Warner Norcross + Judd

A RETROSPECTIVE OF

2019

eDiscovery, Privacy and Cybersecurity in 2019

BY KELLY HOLLINGSWORTH

GDPR

A YEAR IN REVIEW

2019 was an active year for enforcement of the European Union (EU) General Data Protection Regulation (GDPR), resulting in more than 25 major fines totaling nearly $475 million. The following highlights a few of the significant actions and lessons learned through 2019.

Largest Fine in 2019 Arises from Data Breach. British Airways is facing the largest potential GDPR-related fine to date, valued at approximately $228 million. The fine comes from the UK's data protection body, the Information Commissioner's Office (ICO), for a data breach that redirected visitors intending to visit British Airways' website to a fake website, which compromised the personal data of around 500,000 individuals. British Airways is appealing the fine.

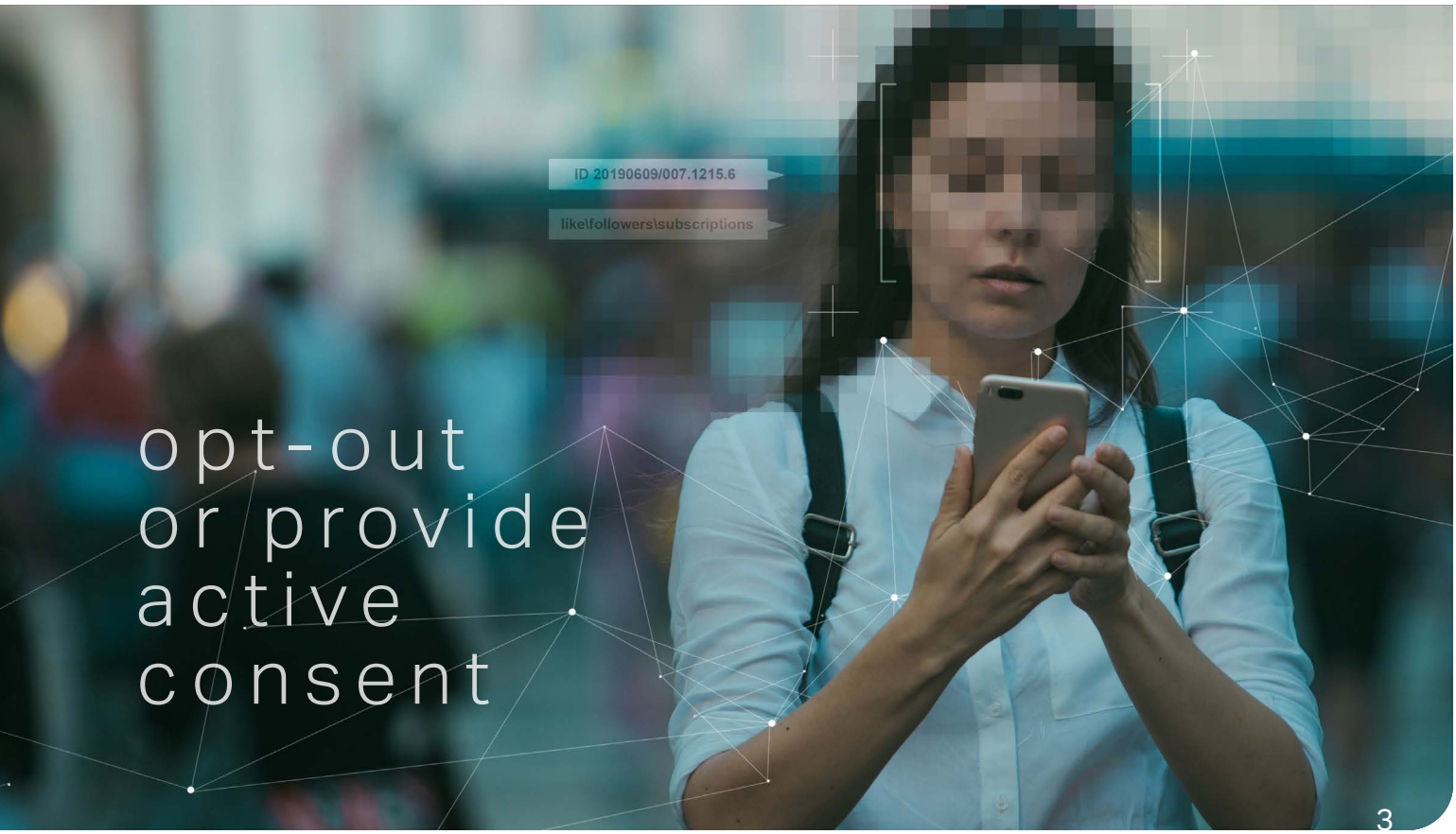
Transparency and Fairness are Key. Marking the first large fine in GDPR history, Google was fined approximately $56 million by French regulators (CNIL) for a number of GDPR violations, including a "lack of transparency, inadequate information and lack of valid consent." CNIL found that Google did not sufficiently inform users about how it was collecting personal data, and because individuals were not able to easily access all the information regarding Google's processing operations in a clear format, Google failed to obtain clear and informed consent. As a result, CNIL concluded that Google failed to establish a valid legal basis to process individuals' data.

Additional Guidance on Cookie Consents. The Court of Justice of the European Union (CJEU) delivered a judgment against the German company Planet 49, finding that pre-checked cookie consents are invalid. Users visiting Planet 49's website were presented with a pre-checked box consenting to Planet 49's use of cookies to track the user's behavior. The CJEU determined that, except as it relates to necessary cookies, pre-checked boxes authorizing the use of cookies and similar technologies do not constitute valid consent, which must be freely given, specific, informed and unambiguous. The CJEU also determined that cookie consents cannot be bundled with other data collection consents, and that users must be provided with information on the duration of the cookies and whether third parties will have access to the cookies.

"Training Purposes" Not a Lawful Basis for Recording Calls. In a case against a Denmark's largest telecommunications company, the Denmark Data Protection Authority (DPA) determined that consent is required when companies record customer calls. Although the company at issue purported to record its calls for the legitimate interest of training its employees and improving customer service, the DPA rejected this as a legal basis, particularly because there was no way for customers to opt-out of the recording. The DPA determined that the company could not record customer calls for training or any other purpose until it offered customers either the ability to opt-out of the recording or a way to provide active consent.

Failure to Respond to Rights of Data Subjects Can Result in Penalties. A number of data protection authorities penalized companies for failing to respond to individual rights requests, such as requests for erasure (Romania), requests to opt-out of advertising (France) and attempts by individuals to withdraw consent (Poland).

Looking Ahead. 2020 is already shaping up to be another active year for GDPR enforcement, and trends are emerging. Most notably, although many enforcement actions to-date involve data breaches, a greater number focus on violations of the GDPR's data processing principles, including lawfulness, fairness, transparency and data minimization. Thus, in addition to continually monitoring data security controls, those subject to GDPR should re-evaluate their internal practices and policies to ensure they are compliant with GDPR data processing principles more broadly.



BY NORBERT F. KUGELE

State Privacy Laws

IN REVIEW FOR 2019

In the absence of any comprehensive federal privacy laws, states continue to innovate and pass new privacy laws. These laws often impact companies without any physical presence in the enacting state, and many states follow the lead of trendsetting states, such as California.

CONSUMER PRIVACY LAWS

Preparation for the California Consumer Privacy Act (CCPA), which became effective on January 1, 2020, was 2019's biggest state privacy news. While the CCPA does not prohibit any particular uses of data, it requires detailed notices about data collection activities and gives California residents the right to request: (1) access to data collected about them; (2) deletion of certain of their data; and (3) an opt out from the sale of their data. Legislatures in at least nine other states are considering similar types of laws.

DATA BROKER LAWS

States are passing more laws to regulate data brokers, with the latest trend of laws focused on establishing a data broker registry. Vermont enacted the nation's first such law in 2018 that went into effect in 2019, and California enacted its own version in 2019, effective January 1, 2020.

Nevada and Maine, meanwhile, also passed laws in 2019 governing data brokers, but without establishing a registry. Nevada's law requires Internet website operators to provide a right to opt out of the sale of personal information (similar to the CCPA's opt-out requirement), while Maine's new law requires broadband providers to obtain express consent before selling a consumer's online information.

BIOMETRIC PRIVACY LAWS

Illinois, Texas and Washington have biometric privacy laws, but only Illinois gives its residents the right to bring lawsuits to enforce the law. In 2019, the Illinois Supreme Court issued a landmark decision stating that plaintiffs do not have to demonstrate actual harm in order to recover statutory damages ranging from $1,000 to $5,000 per violation of the laws' notice and consent requirements. As a result, more lawsuits are being filed under the Illinois law.

INTERNET OF THINGS

States are now passing laws regarding the security of connected devices. California passed the first law in 2018, but Oregon followed suit with its own law in 2019. Both laws went into effect on January 1, 2020.

INFORMATION SECURITY/DATA BREACH LAWS

States continue to pass cybersecurity-related legislation:

- At least 26 states now have data security laws that require businesses to maintain reasonable security procedures and practices—twice the number since 2016.
- All 50 states now have breach notification laws on the books, and states continue to revise these laws, broadening the types of information that falls within their scope.
- At least 35 states now also have data disposal laws that require proper disposal of personal information.
- Eight states, including Michigan, have now adopted the NAIC Insurance Data Security Model Law that requires insurance companies and other entities that are licensed by a state department of insurance to develop, implement and maintain an information security program based on a risk assessment.

BY SCOTT CARVO

MICHIGAN RULES OF

Professional Conduct

In 2012, the American Bar Association updated the Model Rules of Professional Conduct to require that lawyers be competent, not only in the law and its practice, but also in technology. In 2019, Michigan became the 37th state to formally adopt technology competence in its Model Rules of Professional Conduct. The adoption became effective January 1, 2020.

To adopt technology competence, Michigan updated the comments to Rule 1.1 of the Michigan Rules of Professional Conduct:

Maintaining Competence. To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education, including the knowledge and skills regarding existing and developing technology that are reasonably necessary to provide competent representation for the client in a particular matter. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances.

Michigan also amended Rule 1.6 regarding the confidentiality of information:

When transmitting a communication that contains confidential and/or privileged information relating to the representation of a client, the lawyer should take reasonable measures and act competently so that the confidential and/or privileged client information will not be revealed to unintended third parties.

The commentary in the order amending the Rules provides:

The amendments of the comments of MRPC 1.1 and MRPC 1.6 address a lawyer's obligation to maintain reasonable competence in relevant technology and ensure reasonable efforts to maintain confidentiality of documents.

2019 Case Studies

AND LESSONS LEARNED

BY KEN TREECE

Michael Kors, LLC v Ye, 2019 WL 1517552 (SDNY Apr 8, 2019)

The plaintiff sued the defendant for violations of trade dress infringement under the Lanham Act based on the defendant's marketing of products with a confusingly similar logo.

The defendant propounded numerous broad document requests concerning the plaintiff's use of its trade dress and trademark including business, strategic and market plans. The plaintiff objected to the requests based on their relevancy and scope, and the defendant moved to compel.

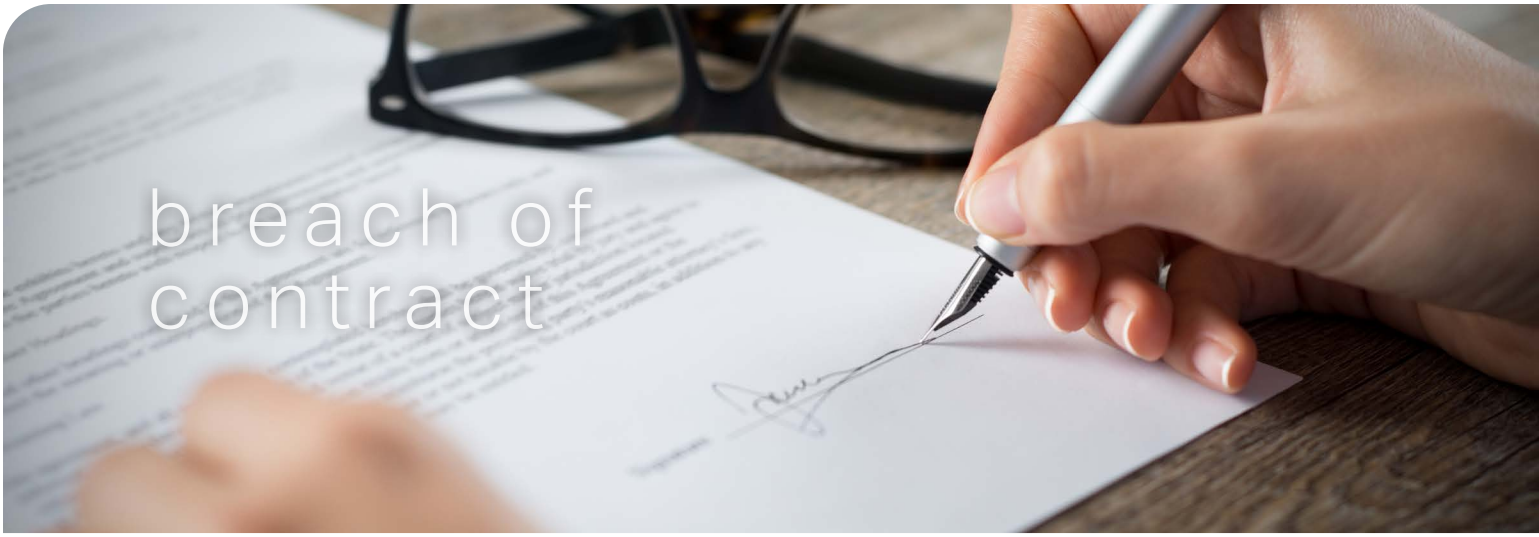
The court reviewed the document requests and found that they were "neither tailored to the needs of this case nor consistent with" the obligation under Rule 34 to "describe with reasonably particularity each item or category" of documents and information sought.

The court also agreed with the plaintiff's contention that the document requests were disproportional to the needs of the case given that the potential relief obtainable from the sale of the defendant's products was small—roughly fifty-thousand dollars maximum. Given the amount at stake, the court stated that "the discovery sought by Defendant would no doubt result in attorneys' fees and expenses on both sides exceeding the damages that could be obtained in this case. When faced with Plaintiff's objection, Defendant should have narrowed its requests to reach a compromise with Plaintiff on the scope of the documents to be produced."

While finding that some of the plaintiff's document requests were warranted, the court ordered the plaintiff to amend her requests to make them proportional to the needs of the case given the damages at stake.

In a case with relatively low damages, effective advocacy must be balanced against the need to keep litigation costs down, by narrowing discovery requests, seeking compromise over objections, and meeting and conferring in good faith to resolve disputes and avoid court intervention – "all critical obligations under Rules 1 and 26."

Lesson Learned



breach of contract

FCA US LLC v Bullock, 2019 WL 258169 (ED Mich Jan 18, 2019)

Before starting her own law firm, the defendant worked for two law firms at which she represented the plaintiff in breach of warranty cases. The defendant filed a breach of warranty claim on behalf of one of the plaintiff's customers. This led to the plaintiff suing the defendant for breach of contract, breach of fiduciary duty, trade secret misappropriation and violation of federal trade secret law.

A forensic examination of a laptop computer used by the defendant while working on behalf of the plaintiff revealed that she had connected ten USB storage drives to the computer and created several folders entitled "Helpful Info," "Lemon Law Cases," "My Business" and "Releases." The same day she uninstalled Dropbox from the computer and emptied her recycle bin.

In response to the plaintiff's discovery requests, the defendant produced over 1,300 electronic records that she represented were all of the "all documents relating in any manner to [her] representation of FCA US that are in her custody and control[.]" The plaintiff moved for an order seeking a forensic examination of the defendant's business/personal computers and cell phones. The plaintiff argued that it was not bound by the defendant's representations given her misappropriation of the plaintiff's documents. The court disagreed.

The fact that the plaintiff alleged that the defendant did something wrong did not give the plaintiff "free reign" to conduct forensic imaging of her computers and cell phone. Without contrary evidence, the defendant's representation that she had turned over all responsive, nonprivileged documents precluded such an intrusion both on proportionality and privacy grounds. However, the defendant would be required to turn over any responsive, deleted files that could be recovered from her computers and cell phone as those were within the scope of permissible discovery.

Without evidence of wrong-doing, proportionality and privacy concerns may preclude the forensic examination of a party's electronic devices—even where those devices are central to the causes of action. However, the party must still produce recoverable deleted files from those devices if responsive and nonprivileged.

Lesson Learned

Karsch v Blink Health Ltd., WL 2708125 (SDNY June 20, 2019)

Karsch, the plaintiff who is a hedge fund manager, sued the defendant, Blink Health Ltd., for failure to convert his repayable convertible note into a five-percent equity stake in the defendant. Twenty-three months prior to filing suit, Karsch sent a written demand letter via his counsel to the defendant. The letter asserted the plaintiff's right to an equity stake in the defendant, accusing the defendant of "securities fraud, common law fraud, breach of fiduciary duty, and breach of contract." If the defendant failed to comply, the letter concluded that the plaintiff would have "'no alternative but to reserve all his legal rights and remedies.'"

Prior to filing litigation, but after sending the demand letter, the plaintiff destroyed his company's email accounts/file server after making a copy. The copy, however, did not contain any files from his company's email accounts for several key custodians. The destruction of the hard drive and the existence of the deficient copy were not disclosed until after the defendant filed document requests and motions to compel production. Upon learning of the plaintiff's actions, the defendant moved for sanctions under Rule 37(e) seeking dismissal of the plaintiff's claims.

In support of its motion, the defendant argued that the plaintiff's duty to preserve was triggered on the date he sent the demand letter to the defendants. The court agreed. "Although [plaintiff] did not file the threatened legal action for another 23 months, the timing of the lawsuit was wholly within his control, and there is nothing in the record to suggest that his threat was not seriously intended when made. Moreover, neither party disputes that the [company server] contained information relevant to the disputes at issue in this action, and that [plaintiff] knew or should have known that it did."

Because the plaintiff had a plausible explanation for the destruction of the email server—not disputed by the defendant—the court declined to find that the plaintiff had an "intent to deprive" the defendant of information on the server. Therefore, it denied the defendant's request to dismiss the plaintiff's claims. However, it did find sufficient prejudice to permit the defendant to present evidence concerning the loss and potential relevance of the information on the email server to the jury along with an instruction to the jury to consider the evidence in making its decision.

Lesson Learned

The duty to preserve evidence does not depend on the time of filing of a lawsuit. A demand letter, depending on its terms, may trigger the duty well in advance of filing. Putative plaintiffs and defendants need to carefully consider pre-suit actions and their potential for triggering the duty to preserve evidence.

BY NATHAN STEED

SIGNIFICANT DATA BREACHES OF 2019

Verifications.io 1

Individuals Affected: 800,000,000 – 1,000,000,000

Cause: An unsecured database was stored on an unsecured server.

Type of Data: Email addresses, phone numbers, birthdates, mortgage amounts and interest rates, social media account data and credit score data

Fallout: Verifications.io shut down its website.

First American Financial Corp. 2

Individuals Affected: 800,000,000 records

Cause: Files were stored on First American's website without any protection or safeguards

Type of Data: Names, addresses, birthdates, bank account numbers, bank statements, social security numbers, driver's licenses, mortgage records and tax documents

Fallout: Documents containing extremely sensitive information were stored online, without any security measures. First American acknowledged the "design defect" and shut down the ability to access the information. In August 2019, it was reported the Securities and Exchange Commission was investigating the incident.

Facebook (1) 3

Individuals Affected: 600,000,000

Cause: Facebook internally stored information in a readable format.

Type of Data: Passwords

Fallout: Facebook internally stored the passwords of users in plaintext format. These passwords were accessible to nearly 20,000 Facebook employees. Facebook further discovered Instagram passwords of millions of users were also being internally stored in a readable format.

Facebook (2) 4

Individuals Affected: 540,000,000

Cause: Third-party app developers uploaded records of Facebook users to Amazon's cloud servers. User data was left exposed on the public web.

Type of Data: Account names, user IDs, phone numbers, gender, country, user comments and reactions to posts

Fallout: Bloomberg alerted Facebook of the breach. Facebook then contacted Amazon to work on taking the data off Amazon's servers.

Zynga 5

Individuals Affected:
170,000,000 – 200,000,000

Cause: Hackers illegally breached Zynga's system.

Type of Data: Names, emails, login IDs, passwords, phone numbers and Facebook IDs

Fallout: Zynga acknowledged player account information, specifically for players of Draw Something and Words With Friends, may have been accessed by hackers and that there was an investigation into the event.

Dubsmash 6

Individuals Affected: 162,000,000

Cause: Details of over 600 million accounts were stolen from 16 hacked websites and put up for sale on the dark web. Dubsmash was one of the affected websites.

Type of Data: User IDs, passwords, email addresses, names, country and language

Fallout: The Dubsmash accounts were breached in December 2018, but the user information was put up for sale in February 2019.

Canaya 7

Individuals Affected: 139,000,000

Cause: A hacker gained unauthorized access to user information during a "malicious cyber-attack."

Type of Data: Names, usernames, email addresses, country, salted and hashed passwords

Fallout: On May 24, 2019, Canaya noticed the malicious activity and stopped the incident while occurring. In response, Canaya has worked with the FBI and other cyber experts and authorities. On January 11, 2020, a list of approximately 4 million accounts and passwords was shared online.

Capital One 8

Individuals Affected: 106,000,000

Cause: A hacker gained unauthorized access to the Capital One server.

Type of Data: Names, addresses, birthdates, credit scores, social security numbers and bank account numbers

Fallout: Capital One acknowledged the breach and worked with federal law enforcement. The hacker was captured by the FBI. Capital One notified affected individuals, providing them free credit monitoring and identity protection.

Evite 9

Individuals Affected: 100,000,000

Cause: Malicious activity was traced back to February 2019, where a hacker stole an "inactive data storage file" containing user information from 2013 and before.

Type of Data: Names, usernames, email addresses, passwords, birthdates, phone numbers and addresses

Fallout: A hacker allegedly put up the sale of the breached personal information. Subsequently, Evite published an FAQ page on their website giving insight into the data breach.

Door Dash 10

Individuals Affected: 4,900,000

Cause: An unauthorized third party accessed data on May 4, 2019.

Type of Data: Names, email addresses, delivery addresses, order histories, phone numbers, passwords, the last four digits of payment card numbers, the last four digits of bank account numbers and driver's license numbers

Fallout: The breach affected consumers, Door Dash drivers and merchants who joined the Door Dash platform on or before April 5, 2018. Users who joined after April 5, 2018 were not impacted.

Warner Norcross + Judd

wnj.com