Warner Norcross + Judd

A Retrospective of eDiscovery, Information Governance and Data Security in 2018

A Retrospective of eDiscovery, Information Governance and Data Security in 2018

Table of Contents

Welcome

Warner Norcross + Judd is pleased to share this overview of legal changes, trends and case studies in the 2018 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.

B. Jay Yelton III
Co-chair, Data Solutions Practice Group

Scott Carvo
Co-chair, Data Solutions Practice Group

California Consumer Privacy Act Breaks New Ground in U.S. Privacy Law

During 2018, California enacted a new privacy law that will go into effect in 2020. The California Consumer Privacy Act (CCPA) gives individuals considerable rights with respect to their personal information. While there are many similarities to the European Union's (EU) General Data Protection Regulation (GDPR), the new law is not modeled on the GDPR and there are some significant differences.

The new law applies to any organization that collects information from California residents, does business in California and meets any one of three additional requirements:

- **Has an annual gross revenue in excess of $25 million;**
- **Annually buys, sells or receives personal information of 50,000 or more California residents (or 50,000 or more "devices" or "households" located anywhere); or**
- **Derives 50% or more of its revenue from selling California residents' personal information.**

Even businesses with no physical presence in California may be subject to this law if they have a website accessible to California residents or otherwise do business with California businesses or residents.

The CCPA gives California residents the following rights:

- **To know what information has been collected, including the sources of the information and the business or commercial purposes for the data collection;**
- **To know what information has been shared;**
- **To access personal data;**
- **To have the business delete any personal data that the business collected from the California resident (with some limited exceptions);**
- **To opt out of having the California resident's personal information sold; and**
- **To be free from discrimination for exercising the resident's rights, including denying goods or services, charging different prices or rates for goods or services, or providing a different level or quality of goods or services — unless such differences are directly related to the value provided to the resident by his or her data.**

Although the law does not put any specific restrictions on what a business may do with the data that it collects, a business that is subject to the law must do the following:

- **Provide at least two methods for a California resident to exercise his or her rights, including a toll-free telephone number and, if the business has a website, a website address.**
- **Provide a notice of the categories of data the business collects and the purposes of the collection.**
- **If the business sells any personal data, have a "Do Not Sell My Information" button on the home page of its website. Additionally, California residents under the age of 16 years must opt in to data sales; and those under the age of 13 must opt in with parental consent.**

- **Create and post procedures that enable California residents to request their information for viewing or deletion.**
- **Verify the authenticity of any request to access, to delete or to not sell data and respond within 45 days (subject to a 45-day extension upon notice to the individual).**

The California Attorney General is required to issue regulations by July 2020, and may not enforce the law until the *earlier* of July 1, 2020, or six months after the publication of the final regulations. The California Attorney General may impose penalties of up to $2,500 per individual violation.

Additionally, California residents whose data is the subject of a data breach can sue for between $100 and $750 per incident if the business failed to implement reasonable security procedures. The CCPA expressly voids any arbitration provision or class action limitation on this right. Consumers are permitted to file these lawsuits beginning January 1, 2020.

The CCPA is the first U.S. law to provide such extensive rights to individuals for their personal data. While similar concepts apply under HIPAA and the GDPR, the CCPA's rules are different and in some instances go further than either of these laws. If your business meets the statutory thresholds described above, we strongly advise starting compliance efforts well in advance of 2020.

Phone Geolocation Not Subject to Search and Seizure Under the Fourth Amendment

On June 22, 2018, the Supreme Court issued an opinion in *Carpenter v. United States* regarding whether police must obtain a warrant to access detailed geolocation information generated by a cellphone's communication with cell towers. The Court's opinion was highly anticipated, given its potential repercussions on the legitimate expectation of privacy provided to individuals under the Fourth Amendment.

In its decision, the Court held that an individual has a legitimate expectation of privacy in the record of his or her physical movements, as recorded by his or her cell phone and its communication with nearby cell phone towers. To support its decision, the Court noted that geolocation data provided by a cell phone is detailed and easy to compile, similar to data provided by a vehicle's GPS tracking system. Furthermore, the Court acknowledged that cell phones continue to hold a unique significance in society given the comprehensive and detailed record they keep of an individual's movements and habits, and provide much more sensitive information about an individual that could implicate additional privacy concerns. Thus, the Court found that the access of geolocation data on one's cell phone constitutes a search under the Fourth Amendment.

While this decision served to maintain some expectation of privacy in cell phones, the Court noted that the decision in *Carpenter* was narrow. The Court did not state that geolocation data could never be accessed and used by police without a warrant; rather, it simply held that the length of time the police had access in this case — one week — violated the legitimate expectation of privacy. For now, the Court has continued to uphold some level of legitimate expectation of privacy in one's phone.

But What About Phone Access via Biometrics Under the Fifth Amendment?

A few years ago, the only way to unlock one's phone, computer or other device was through a password or PIN code, if that individual chose to have one. Because of this, the law was relatively well established — unless the individual provided consent and unlocked the device, or the authorities obtained a warrant, the individual was not required to unlock the device.

Questions have arisen, however, in regards to unlocking phones with biometrics. These mechanisms of unlocking one's phone, computer or other devices involve one's physical attributes, such as fingerprints or facial features, if facial recognition technology is used. Normally, individuals could invoke their Fifth Amendment right not to incriminate themselves and refuse to unlock, via password or PIN, their phone or computer for authorities. Some have suggested, however, that individuals may not be able to invoke this right if their phone is unlocked via fingerprint or facial recognition technology. This is because traditionally, one's physical attributes have not been considered testimonial — and the Fifth Amendment only protects testimonial acts.

For the most part, speaking and writing are considered "testimonial" acts under the Fifth Amendment, and are thus protected. Furthermore, writing protects typing, which in turn protects the entering of a password on a device. Pressing a fingerprint onto a pad or phone or holding up one's phone to their face, however, potentially does not fall under these categories of speaking and writing. This leaves these acts up to interpretation.

The area of unlocking devices through biometric data has little precedent in the legal realm — as of now, there are no Court of Appeals or Supreme Court cases that have touched on the issue. Ultimately, it remains to be seen how this question will interact with the protections given for cell phones under the Fourth Amendment.

FDA Guidance on Medical Device Cybersecurity?

With the increasing interconnectivity of medical devices to the Internet and other networks comes additional risk, as the healthcare and medical device sectors in particular face a growing number of cyber incidents, including cyber threats and attacks. These cyber incidents have the potential to disrupt the ability of medical devices to provide patients with adequate monitoring and care, and could result in the exposure of patient information. As a result, the Food and Drug Administration (FDA) developed and released draft guidance in October 2018 for manufacturers of medical devices, to ensure that manufacturers are designing and developing devices that are secure and contain protections for their users. The new guidance has three main elements and is intended to align with the globally recognized National Institute of Standard Technology's (NIST) Cybersecurity Framework.

First, the FDA suggests categorizing devices into one of two categories—Tier 1 devices, which have a high cybersecurity risk, or Tier 2 devices, which have a standard cybersecurity risk. This categorization would help remedy the current differences between the existing FDA medical device safety risk classifications and general security risks. Tier 1 devices would include devices such as pacemakers, dialysis devices, and infusion and insulin pumps, among others, which are capable of connecting to other devices or the Internet at large. Tier 2 devices would encompass any device that does not meet the criteria for Tier 1 devices.

Second, the FDA suggests that manufacturers use a Cybersecurity Bill of Materials (CBOM), which the FDA says will help manufacturers more uniformly and effectively implement cybersecurity risk management processes, including identifying assets, threats and liabilities and setting appropriate cybersecurity requirements. The largest benefit of CBOMs is that they may help medical device manufacturers establish which components of their devices are most vulnerable to cyber incidents.

Finally, the FDA mandates that manufacturers must comply with new cybersecurity documentation requirements in order to manufacture their devices. To do so, manufacturers must submit a design documentation demonstrating that their devices meet particular criteria, depending on whether the devices are classified as Tier 1 or Tier 2. The documentation requirements were created to make manufacturers consider how their designs operate as a whole in the premarket stage and ensure that the device designs contain prevention measures against cyber incidents, such as detection, response and recovery mechanisms.

The FDA Guidance is intended to recognize the ever-increasing risk of cybersecurity threats to medical devices, and the healthcare industry in general. The guidance, however, is in its beginning stages. Only time will tell if the guidance will have a positive impact on the protection of medical devices against cyber incidents.

GDPR Effect on U.S. Businesses

The General Data Protection Regulation (GDPR) went into effect on May 25, 2018. The GDPR is a new European Union (EU) privacy and protection law designed to provide greater protections to the personal data of individuals in the EU. The new regulation requires data "controllers" and "processers" to comply with a host of obligations. Companies that fail to do so are subject to fines up to four percent of their global annual revenue or 20 million euros — whichever fine is higher. The broad language of the GDPR binds both EU-based and international businesses and is forcing them to reorganize their data retention and processing practices.

Territorial Reach

Article 3 of the GDPR expands the territorial reach of EU data law to organizations across the world. GDPR requirements apply to:

1. Organizations that maintain an establishment in the EU "regardless of whether the processing actually takes place in the EU";

2. Organizations not established in the EU that process (e.g., collect, store or transmit) personal information of EU residents in connection with offering goods or services, even those services provided online; and

3. Organizations not established in the EU that process personal information of EU residents for the purpose of monitoring the online behavior of an individual.[1]

"Organizations, including U.S.-based companies that fall within any of these three categories [are] required to comply with the numerous obligations imposed by the GDPR."[2]

Impact on Data Retention

Data retention is a major focal point of the GDPR. Article 5(1)(e) requires personal data to be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." GDPR's extraterritorial reach therefore limits how long a U.S. organization may retain personal data of an EU resident. The GDPR does not specify exact retention periods. Instead, it is up to individual businesses to determine how long *is necessary* to retain personal data for the purposes for which it was processed. Determining factors may include, but are not limited to, statutory retention periods, claim limitation periods, industry practices and individual business needs.[3] Without a uniform retention requirement, data retention statutes differ from country to country, and businesses are expected to retain certain types of data for longer periods than others. For example, Giulio Coraggio, head of DLA Piper's technology sector practice in Italy, explained "[i]t is appropriate to retain former employees' personal data up to the expiry of the statute of limitation period provided by local laws."[4] Therefore, multinational organizations operating across European borders should consider the legal differences of the countries they conduct business in.[5] In response to the enactment of the GDPR, many European countries have amended their statutory retention schedules to embody GDPR requirements.

Conflicts with U.S. Law

Given the novelty of the GDPR, there is little guidance regarding the conflict between legally-based U.S. retention schedules and the GDPR's requirement to retain data for only as long as necessary. Art. 21(1) allows for the continued processing of personal data if the company can demonstrate "compelling legitimate grounds" for doing so. In situations where a U.S. company must retain data to comply with U.S. retention laws, it may be able to demonstrate that compliance with American laws is a legitimate interest.[6] However, the language of the GDPR is clear that its requirements apply to all organizations processing EU data. If a U.S. organization is not bound by legal obligations, it should only keep data of individuals for as long as necessary to avoid sanctions.

[1] *The General Data Protection Regulation: A Primer For U.S.-Based Organizations That Handle EU Personal Data*, GIBSON DUNN (December 4, 2017).

[2] *Id.; see also* Adam Deflorian, *What Does EU's General Data Protection Regulation Mean For American Brands?*, FORBES (Mar. 27, 2018).

[3] *How Long Should You Retain Your Employee Data Under GDPR?*, SILICONREPUBLIC (May 7, 2018).

[4] Marcus Hoy, *Ex-Employee Data Retention Policies Face New EU Privacy Regime*, BLOOMBERG LAW (Dec. 13, 2017).

[5] *How can the GDPR Data Retention Policy be Defined for Multinational Companies?*, PAYROLL SERVICES ALLIANCE (Feb. 20, 2018).

[6] Stacey Garrett, *Are U.S. Records Retention Requirements on a Collision Course with the GDPR's 'Right to Erasure?'*, LAW.COM (May 2, 2018).

GDPR Enforcement Actions

The European Union's (EU) General Data Protection Regulation went into effect on May 25, 2018, and we are already seeing EU data protection authorities taking enforcement actions. Here is a quick summary of published enforcement actions taken during 2018:

UK Enforcement Action

AggregateIQ Data Services Ltd. (AIQ) is a Canadian data analytics firm that uses data to target political advertisements to voters. Its clients include UK political organizations. Although AIQ did not have any establishment in the EU, the UK's Information Commissioner's Office (ICO) found that AIQ fell within the territorial scope of the EU because it was monitoring behavior of data subjects in the EU. The ICO further concluded that AIQ was processing data in a manner that data subjects were not aware of, for a purpose they would not have expected, without legal justification, and without meeting the GDPR's transparency requirements. Although the ICO did not issue any monetary penalty, it did issue an Enforcement Notice that requires AIQ to "cease processing any personal data of UK or EU citizens obtained from UK political organizations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes." AIQ is appealing the decision.

Austrian Enforcement Action

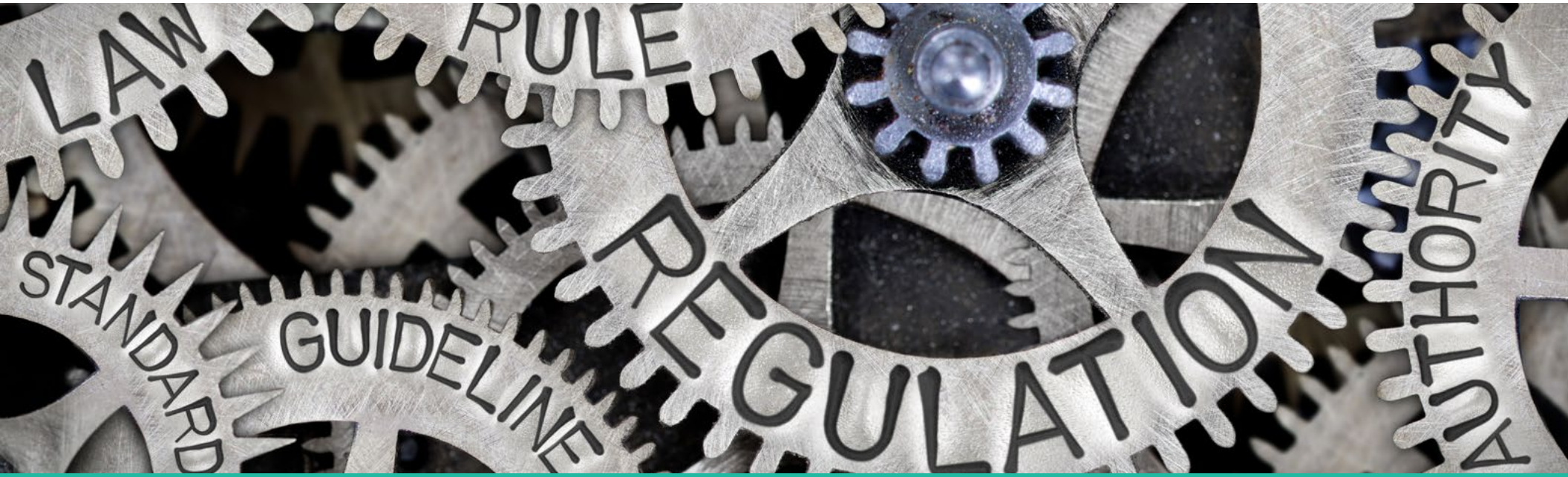
The Austrian Data Protection Authority (DSB) took action against an entrepreneur for installing a CCTV camera in front of its establishment that also recorded a large part of the sidewalk. The DSB found that "large-scale" monitoring of a public space was not allowed under the GDPR, and the camera was not appropriately marked as conducting video surveillance, meaning that the GDPR's transparency requirement had not be satisfied. The DSB fined the entrepreneur EUR 4,800 for the violation.

German Enforcement Action

The data protection authority for the German state of Baden-Württemberg (LfDI) imposed a fine of EUR 20,000 on a social media provider for a violation of its data security obligations under the GDPR. The social media provider suffered a breach following a hacker attack in the summer of 2018. While the social media provider promptly provided notification, during its investigation, LfDI found that the social media provider stored passwords in plain text and in an unencrypted format, which helped facilitate the attack. The penalty in this case reflected the social media provider's full and willing cooperation with the LfDI.

French Enforcement Action

France's data protection authority (CNIL), issued a formal warning to two companies — Teemo, Inc. (Teemo) and Fidzup SAS (Fidzup) — that CNIL alleged had improperly collected and retained geolocation data in violation of the GDPR. Both companies provide software development kits that are used in mobile applications to track the locations of users in order to send advertisements targeted to the users' locations. CNIL found that users of mobile apps with Teemo and Fidzup software development kits either did not receive any information about the data collection activities (in Teemo's case) or did not receive notification of the purposes of the data collection (in Fidzup's case). CNIL also found that Teemo's retention of geolocation data for 13 months violated the GDPR's requirement to define and respect a data retention period that is proportionate to the purpose of the processing.



eDiscovery Mistakes and Lessons Learned in 2018

1. Ineffective Litigation Hold

EPAC Technologies, Inc. v. HarperCollins Christian Publishing, Inc., 2018 WL 1542040 (MD Tenn Mar 29, 2018)

- The plaintiff alleged that the defendant breached the terms of a Master Services Agreement and sued for the damages resulting therefrom. By auditing the defendant's document productions, the plaintiff determined that the defendant had not produced its relevant email communications with the plaintiff or with third parties. The plaintiff asked for the appointment of a Special Master pursuant to Federal Rule of Civil Procedure 53.

- The Special Master determined that, while the defendant did issue a timely litigation hold, the hold was "a boilerplate form deployed without guidance" and that it was "ignored by all recipients." The failure to properly implement and monitor the litigation hold led to the deletion of over 750,000 emails, as well as the loss of other electronic and tangible information. The Special Master characterized the defendant's failure as "arrogance by management, lack of initiative by IT and a pitiable lack of legal leadership...." He contrasted the efforts undertaken in this case with those the defendant took in a concurrent Department of Justice investigation. The Special Master noted that the defendant "hired eDiscovery counsel and an eDiscovery service provider" showing it "knew what to do" and "chose not to do it" in this litigation.

- The Court reviewed the Special Master's report and concluded that the defendant's "preservation and production deficiencies have turned...into a seemingly endless marathon of discovery about discovery." The Court ordered that the defendant bear 75% of the Special Master's fees and costs and 50% of the plaintiff's attorney fees and costs associated with the Special Master's proceedings.

Lesson Learned

Issuing a litigation hold is step one; not the end of the counsel's and client's responsibilities to preserve potentially relevant electronic data. The litigation hold must be carefully thought out to target the most likely sources of discoverable information. Once issued, the counsel and client should conduct regular follow-ups to ensure its effective implementation.

2. Multiple Document Versions Create Mischief

Webasto Thermo & Comfort North America, Inc. v. BesTop, Inc., 323 F Supp 3d 935 (ED Mich 2018)

- The plaintiff filed a claim against the defendant alleging that the defendant's "Sunrider for Hardtop" device infringed its patent. The defendant filed a motion to dismiss arguing that its device was "prior art." In support of its argument, the defendant attached a PowerPoint presentation given to Fiat Chrysler Automobiles Group (FCA) showing the "Sunrider for Hardtop" before the plaintiff filed its patent application. A declaration from its Director of Engineering stated that he had designed the prototype and made the presentation to FCA.

- In response to the plaintiff's subpoena, FCA produced copies of the PowerPoint presentation it received from the defendant. With the exception of the title page, every page of the PowerPoint had a footer that contained the language, "Disclosure or duplication without consent is prohibited." The footer arguably contradicted the defendant's "prior art" argument because the disclosure to FCA was made confidentially and not for public consumption. The presentation copy the defendant submitted with its Motion to Dismiss did not contain the footer language anywhere. The plaintiff filed a motion for sanctions against the defendant for making misrepresentations to the court in its Motion to Dismiss.

- In response, the defendant provided shifting explanations for what occurred. The defendant's counsel initially claimed that he did not pay attention to the fine print on the slides. He said when he converted the native file to a PDF file an apparent technical glitch resulted in the footer being deleted. The defendant's counsel later testified that actually he believed he was working with the native file when preparing the declaration, when in fact he was working with another scanned version of the presentation without crucial footer language. He claimed he did not know that there were multiple copies of the presentation circulating in his law office. He also took the position that the absence of the footer had no bearing on the resolution of defendant's Motion to Dismiss. The Court did not agree.

- The Court found that the defense counsel had been reckless in submitting the incomplete version of the presentation in support of the defendant's Motion to Dismiss. The Court also raised concern that the defense counsel failed to immediately inform the Court once he learned of the error or to investigate the cause of the error or even to apologize to the Court. As for the defendant's counsel's opinion that the footer was irrelevant, the Court labelled it "absurd." The Court ordered that the defendant pay the plaintiff's reasonable attorney fees in litigating "what should have been an otherwise unnecessary motion for sanctions" and precluded the defendant's use of any evidence related to its PowerPoint presentation to FCA.

Lesson Learned

That multiple versions of an electronic document exist within an organization is not breaking news. Knowing this, counsel must be careful to examine any electronic evidence it plans to rely on in court submissions or at trial. Make sure that the document is what you represent it to be. And, if it is not, be prepared to swiftly and humbly correct the error with opposing counsel and the court.

3. Overbroad Search Terms

Webasto Thermo & Comfort North America, Inc. v. BesTop, Inc., 326 FRD 465 (ED Mich 2018)

- Also in the *Webasto* case, the Court entered a stipulated order governing the production of ESI. The stated purpose of the ESI Order was "to promote, whenever possible, the early resolution of disputes regarding the discovery of electronically stored information (ESI) without Court intervention." Despite this stated purpose, the plaintiff filed an emergency motion for a protective order to stay ESI discovery and for cost-shifting. The plaintiff argued that the defendant violated the ESI Order by propounding overly broad search terms and refusing to "work in good faith to target its search terms to specific issues in this case."

- The ESI Order precluded the use of "[i]ndiscriminate terms, such as the producing company's name or its product name...unless combined with narrowing search criteria that significantly reduce the risk of overproduction." The search terms propounded by the defendant were all single words and referred to the plaintiff's products, to the defendant's company name and to generic items, such as "sale," "fabric" and "drawing." When these terms were run against the plaintiff's relevant email accounts, over 614,000 records were identified. Review of the first 100 records showed that they were unrelated to any of the issues in the case.

- The Court found that the defendant's search terms were "overly broad, and in some cases...specifically excluded under ¶ 1.3(3) of the ESI Order." The Court noted that "[a]dversarial discovery practice, particularly in the context of ESI, is anathema to the principles underlying the Federal Rules...." The Court ordered the parties to meet and confer in good faith to narrow the defendant's search terms to reasonably limit the plaintiff's email production. If the defendant failed to narrow its search terms, the Court would reconsider the plaintiff's request for cost-shifting.

Lesson Learned

Serving targeted discovery requests is generally a good idea in this world of ever-increasing volumes of electronic data. It reduces both the time and expense of discovery. And, it's a good idea to follow a court's order regarding the parameters of discovery. Patent violations of those orders may result in costly sanctions.

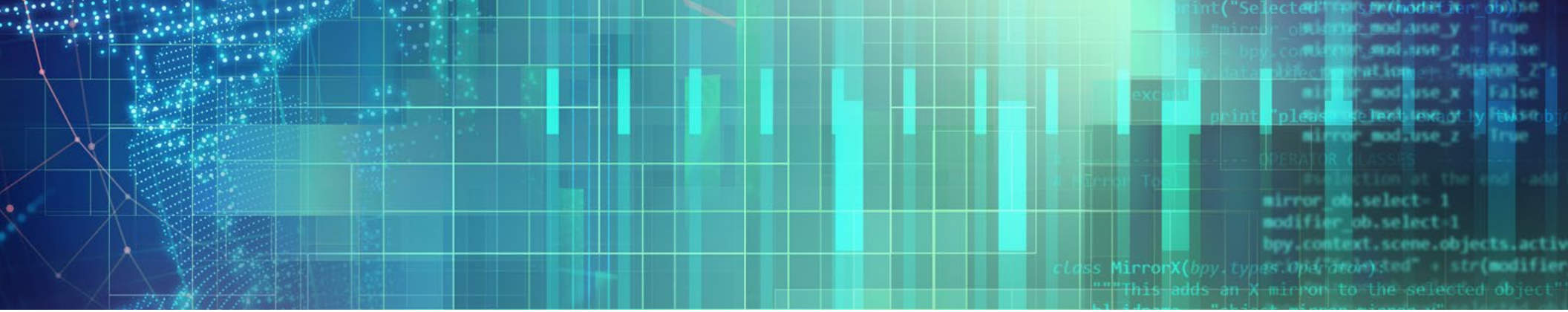
4. Boilerplate Discovery Objections

Wesley Corporation v. Zoom TV Products, LLC, 2018 WL 372700 (ED Mich Jan 11, 2018)

- The plaintiffs sued alleging that the defendants had breached their settlement agreement relating to previously filed patent and trademark infringement litigation. The plaintiffs moved to compel the defendants to produce documents and to amend their interrogatory responses. The defendants' response to almost every interrogatory invoked the standard laundry list of objections: "vague, overly broad, unduly burdensome, harassing, and/or seeking information that is irrelevant and/or not reasonably calculated to lead to the discovery of admissible evidence." Their responses to almost every document request were similar in form.

- At the hearing on the plaintiffs' motion to compel, the parties agreed to a 45-day extension of the discovery deadline to allow defendants to amend their discovery responses. The Court approved the extension, but took the defendants to task for their use of boilerplate objections—and granted the plaintiffs' request for attorney fees. The Court noted the "strong and widespread criticism" of boilerplate objections in federal case law, concluding, "[t]hese cases, in their interpretation of the discovery rules and their denunciation of boilerplate, "are not aspirational, they are the law."

- The Court went on to state its displeasure at having to regulate



the discovery process "where attorneys engage in foot-dragging and obstructionism." The Court promised that further interventions would be "accompanied by more significant sanctions...."

Lesson Learned

Boilerplate objections are a sure way to get on a court's bad side. Using them can lead to waiver of objections, including privilege objections. Don't use them.

5. Inadequate Privilege Log Descriptions

BlackRock Balanced Capital Portfolio (FI) v. Deutsche Bank Nat'l Trust Company, 2018 WL 3584020 (SDNY July 23, 2018)

- This is one of the many residential mortgage-backed securities trust cases. Before the Court was the plaintiff's motion directed at deficiencies in the defendant's privilege log. The Court allowed the defendant to import metadata to assist in the generation of its privilege log, but noted that the defendant still had the obligation to ensure that its privilege log complied with federal and local rules. Finding the privilege log deficient, the Court directed the defendant to review and correct its log as necessary, to conduct a "substantive and detailed" meet-and-confer with the plaintiff to resolve outstanding issues, and then bring any unresolved issues to the Court's attention.
- The parties could not resolve issues related to deficient log entries or to the defendant's invocation of the "common interest privilege." The Court conducted an *in camera* inspection of representative documents submitted by the defendant.
- The Court's inspection revealed that some of the sample documents were adequately described on the privilege log and were in fact privileged. However, because of the overwhelming problems with the log, the Court ordered that the defendant "has waived its privilege with respect to all documents listed on its privilege log...unless it can make a particularized showing as to individual documents that it believes are: (1) adequately described on its log; and (2) in fact, privileged." The Court limited this safety valve to documents "with complete information — that is, the name of the author of the document, the name of any attorney, a clear description of the document, etc...." The Court's order of the waiver impacted over 70,000 of defendant's privilege log entries.

Lesson Learned

The failure to produce an adequate privilege log can result in waiver and the obligation to produce privileged materials to an opponent — a potentially devastating consequence. Know what is required by local rule and/or case law in the relevant jurisdiction. If the requirements seem burdensome, apply to the court for relief in advance. Don't risk producing an inadequate privilege log and then throwing yourself on the mercy of the court.

6. Failure to Narrow Scope of Subpoena

In re *Modern Plastics Corp.*, 2018 WL 1959536 (6th Cir. 2018)

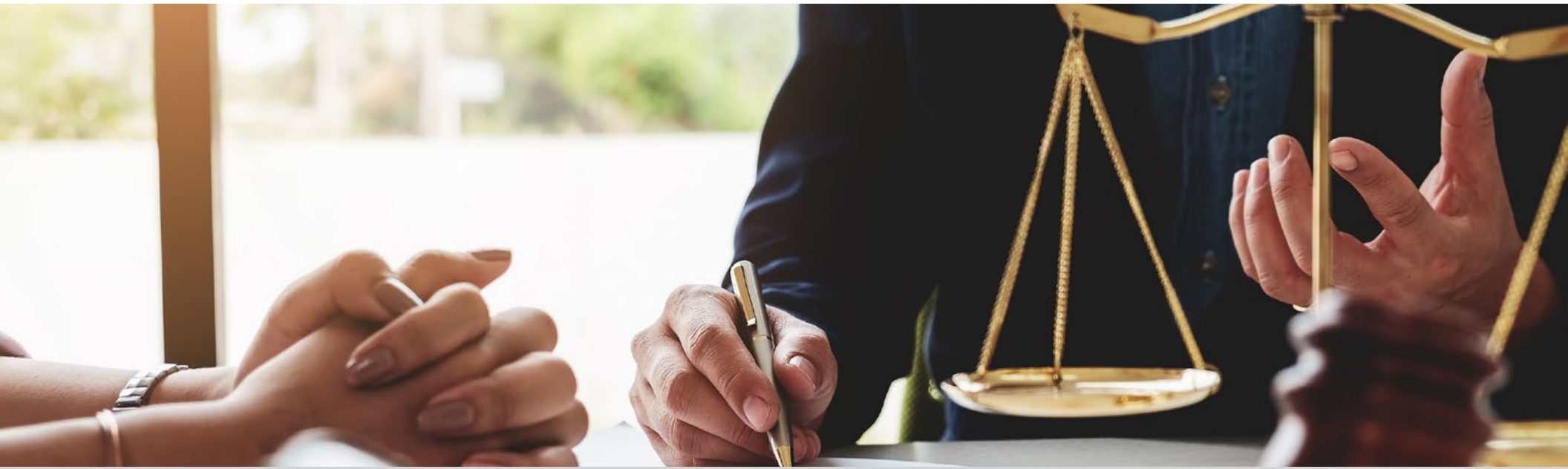
- A creditor brought an adversary proceeding against the bankruptcy trustee for breach of fiduciary duty alleging that the trustee allowed certain bankruptcy estate assets to deteriorate in value. The creditor's counsel served subpoenas on five non-parties, including the bank from which it had purchased the mortgages and the bank's counsel.

- The subpoenas sought production of as many as 58 broad categories of documents going back over nine years. The non-parties attempted to narrow the scope of the subpoenas, informing the creditor's counsel that without narrowing, their compliance efforts would be "quite expensive," as they anticipated a high volume of potentially responsive and privileged documents for review. The creditor's counsel was uncooperative. The non-parties filed timely responses and objections to the subpoenas that included a request for reimbursement.

- The creditor's counsel was kept apprised of the non-parties' compliance efforts through periodic updates from their counsel. When responsive documents were ready for production, the creditor's counsel was informed that no production would be made until a protective order was entered and that the non-parties expected reimbursement of over $150,000 in attorney fees and expenses. The creditor's counsel objected to the reimbursement demand and motions were filed with the Court to resolve the issue.

- Citing Rule 45(d), the Court awarded over $100,000 in attorney fees and almost $60,000 in costs to the non-parties for their efforts in complying with the subpoena. When the creditor's payment was not forthcoming, the non-parties filed a motion for contempt that was granted. The Court awarded the non-parties an additional $4,725 for fees and costs incurred in litigating the contempt motion. The creditor paid the outstanding awards, but appealed the Court's rulings.

- The Sixth Circuit Court of Appeals affirmed. The Court held



that the monetary awards were proper under Rule 45(d)(1) which requires an issuing party to "take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena" and provides that the "Court... enforce this duty and impose an appropriate sanction — which may include...reasonable attorney's fees — on a party or attorney who fails to comply."

- The Court reasoned that the creditor's counsel was an experienced commercial litigator who should have known compliance with the subpoenas "would involve considerable time and resources...." The creditor's counsel could have avoided "much of the expense...either initially, or by engaging with [non-parties'] counsel to address the concerns...[and] tailor the document requests."

Lesson Learned

Rule 45 provides greater protection to non-parties — including mandatory cost-shifting of any "significant expenses" incurred by the non-party in complying with the subpoena. This makes it incumbent on the party issuing the subpoena to narrowly tailor its requests and to work cooperatively with the non-party to limit the cost of compliance.

7. Overbroad Discovery Requests for Social Media

Hinostroza v. Denny's Inc., 2018 WL 3212014 (D. Nev. June 29, 2018)

- The plaintiff allegedly slipped and fell at the defendant's restaurant, claiming multiple injuries and physical impairments requiring future lumbar surgery. The defendant requested that the plaintiff provide releases to allow the defendant to obtain certain records. The plaintiff provided some releases, but not others. The defendant filed a motion to compel regarding requests for several items, including text messages and emails between the plaintiff and witnesses, activity tracker information and social media content.

- The magistrate judge ruled that phone records were discoverable where the request was limited in date and time and about a key issue in the case. The magistrate judge compelled the plaintiff to produce text messages, emails and written communications with witnesses related to the slip and fall and those related to any discussion of resulting physical injuries or emotional distress. The Court also ordered the plaintiff to produce her texts and emails sent in the 48 hours after the accident to the extent they related to the accident or any resulting physical injuries or emotional distress.

- As for data from the plaintiff's activity tracker, the plaintiff responded that she had no responsive documents in her possession, custody or control and reserved the right to supplement her response. The magistrate judge found her response insufficient because the plaintiff failed to describe the search she conducted for those records and ordered her to provide a description of her search efforts to the defendant.

- With regard to social media content, the magistrate judge noted that social media content is usually "neither privileged nor protected by any right of privacy"... and was "relevant... because social media activity... is reflective of an individual's contemporaneous emotions and mental state." The plaintiff was ordered to identify all her social media platform accounts and have her counsel review them and "disclose to Defendant all information which references the alleged accident, is relevant to Plaintiff's claims, and exhibits Plaintiff's emotional or mental state, expressions, and reactions related to the alleged accident."

Lesson Learned

There is nothing sacred about social media. When it is relevant to a claim or defense in litigation it must be preserved, collected and produced like any other electronic data. However, requests for social media evidence are not an excuse for "fishing expeditions." Like all other discovery requests, they must be limited to evidence that is relevant and proportional to the needs of the case.

8. Failure of Counsel to Advise Client to Issue Proper Litigation Hold

Industrial Quick Search, Inc. v. Miller, Rosado & Algois, LLP, 2018 WL 264111 (S.D.N.Y. Jan. 2, 2018)

- This case concerns legal malpractice and breach of contract allegations against the defendants that had represented the plaintiffs in a prior copyright infringement action. The plaintiffs operated a web-based directory of industrial products and services. With help from a third party with access to the competitor's information, the plaintiffs took copyrighted material from a competitor when setting up the directory.

- In the copyright infringement action, the competitor filed a Rule 37 motion for sanctions against the plaintiffs. The Court found that the plaintiffs had intentionally destroyed relevant documents and entered an order striking their pleadings and entering default judgment against them (the plaintiffs were the defendants in the copyright infringement action). The plaintiffs later settled the case for $2.5 million.

- In the malpractice case, the plaintiffs alleged that the defendants negligently failed to provide competent advice regarding the discovery process. The parties filed cross-motions for summary judgment and the Court ordered the parties to trial on this claim.

- In the absence of case law supporting the proposition that failure to institute a litigation hold or monitor discovery compliance constituted attorney negligence, the Court concluded that such a failure would fall below "the ordinary and reasonable skill possessed by members of the legal bar" and constitute attorney negligence and that genuine issues of material fact existed regarding the plaintiffs' related claims.

- The Court rejected the defendants' argument that they owed no duty to their clients as a matter of law because they were retained two years after the plaintiffs received the cease-and-desist letter that triggered the plaintiffs' duty to preserve. The Court found that once they were retained, the defendants had an independent obligation to ensure relevant evidence was preserved as well as a duty to explain to their client about their duty to preserve relevant evidence.

Lesson Learned

Responding to the discovery in litigation is a collaborative effort between the client and counsel. The client needs to inform the counsel of where the evidence is, and the counsel must direct the client regarding its legal obligation to preserve evidence. Even if engaged late in the game, the counsel should be prepared to review the duty to preserve with its client if for no other reason than to understand what potential discovery landmines exist.

9. Requesting Details of Opponent's Use of Technology-Assisted Review

Entrata, Inc. v. Yardi Systems, Inc., 2018 WL 5470454 (D Utah Oct 29, 2018)

- This case concerns a dispute between two companies selling competing software products for property management. The plaintiff alleged that the defendant has engaged in unfair, unlawful and anti-competitive business practices against it and its customers.

- The parties attempted on numerous occasions to agree to an ESI discovery protocol, but to no avail. The parties neither executed a final protocol nor requested Court approval of either of their competing protocols.

- With no agreed ESI protocol in place, the plaintiff used technology-assisted review (TAR) to facilitate its document productions. The plaintiff previously made clear to the defendant that it intended to use TAR to identify potentially responsive documents for review

prior to production. After the plaintiff's document productions, the defendant then raised questions about the plaintiff's TAR methodology. The defendant requested TAR metrics, alleging the plaintiff's methodology was "unreliable and . . . insufficient." The plaintiff declined to turn over the requested metrics. On the last day of fact discovery, the defendant filed a motion to compel the plaintiff to disclose "the complete methodology and results" of its TAR process.

- The magistrate judge denied the motion, noting that the defendant offered no evidence to support its allegation that the plaintiff's TAR process was deficient. Without more detailed reasons why production of the plaintiff's TAR information is needed, the Court was unwilling to order the plaintiff to produce such information. The defendant objected to the magistrate judge's order.

- The defendant argued that the Federal Rules of Civil Procedure and relevant case law required the plaintiff to share its TAR methodology without a prior showing of any deficiencies in the plaintiff's document production. The defendant also argued that the plaintiff could not employ TAR without first obtaining Court authorization. The Court rejected the defendant's arguments and denied its motion.

- The Court acknowledged that the Federal Rules require cooperation, but fall short of mandating that a party divulge its TAR methodology. The Court's survey of relevant case law revealed that only where the parties had entered into an ESI protocol was transparency regarding TAR methodology required.

- On the question of obtaining court approval before using TAR, the Court also found that case law has developed to the point that "it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it."

Lesson Learned

In cases with high volumes of ESI, the parties should attempt to agree to an ESI protocol or request the court to enter an order with input from the parties. Any issues regarding methodology should be addressed promptly. In any case, when challenging methodology, be prepared to show how the methodology failed to identify and produce relevant information.

Top 5 Privacy Policy Updates You Should Make for the Digital Age

In a time where privacy is increasingly a concern among consumers and businesses alike, it is important that companies with an online presence have a robust privacy policy to inform users of how their data is collected and used. Many websites have such a policy, but — unless there is an issue concerning user data or a data breach — the policy often remains unchanged, gathering dust as a "formality" hidden at the bottom of the home page. In light of that, privacy policies are often missing some important elements that protect both companies and users from data issues that might arise from use of an online platform. A few examples of commonly forgotten elements for a good privacy policy include:

General Data Protection Regulation (GDPR)

The European Union's GDPR is a sweeping regulation that, due to the global nature of the Internet, has implications for many businesses — even some of those who do most of their business locally. Companies working on GDPR compliance should consider updating their privacy policies to reflect any changes to how they collect and manage user data.

Digital Millennium Copyright Act (DMCA)

Although the DMCA is not new legislation, the effects can be seen in new ways as companies increasingly gather user input and data through online platforms. If a company website invites users to input content, the privacy policy should be clear about what data the user may and may not submit. For example, a company may run a promotional contest asking users to submit original content — perhaps a story, song or piece of artwork. If a user submits copyrighted work and the company promotes that work, there are situations in which the company could be in violation of the DMCA. Companies with websites that allow for user submissions should be familiar with the DMCA and should have applicable language in their privacy policies regarding potential copyright issues surrounding those submissions.

General Copyright Issues

In addition to users submitting material in potential violation of someone else's copyright, companies that allow user submissions should also make clear who owns any original material that users submit on the company website. For example, if users are allowed to enter reviews online, the content of those reviews should become the property of the company. This avoids any copyright complications if the company uses original, user-submitted content in marketing material.

Data Analytics

Many companies use third-party analytics services, such as Google Analytics or Adobe, to analyze website traffic and use of their web services. A comprehensive privacy policy should include a description of those analytics, including any third-parties who can gain access to user data. Such a disclosure is often required by the third-party service. Additionally — and equally important — users have an interest in knowing exactly how their data is being accessed and used, especially by those outside of the company. If your website is used by residents of the EU, the GDPR requires specific details about third-party data collection on your website.

User Management

Finally, a good privacy policy should tell the user what control they have over the data that is being collected, and how to control it. For example, if a website allows users to submit content, it should be clear how to contact the company if the user would like to manage the information submitted with that content.

There are certainly other necessary elements in a comprehensive privacy policy, but these are just some of the components that are often missing. Some websites incorporate these elements in their Terms of Service or Terms of Use, which are both good alternatives. Still, if the policy is meant to manage user data, it is a good practice to include those policies within a comprehensive privacy policy.

Top Ten Data Breaches of 2018

Facebook 1

Individuals Affected: 2,200,000,000

Cause: Malicious third-party scrapers searched for a registered user's phone number or email address, which allowed the scrapers to remove information from their public profile.

Type of Data: Public profile information

Fallout: Facebook CEO Mark Zuckerberg acknowledged that the third parties were able to gather information for years prior to discovery, meaning that the breach affected a majority of Facebook users.

Aadhaar 2

Individuals Affected: 1,100,000,000

Cause: Cybercriminals accessed India's national ID database and sold data at 500 rupees or $8.

Type of Data: Names, addresses, photographs, phone numbers and email addresses

Fallout: The Indian Tribune broke the story regarding the breach of Aadhaar, revealing to the Indian government that it had purchased the login credentials to a service being offered by anonymous sellers over WhatsApp. Using the service, the reporters could enter any Aadhaar number and retrieve information about an individual. An additional payment of 300 rupees provided access to a software through which anyone could print an ID card for an Aadhaar number.

Exactis 3

Individuals Affected: 340,000,000

Cause: Exactis left a database exposed on a publicly accessible server.

Type of Data: Phone numbers, home addresses, email addresses and other highly personal information including interests, habits and the number, age and gender of an individual's children

Fallout: The Exactis breach resulted in a wide-range of personally identifiable information becoming available, including an individual's hobbies and interests. The information disclosed in this breach, in particular, could be used to impersonate victims, conduct social engineering and commit fraud.

Marriott International 4

Individuals Affected: 327,000,000

Cause: Hackers gained unauthorized access to the Starwood Hotels and Resorts reservation system.

Type of Data: Names, mailing addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, payment card numbers and expiration dates

Fallout: The breach affected the reservation system for Marriott's Starwood Hotels and Resorts brand. Furthermore, while the hackers acquired the payment card numbers and expirations of millions of guests, this information was encrypted. Marriott has been unable to confirm whether the hackers have decrypted the credit card numbers.

Under Armour 5

Individuals affected: 150,000,000

Cause: An unauthorized party gained access to data from MyFitnessPal user accounts.

Type of Data: Usernames, email addresses and hashed passwords

Fallout: While the breach did not affect payment card data, hackers may be able to use or sell password information acquired from the breach to gain access to more sensitive information or break into other accounts of victims of the breach.

FitMetrix (owned by MindBody) 6

Individuals affected: 113,500,000

Cause: FitMetrix operated several servers without passwords.

Type of Data: User names, gender, phone numbers, profile photos, primary workout location and emergency contacts

Fallout: While many of the records leaked were not fully complete, it is unknown how long the servers were exposed and leaking information.

Quora 7

Individuals affected: 100,000,000

Cause: Computer systems were compromised by a "malicious third party."

Type of Data: User names, email addresses, IP addresses, encrypted passwords, user account settings, personalization data and content (including blog posts, questions, answers, comments)

Fallout: The company is still investigating the breach; however, it has stated that the incident is unlikely to result in identity theft because Quora does not collect sensitive information like social security numbers or credit card numbers.

MyHeritage 8

Individuals affected: 92,283,900

Cause: A private server outside of MyHeritage contained a file with MyHeritage information.

Type of Data: Email addresses and hashed passwords of users

Fallout: MyHeritage stores its family tree and DNA data on separate servers than those it uses for user email addresses. It said there is no reason to believe that the information has been compromised.

Facebook 9

Individuals affected: 50,000,000 initially reported; however, Facebook has now said the number is more like 30,000,000

Cause: Hackers exploited a feature in Facebook's code allowing them to take over user accounts.

Type of Data: Phone numbers, email addresses, names, gender, relationship status and recent check-in locations

Fallout: Facebook officials do not know the identity or origin of the attackers and it is unclear how many users were affected. The investigation is still in its early stages; however, this is believed to be the largest breach in Facebook's history.

Localblox 10

Individuals affected: 47,000,000

Cause: Localblox left a large store of profile data on a public but unlisted Amazon S3 storage bucket without a password.

Type of Data: Names, physical addresses, birth dates and other data from social media websites (including Facebook, LinkedIn, Twitter and Zillow)

Fallout: The leaked data was collected from multiple sources, such as social media websites, and aggregated by IP addresses.

Warner Norcross + Judd