 1 (never) to 5 (a lot more).

1 Never **5** A Lot More

In addition, the judges identified substantial areas for improvement in attorneys' proportionality claims.

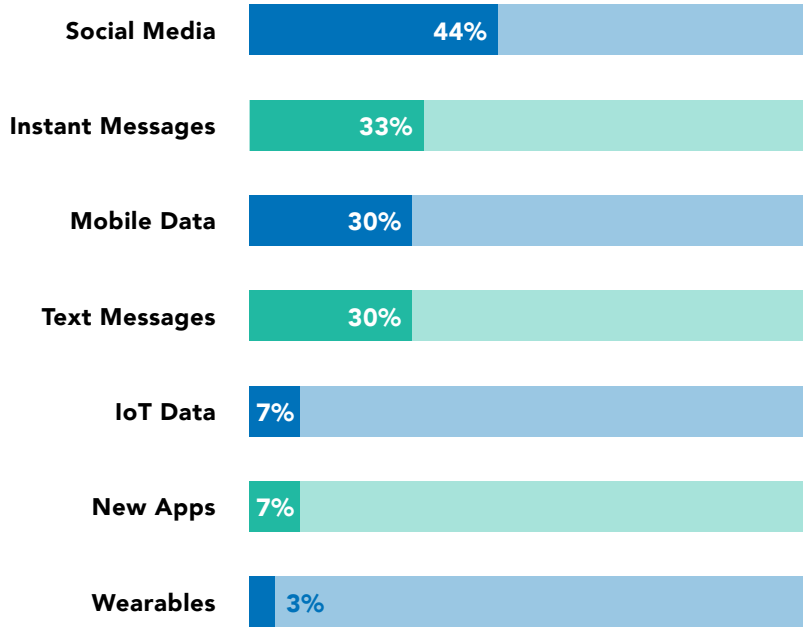


Note: Respondents could choose more than one response to this question.

**These statistics are from page 15 of the Exterro 4th Annual Federal Judges Survey*

Re-evaluating the Scope of Your Legal Hold

When asked how attorneys should improve their data preservation efforts, the recently surveyed judges encouraged attorneys to develop or modify legal hold processes for preserving new data types. They identified the following data types as being increasingly relevant evidence.



**These statistics are from page 19 of the Exterro 4th Annual Federal Judges Survey*

Boiler Plate Objections — More Risky Than Ever

At least one federal magistrate has had it with document request responses that fail to comply with Rule 34, as amended on December 1, 2015. Magistrate Judge Peck of the Southern District of New York released an opinion last year highlighting ongoing compliance problems with Rule 34. In *Fischer v. Forrest*, 2017 WL 773694 (S.D.N.Y. Feb. 28, 2017), he specifically called out attorneys for filing document request responses that:

Contain a list of General Objections incorporated into each response.

"...General Objections into each response violates Rule 34(b)(2)(B)'s specificity requirement as well as Rule 34(b)(2)(C)'s requirement to indicate whether any responsive materials are withheld on the basis of an objection. General objections should rarely be used after December 1, 2015, unless each such objection applies to each document request (e.g., objecting to produce privileged material)."

Contain an objection based on nonrelevance to "the subject matter of the litigation" or based on the discovery not being "likely to lead to the discovery of relevant, admissible evidence," as this language was deleted from Rule 26.

"Despite this clear change, many courts [and lawyers] continue to use the phrase. Old habits die hard.... 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.'"

Contain "meaningless" boilerplate objections, such as "overly broad and unduly burdensome."

"Why is it burdensome? How is it overly broad? This language tells the Court nothing. Indeed, even before the December 1, 2015 rules amendments, judicial decisions criticized such boilerplate objections."

Do not indicate when documents and ESI that defendants are producing will be produced.

"The response to the request must state that copies will be produced. The production must be completed either by the time for inspection specified in the request or by another reasonable time specifically identified in the response. When it is necessary to make the production in stages the response should specify the beginning and end dates of the production."

The judge encouraged lawyers to update their form files and provided this incentive.

From now on in cases before this Court, any discovery response that does not comply with Rule 34's requirement to state objections with specificity (and to clearly indicate whether responsive material is being withheld on the basis of objection) will be deemed a waiver of all objections (except as to privilege).

So, if you haven't checked your form files since December 2015... you might want to take some time to do so. Other courts are sure to follow suit as December 2015 fades further into the rearview mirror.

State Court Discovery Rule Amendments are Forthcoming

In September 2016, the State Bar of Michigan appointed a Special Committee to evaluate whether and how our civil discovery rules should be modified. This is the first time in 30 years that there has been a comprehensive review and modification of our state's discovery rules. As explained by the SBM President:

"In a rapidly changing world, it is vital that these rules be updated to reflect new realities brought about by changes in technology while ensuring that our courts are accessible and the discovery process is fair to all."

In early 2017 the Special Committee created several sub-committees, which reviewed the rules concerning all aspects of discovery, including: e-discovery; expert witnesses; the scope and course of discovery; case management; the impact of court rule changes on discovery practices in the district, probate and family courts; and the prospect of differentiated case management. Based on the work of those subcommittees, in the fall of 2017 the Special Committee published proposed rule changes and sought input from a broad array of state bar sections, local and affiliate bar associations, and other key stakeholders. Based on the comments received, the Special Committee is now preparing an updated set of proposed rule amendments in hopes to present them to the Representative Assembly this spring and then to the Michigan Supreme Court.

Unfamiliarity with Tech Results in Waiver of Privilege

In 2012, the ABA issued revised Comment 8 to Model Rule of Professional Conduct 1.1. The comment provides that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...." At least 27 states have since adopted an ethical duty of technology competence. In all likelihood, those state bars that haven't done so yet eventually will follow suit. Given the increased emphasis on technology competency, courts will be less likely to give counsel and clients a pass for poor technology choices or uses, as illustrated below.

27 STATES ADOPTED
TECHNOLOGY ETHICS

In *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, 2017 WL 1041600 (W.D.Va. Feb. 2, 2017), a dispute arose over plaintiff's obligation to cover defendant's fire loss claim. Plaintiff's senior investigator uploaded video footage of the fire loss scene for a third party, the National Insurance Crime Bureau (NICB). The footage was uploaded to a web-based file sharing site. The NICB received a link that would allow anyone using it to access the footage. The video files were not password protected and the link had no expiration date.

Later, the senior investigator uploaded the plaintiff's entire claims and investigative files to the same site, accessible by using the same link sent to the NICB. The NICB provided the link to defense counsel in response to a subpoena for all records it held related to defendant's claim. Defense counsel used the link to download the claims and investigative files and reviewed them.

When plaintiff's counsel learned what happened, it moved to disqualify defense counsel, claiming the files were protected by attorney-client and work-product privilege. The court denied plaintiff's motion finding that plaintiff had waived any privilege protection the files may have had by placing them on the file-sharing site without reasonable protection.

> ***The court believes that its decision on this issue fosters the better public policy. The technology involved in information-sharing is rapidly evolving. Whether a company chooses to use a new technology is a decision within that company's control. If it chooses to use a new technology, however, it should be responsible for ensuring that its employees and agents understand how the technology works, and, more importantly, whether the technology allows unwanted access by others to its confidential information.***

Plaintiff objected to the magistrate's ruling. The district court overturned the magistrate's decision, finding that the disclosure was inadvertent and that, upon learning of the disclosure, plaintiff had acted in a timely manner to rectify the error. *Harleysville Ins. Co. v Holding Funeral Home, Inc.*, 2017 WL 4368617 (W.D.Va. Oct. 2, 2017).

Despite the district court's reversal, this opinion reflects the increased responsibility lawyers have when it comes to using technology in practice. Before you rely on technology, be sure you understand it...or associate with someone who does. Don't let a bad technology choice cost you a case...or a client.

**These statistics are from page 10 of the Exterro 4th Annual Federal Judges Survey*

New Amendments to Federal Rule of Evidence 902 Streamline Admission of Electronic Evidence

Federal Rule of Evidence (FRE) 902 stipulates that certain types of documents are self-authenticating and require no extrinsic evidence of authenticity to be admissible at trial. Among these categories of documents are government documents, certified copies of public records, newspapers and certified business records. Amendments to FRE 902, which went into effect December 1, 2017, aim at reducing the necessity of live testimony from multiple witnesses at trial for the sole purpose of authenticating electronic evidence.

The new Rule 902(13) covers records "generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of [FRE] 902(11) or (12)."

In addition, the new Rule 902(14) covers records "copied from an electronic device, storage medium or file" (including email and other user-created records), if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of [FRE] 902(11) or (12)."

In most cases, a party will simply submit an affidavit of a "qualified person" who certifies that the electronic document or record was obtained in conformity with FRE 902(11) and (12). For more complex cases, you should consult with Hon. Paul W. Grimm, et. al., "Best Practices for Authenticating Digital Evidence," (West Pub. 2016).

These amendments increase the importance of using knowledgeable eDiscovery practitioners to help ensure that best practices are followed in the collection and duplication of electronic data. Lawyers can facilitate the future authentication of electronic evidence by following forensic collection procedures. This can significantly reduce the likelihood, or at least the effectiveness, of costly challenges to electronic evidence or the need to have extra authentication witnesses present at evidentiary hearings or trials.

Top Cybersecurity and Privacy Stories of 2017

1. Will the Equifax breach lead to new legislation?

After a delay of many months, Equifax reported that it suffered a data breach that compromised data of over 143 million Americans. The fact that Americans have no ability to opt out of Equifax's data collection and processing activities makes this all the worse and may lead Congress to enact a federal law on data security and breach notification. Given the magnitude of this breach, it also raises the question of whether we can ever again rely on a Social Security number (SSn) as an individual identifier.

2. Ransomware attacks keep coming.

The rate of ransomware incidents continues to grow, and 2017 saw two of the biggest ransomware attacks with the WannaCry and Not Petya attacks. These attacks used a Microsoft Windows exploit that was stolen from the CIA. WannaCry, in particular, struck many hospitals hard, demonstrating how difficult it is to know what software any particular piece of technology is running and keeping that software patched.

3. Can we secure the Internet of Things (IoT)?

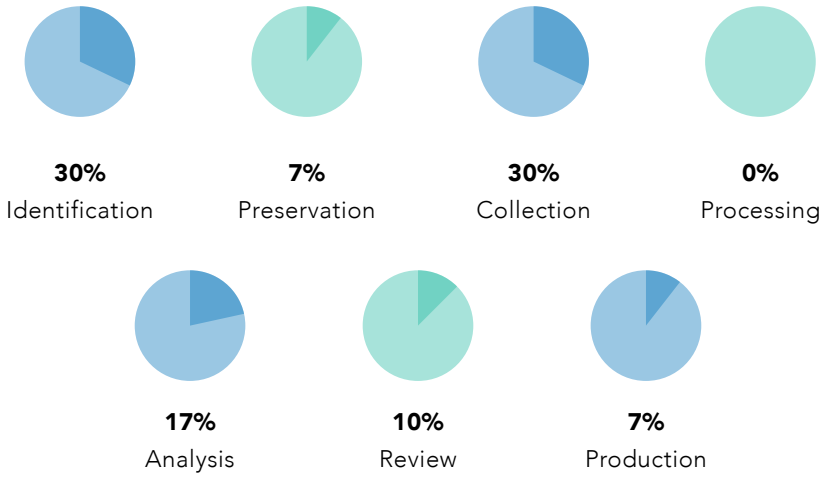
Stories continue to emerge about how easy it is for "smart" devices to be hacked. Implantable cardiac devices such as pacemakers and defibrillators turned out to be vulnerable to hackers, and older Amazon Echo devices could be turned into eavesdropping devices. As more vulnerabilities come to light, will consumers be willing to buy Internet of Things (IoT) products?

4. European Union (EU) GDPR compliance deadline looming.

Many U.S. companies have struggled to understand whether the EU's General Data Protection Regulations apply to them, and if so, how to comply. Many of the regulations are vague, and guidance from the EU continues to evolve. But the regulations purport to apply to data collected from individuals in the EU wherever in the world that data is stored or used, and with penalties of up to the greater of 20 million euros or 4% of global revenue, the potential costs of noncompliance are steep.

eDiscovery Mistakes in 2017

Not surprisingly, eDiscovery mistakes continued to occur throughout 2017. According to a recent survey of federal judges, mistakes continue to occur at almost every stage of the discovery process.



In fact, 73% of the judges surveyed recommend that legal professionals should take eDiscovery Continuing Legal Education (CLE) credits, seminars and/or courses to increase their knowledge and skills in this area. Here is a list of some of the most notable eDiscovery mistakes that occurred last year:

Reliance on Unfamiliar eDiscovery Technology: *The New York Times*, page B2 (7/22/17)

- In response to a third-party subpoena, a partner from a New York law firm was retained to review and produce responsive, non-privileged Wells Fargo bank data.
- Based on a misunderstanding with the eDiscovery vendor who was hosting the collected data, the partner believed she had reviewed the entire set of documents collected, when in fact she had only reviewed a subset.
- When the partner approved the vendor's production of the entire data collection, it resulted in the inadvertent production of Wells Fargo customer information, including personally identifiable information about approximately 50,000 of the bank's wealthiest customers and their assets, which opposing counsel revealed to *The New York Times*.
- This error was particularly problematic because the partner failed to require a confidentiality and/or clawback agreement prior to production.
- The production seemingly violated various privacy protection laws, Financial Regulatory Authority Inc. guidance and U.S. Securities and Exchange Commission regulations.

**These statistics are from page 10 of the Exterro 4th Annual Federal Judges Survey*

Narrowly Drafted Clawback Agreement Fails to Protect Against Waiver of Inadvertently Disclosed Privileged Documents: *Irth Solutions, LLC v. Windstream Communications, LLC*, 2017, WL 3276021 (S.D. Ohio Aug. 2, 2017)

- FRE 502, promulgated in 2008, provides a uniform standard for analyzing "inadvertent disclosures." More importantly, Rule 502(d) allows a court in a federal proceeding to enter an order declaring that the disclosure of privilege material, unless intentional, will not operate as a waiver in the current proceeding or in any subsequent state or federal proceeding. These orders can significantly reduce the time and expense of privilege review of discovery documents, and reduce the risk of waiver from disclosure during discovery.
- Nevertheless, the parties in *Irth Solutions* decided that the scale of the case did not require a formal court order under FRE 502(d). Instead, the parties agreed that if a privileged document was disclosed inadvertently, the disclosure would not waive privilege.
- After making an initial production of 2,200 pages of documents, defendant contacted plaintiff and requested a clawback of 43 privileged documents. Plaintiff argued that the clawback agreement did not apply because the disclosure of the 43 documents resulted from more than mere inadvertence. As support, plaintiff pointed to the fact that attorney names and positions were prominently displayed on several of the 43 documents.
- The court agreed with plaintiff and found the disclosures to be "completely reckless." As consequence, the Court held that the "defendant's conduct waived the privilege." A properly drafted Rule 502(d) Order would have protected the disclosure of these documents from operating as a waiver, whereas the parties' narrowly drafted clawback agreement did not.

Inadequate Steps to Preserve Data Supporting Denial in Answer: *Moody v. CSX Transp., Inc.*, 2017 WL 4173358 (W.D. N.Y. Sept. 21, 2017)

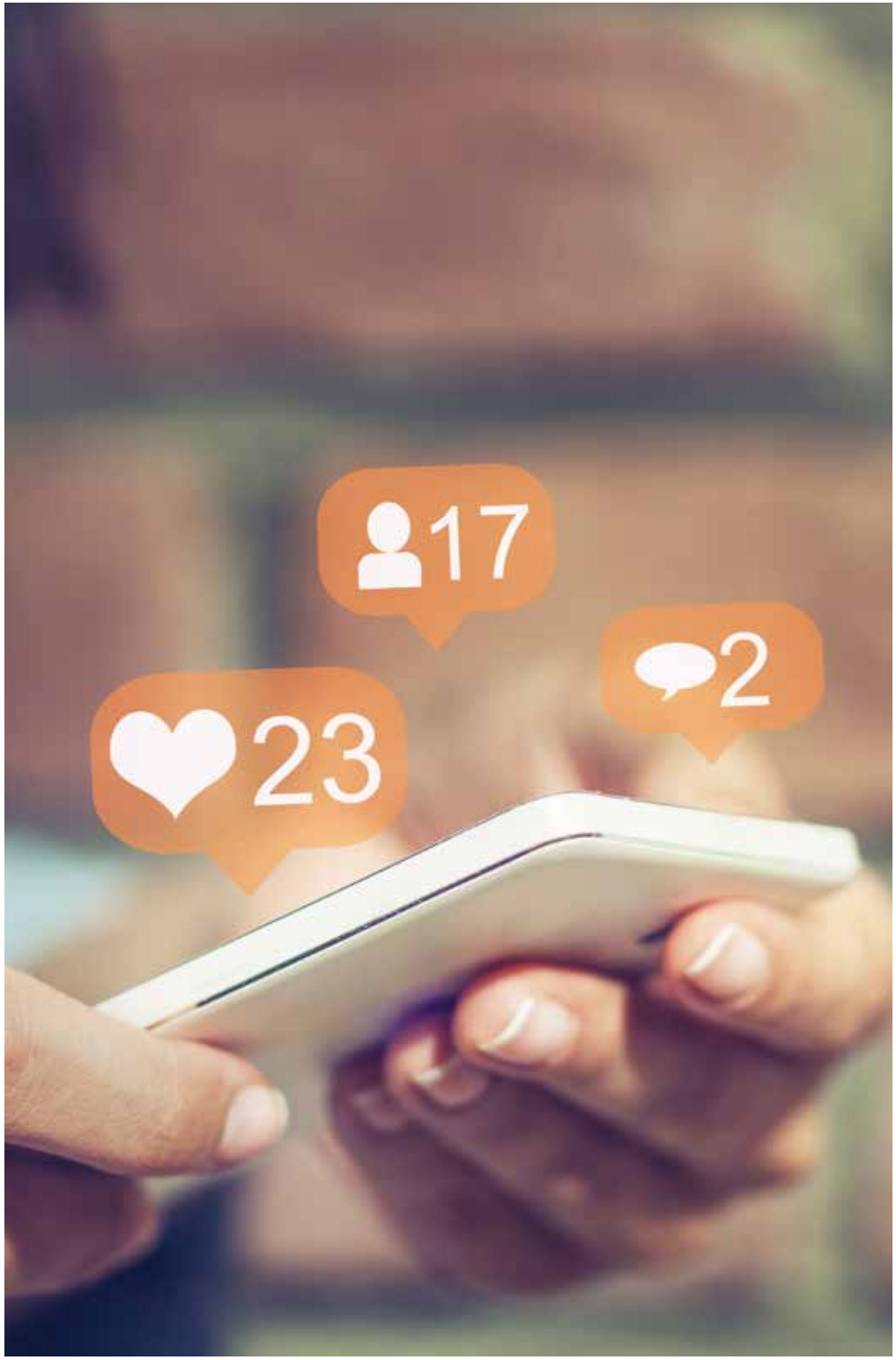
- Plaintiff crawled underneath a stationary train in the defendant's railyard and was severely injured when the train started moving.
- In its answer, defendant denied plaintiff's claim for failure to warn by sounding a horn or bell prior to moving the train car.
- Consistent with defendant's standard procedure, defendant's railroad foreman took steps to preserve the train's event recorder data which would have conclusively shown whether or not the train bell or horn was sounded prior to the train's movement. However, almost two years later, defendant realized that the recorder data was unavailable for production due to an initial error by the foreman in uploading the recorder data to the company vault.
- Court sanctioned (adverse jury instruction) defendant for failing to take reasonable steps to preserve the event recorder data. Particularly distressing to the Court was the fact that between the time of the accident and the time of plaintiff's discovery request for the event recorder data, no one from the railroad or its counsel actually had verified that the data was properly preserved. If timely verification efforts had occurred, there would have been an opportunity to restore or reacquire the relevant data.

Failure to Identify & Collect Third-Party Data: *Williams v. Angie's List, Inc.*, 2017 WL 1318419 (S.D. Ind. April 10, 2017)

- Employees sued company for undercompensating them for overtime worked.
- Company produced hours worked data for only one year, arguing that additional data fell outside its "possession, custody and control" because the data resided with a third-party, cloud-based service provider.
- Court granted employees' motion to compel finding that based on the contractual relationship between the company and the service provider, the company has the legal right to obtain the discovery sought.

Overbroad Request for Production of Social Media: *Gordon v. T.G.R. Logistics, Inc.*, 321 F.R.D. 401 (D. Wyo. May 10, 2017)

- Defendant company moved to compel production of plaintiff's "entire Facebook account history" on the ground that the information would be relevant to her claims of physical and emotional injury resulting from a motor vehicle accident.
- Court denied company's motion to compel because the discovery request exceeded the proper limits of proportionality.
- The Court explained that granting access to plaintiff's entire Facebook history would provide minimal relevant information while exposing substantial amounts of irrelevant information.



Top Ten
Data Breaches of 2017

1 River City Media

Individuals affected: 1,370,000,000

Cause: RCM, a U.S.-based email and Short Message Service (SMS) marketing company, failed to password-protect a backup that was accessible online. The records were available for at least three months.

Type of data: Names, IP addresses, ZIP codes and physical addresses associated with the email addresses.

Fallout: Some of River City Media's campaigns were legitimate, but as a spamming company others fall within a gray area. Several of RCM's clients have terminated their agreements with RCM.

2 Equifax

Individuals affected: 145,500,000

Cause: Criminals were able to exploit a vulnerability in a website application.

Type of data: Names, birth dates, social security numbers, addresses, some drivers' license numbers and credit card numbers.

Fallout: The U.S. Senate is considering several bills aimed at imposing even greater penalties for companies that experience data breaches. State Attorneys General are investigating what recourse they have against Equifax for the disclosure. Additionally, Equifax's CEO resigned.

3 T-Mobile

Individuals affected: 69,600,000

Cause: A bug on the T-Mobile website may have allowed hackers to view personal information of website visitors.

Type of data: Email addresses, account numbers and even phone IMSI numbers (a unique number that identifies subscribers) were open to discovery.

Fallout: T-Mobile's investigation determined that no customer information was compromised as a result of the security flaw.

4 Uber

Individuals affected: 57,000,000

Cause: Hack of a third-party server

Type of data: Data about riders and drivers including phone numbers, email addresses and names.

Fallout: Uber paid the hackers $100,000 to destroy the information. Once the story became public, Uber fired two of its top security officials. A "bug bounty" program is typical, but payments are generally in the $5,000 to $10,000 range. Most experts believe that the $100,000 payment is a record.

5 Dun and Bradstreet

Individuals affected: 33,500,000

Cause: Currently unknown, but may have resulted from a customer of D&B disclosing the information.

Type of data: Email addresses and other contact information from employees of thousands of companies.

Fallout: Access to this type of data could facilitate spear phishing attacks in the future.

6 We Heart It

Individuals affected: 8,000,000

Cause: Unknown

Type of data: Email addresses, usernames and encrypted passwords.

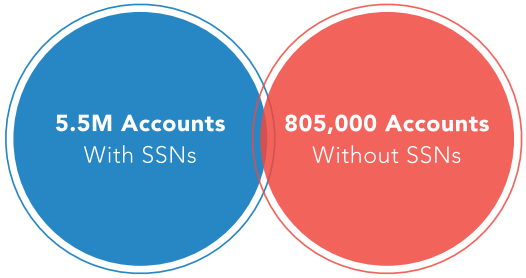
Fallout: The image-sharing site is used by upwards of 40 million teens. The breach took place a few years ago and affects accounts created between 2008 and November 2013. This shows how long it may take certain companies to discover a data breach.

7 Kansas Department of Commerce

Individuals affected: 5,500,000

Cause: Hackers

Type of data: Social Security Numbers (SSns)



Fallout: The data is from websites that help connect people to jobs, such as Kansasworks.com, where members of the public seeking employment can post their resumes and search job openings. Kansas was managing data for 16 states at the time of the hack, but not all were affected. In addition to the 5.5 million personal user accounts that included SSns, about 805,000 more accounts that did not contain SSns were also exposed.

8 Cloudfare

Individuals affected: 4,300,000

Cause: A coding error involving just a single wrong character.

Type of data: Chat messages, encryption keys, cookies, password manager data, hotel bookings and more.

Fallout: The leaked data had been cached by major search engines and the discovery triggered a frantic effort to remove the cached data before the flaw was publicized. Much of the exposed data would have normally been protected by SSL/TLS, but the nature of the vulnerability caused it to be exposed to the internet in unencrypted form. The sensitive data was exposed for months.

9 Broadsoft

Individuals affected: 4,000,000

Cause: Configuration error left a data storage bin containing seven years of data exposed to the public.

Type of data: Transaction numbers, MAC numbers, user names, account numbers for types of service purchased along with internal development information like SQL database dumps and code with login credentials.

Fallout: Time Warner Cable (TWC) had partnered with Broadsoft (a global communications company) to assist in unifying TWC communications. TWC reached out to its customers indicating that they should change their password, even though it was Broadsoft that experienced the breach.

10 America's Job Link Alliance (AJLA)

Individuals affected: 2,100,000

Cause: Hackers registered an account on the job portal and then used a vulnerability in the source code to extract data from other users.

Type of data: Names, dates of birth and SSns for users in ten of the 16 states.

Fallout: The FBI was involved in the investigation but AJLA was quick to notify and provide updated information on its website. It has also cooperated with the various states to assist their residents. AJLA was also quick to publicly disclose the breach — it had issued a press release within 2 weeks of its discovery.

Future Updates

- 2018 Spring Data Solutions Symposiums are in Troy on April 18, 2018 and in Grand Rapids on April 26, 2018. For more information and registration, please visit WNJ.com/2018DataSolutions.
- If you want to receive our Data Solutions eAlerts, seminar/webinar announcements and future Whitepapers, please subscribe by visiting WNJ.com/Subscribe.


Jay Yelton
269.276.8130
jyelton@wnj.com


Scott Carvo
616.752.2759
scarvo@wnj.com


Nate Steed
616.752.2723
nsteed@wnj.com


Dawn Ward
616.396.3039
dward@wnj.com


Norbert Kugele
616.752.2186
nkugele@wnj.com


Brian Lennon
616.752.2089
blennon@wnj.com

By providing discerning and proactive legal advice, Warner Norcross + Judd LLP builds a better partnership with its clients. Warner 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 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 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 Scott R. Carvo (scarvo@wnj.com or 616.752.2759).

Warner Norcross + Judd

Thank you!

Please visit WNJ.com.