Westlaw Journal
WHITE-COLLAR CRIME

Litigation News and Analysis • Legislation • Regulation • Expert Commentary

VOLUME 32, ISSUE 8 / APRIL 2018

WHAT'S INSIDE

EMOLUMENTS CLAUSE

U.S. judge refuses to toss suit against Trump on foreign payments

(Reuters) – President Donald Trump's legal troubles deepened March 28 as a federal judge refused to throw out a lawsuit accusing him of flouting constitutional safeguards against corruption by maintaining ownership of his business empire while in office.

District of Columbia et al. v. Trump, No. 17-1596, 2018 WL 1516306 (D.C. Mar. 28, 2018).

U.S. District Judge Peter Messitte in Greenbelt, Maryland, allowed the lawsuit filed by Maryland and District of Columbia to proceed, rejecting a U.S. Justice Department request that it be dismissed. The judge, however, narrowed the claims to include only those involving the Trump International Hotel in Washington and not Trump's businesses outside of the U.S. capital.

U.S. President Donald Trump REUTERS/Kevin Lamarque

A U.S. judge in Manhattan in December threw out a similar lawsuit against Trump brought by another group of plaintiffs.

Both lawsuits accused Trump of violating the U.S. Constitution's "emoluments" provisions designed to prevent corruption and foreign influence. One bars U.S. officials from accepting gifts or other emoluments from foreign governments without congressional approval. The other forbids the president from receiving emoluments from individual states.

If the lawsuit presided over by Judge Messitte continues to move forward, the plaintiffs have indicated they would seek a number of documents related to the president, including his tax returns, which Trump has refused to release.

CONTINUED ON PAGE 5

EXPERT ANALYSIS

The Justice Department's False Claims Act memorandum: An invitation for advocacy

John F. Wood and Eric S. Parnes of Hughes Hubbard & Reed discuss a new Justice Department memo and analyze what it could mean for False Claims Act suits.

SEE PAGE 8

42089825

Westlaw Journal White-Collar Crime

Published since April 1987

Director: Nadia Abadir

Editors:
Phyllis Lipka Skupien, Esq.
Phyllis.Skupien@thomsonreuters.com

Kevin M. McVeigh, Esq.

Desk Editors:
Jennifer McCreary, Elena Neuzil, Katie Pasek, Sydney Pendleton, Abbie Sarfo, Maggie Tacheny

Graphic Designers:
Nancy A. Dubin, Ramona Hunter

Westlaw Journal White-Collar Crime
(ISSN 2155-5923) is published monthly by Thomson Reuters.

Thomson Reuters
175 Strafford Avenue, Suite 140
Wayne, PA 19087
877-595-0449
Fax: 800-220-1640
www.westlaw.com
Customer service: 800-328-4880
For more information, or to subscribe, please call 800-328-9352 or visit legalsolutions.thomsonreuters.com.

TABLE OF CONTENTS

The looming impact of the General Data Protection Regulation on e-discovery

By Debbie Reynolds
EimerStahl Discovery Solutions

The legal world is bracing for the impact that the General Data Protection Regulation will have on the technologies and best practices that are now standards in e-discovery.

The GDPR, a European Union law that was passed in 2016 and fully takes effect May 25, protects the data privacy rights of all people in the EU, including noncitizens and visitors, also known as "data subjects," regardless of where their data resides. (The text of the law is available at https://bit.ly/1TtxgbB.)

In addition to being an astonishing law in terms of its territorial reach, the GDPR also carries severe financial penalties for violations. For example, if the GDPR is violated, any company that provides goods or services to or maintains personal data of EU data subjects could be fined up to 4 percent of their organizations' worldwide gross annual revenue or 20 million pounds, whichever is greater.

E-discovery as a discipline has developed in step with the rise of the digital age since the 1990s, and it continues to evolve and grow because of the increased technological sophistication required to defensibly manage emerging data types and ever-growing volumes of electronic evidence in legal matters. In e-discovery, it has become more common than ever for cases in the U.S. to require the handling of data from all over the world.

The rise of the internet has enabled companies to do business globally, and even in countries where they have no physical presence, because technology allows data to flow rapidly and easily across international borders.

The increasing varieties of electronic data generated by individuals from emails, smartphones, websites, social media platforms, and web-connected devices like cloud-based voice command assistants and thermostats are creating vast oceans of private data that may be required as part of legal e-discovery.

Dealing with these new data types in e-discovery is a constant challenge, but laws like the GDPR raise new concerns and create new obligations to protect and manage private data in legal matters.

Due to the stringent EU data privacy requirements of the GDPR, the legal world will be forced to create new technologies, workflows and best practices to prepare for proactive data privacy management and ongoing GDPR compliance in e-discovery.

The GDPR mandates e-discovery changes that will require a fundamental reimagining of our current ideas about how best to manage legal data during e-discovery and which approaches will ensure compliance with data privacy rules.

The GDPR will be a game changer with respect to how we approach e-discovery; it will alter how we plan and manage data privacy on legal matters going forward. The critical areas of the GDPR that will most impact e-discovery will be consent, pseudonymization, and privacy by design.

CONSENT

The GDPR gives EU data subjects legal control and individual redress rights related to access and use of their data anywhere in the world.

The GDPR gives EU data subjects legal control and individual redress rights related to access and use of their data anywhere in the world.

Consent under the GDPR includes the right of data subjects to:

- Provide approval for the use of their data.
- Be informed about how their data will be used and for what purpose.
- Access any of their data that is being used upon request.
- Revoke consent at any time.
- Have their data returned to them.
- Have their data deleted upon request.

In e-discovery, data collected from people in the U.S. for legal matters often will not require individual consent. This differs from the rights of EU data subjects under the GDPR. For example, a U.S. employer essentially owns the rights of all electronic data created in the workplace, and individual consent is not required for an employer to use this data for any purpose, including in legal matters.

Debbie Reynolds, the director of **EimerStahl Discovery Solutions**, an affiliate of law firm **Eimer Stahl LLP**, advises Fortune 500 companies on data privacy and the management of electronic evidence in high-stakes litigation. Reynolds also is an adjunct professor at Georgetown University, a guest lecturer for various U.S. law schools, a published author and a speaker on the impact of global data privacy rules in legal matters. She can be reached at dreynolds@eimerstahl.com.

In the EU, an individual's privacy is considered a fundamental human right, while in the U.S. the focus on privacy protections is based on the types of personal or private data being used, such as health or credit information, in combination with an individual's name.

Currently, in the early stages of an e-discovery matter and often in anticipation of litigation, individuals may be provided a litigation hold notice, which details the need to maintain certain documents that may be needed for a legal case.

An ideal GDPR data workflow to manage consent during e-discovery would be to prepare a data privacy notice, much like a litigation hold notice, for EU data subjects. The notice should explain what data is needed and why before explicit consent it sought.

EU data subjects can consent to some uses of data and not others. As a result, additional documentation will be needed to detail the scope of the data provided for the matter by data subjects and reasons for any gaps in the information provided for legal purposes.

Also, EU data subjects can revoke consent at any time. The revocation of consent must also be documented, and data must be deleted or returned to the data subject upon request.

To comply with the GDPR, the consent of EU data subjects must be obtained, and data subjects must be informed of what is being consented to, before the data can be used for legal matters. Also, data cannot be used for longer than it needs to be used for approved purposes. If it is needed for other purposes, consent must be separately obtained.

For example, in legal matters, there is a trend toward e-discovery data federation, which is the aggregation, retention or re-use of data from one matter in subsequent legal matters as a way to save on the costs of performing new e-discovery.

In the GDPR context, e-discovery data federation may be difficult to utilize if it requires an EU data subject's consent to data use that exceeds its initial purpose or period of initial consensual use. So, if data is needed in the future from the same EU data subject, it may need to be deleted after its initial consensual use and requested again. In addition, new consent may be needed for any further legal e-discovery purposes.

E-discovery is fundamentally a one-way, forward-moving process, where large volumes of data are captured, culled and reduced as it moves downstream until the most relevant data is distilled from the process to be used in legal matters.

This traditional e-discovery workflow is not currently designed to move backward in an attempt to potentially remove previously used EU data subject documents from any phases of an active legal data process.

The GDPR will force technology and workflow changes that will better enable the handling of consent in legal matters, especially as it pertains to instances where an EU data subject revokes consent and data must be removed from an e-discovery workflow process.

Providing transparency to EU data subjects if requested during e-discovery could be a logistical challenge but may be achieved, in part, with existing technologies and augmented data workflows.

For example, if a data subject asks to see their data during an e-discovery process, this may be accomplished with current technologies. To grant EU data subjects access to their data, a restricted e-discovery platform account may be used to provide an EU data subject viewing privileges.

This workflow might be accomplished similarly to how expert witnesses are granted access to specific documents needed on a legal matter. However, if the data provided to one data subject also contains information from other EU data subjects, this may create an additional technological and workflow challenge to obscure one data subject's personal information from that of another EU data subject.

PSEUDONYMIZATION

Pseudonymization is a data privacy protection method recommended throughout the GDPR as a preferred way to safeguard the identity of an EU data subject by substituting pseudonyms for personally identifiable information. In e-discovery, it is customary that all data used in a legal case be associated with the name of the individual from whom the data was collected.

At the beginning of any e-discovery project involving EU data subjects, it may now be necessary to substitute pseudonyms for custodians' real identities. Also, the data subjects' identities may need to be pseudonymized throughout the documents or obscured in some way (such as by using redactions) to comply with the GDPR.

> To complicate pseudonymization further, the definition of personally identifiable information in the EU is far broader than commonly defined in the U.S.

The need to pseudonymize will create an additional layer of search in documents to locate variations of individuals' names to be pseudonymized. It will require new technological features, which have yet to be developed, in e-discovery software tools.

To complicate the challenge of pseudonymization further, "personally identifiable information" is defined much more broadly in the EU than it is commonly defined in the U.S.

In the U.S., individually recognizable private information about an individual may include details like someone's name when shown together with their Social Security number or banking information.

However, the EU recognizes in the GDPR that several data points that create a combination of information about an EU data subject could make any individual identifiable. This information, such as a data subject's social activities, or even club memberships, in combination with their names, may also need to be obscured.

Some current e-discovery tools can redact or obscure specific patterned information in legal documents, such as Social Security numbers and credit card numbers. However, e-discovery tools have not yet developed the ability to automate the mechanics of pseudonymization on additional information that may make any EU data subject personally identifiable.

As a result, pseudonymization that requires more subjective analysis and manual redaction will have to be accomplished

through additional legal team time and significant new document review workflows that do not currently exist in e-discovery projects.

PRIVACY BY DESIGN

Privacy by design is probably the most daunting of all GRPR requirements. In essence, the GDPR ascribes to the idea that technology and data management workflows should be designed in a way that makes it easier to achieve the types of data privacy protections that the regulation requires.

A recent case from Germany provides an example of the challenges software companies will face related to the GDPR and privacy by design. A German court ruled in January that Facebook violated current German data protection laws.

The German court agreed with the Federation of German Consumer Organizations that Facebook unlawfully required members to use their real names. It further deemed unlawful Facebook's practice of presenting members with preselected opt-in data use policy checkboxes that allowed it to use their data for multiple purposes.

Although the GDPR has not yet been fully enforced, privacy by design in the EU has been and will continue to be a pressing issue for software developers to navigate in years to come — especially with the more stringent GDPR penalties starting in May 2018.

When the GDPR has taken effect, many software companies will be watching EU enforcement actions to interpret how best to achieve privacy by design and to have a better understanding of what the EU considers unacceptable privacy design going forward. Similarly, e-discovery tools must soon be able to adapt to and manage information of EU data subjects when their data is involved in legal matters.

As a result, e-discovery technologies will likely implement privacy-ready design into their software soon. Also, as more cases include data from different countries, e-discovery and legal professionals will be developing workflow suggestions and urging technology companies to create automated ways to track and monitor GDPR compliance in the future. WJ

Trump

CONTINUED FROM PAGE 1

The lawsuit, filed last June, said the Republican president has failed to disentangle himself from his hotels and other businesses, making him vulnerable to inducements by officials seeking to curry favor.

Maryland Attorney General Brian Frosh, a Democrat, said in an interview he was pleased with the judge's action.

"It demonstrates that Donald Trump is not above the law, that he like every other federal employee is governed by the emoluments clause, the original anti-corruption law of the United States. And we intend to hold him accountable," Frosh said.

Justice Department spokeswoman Kerri Kupec said, "As we argued, we believe this case should be dismissed, and we will continue to defend the president in court."

As part of the suit, the District of Columbia and Maryland said their local residents who compete with Trump's businesses like Trump International Hotel are harmed by decreased patronage, wages and tips.

Trump's attorneys said such claims were speculative and raised doubts that any harm to competition could be traced directly to Trump's status as president.

Judge Messitte rejected that view, saying the plaintiffs' allegations were sufficient to allow the case to proceed.

"Their allegation is bolstered by explicit statements from certain foreign government officials indicating that they are clearly choosing to stay at the president's hotel, because, as one representative of a foreign government has stated, they want him to know 'I love your new hotel,'" the judge wrote.

Judge Messitte also noted that since the 2016 presidential election, "foreign governments have indisputably transferred business from the Four Seasons and Ritz Carlton hotels in the District to the president's hotel."

LEGAL WOES

Trump's legal woes are mounting. His lead lawyer in the intensifying special counsel investigation into Russia's role in the 2016 presidential election resigned last week.

A New York state judge March 20 allowed a defamation lawsuit by a woman who accused Trump of sexually harassing her after she appeared on his former reality TV show to proceed.

He also is facing lawsuits from adult film actress Stormy Daniels and former Playboy model Karen McDougal arising from affairs they said they had with the president.

Trump, a wealthy real estate developer who as president regularly visits his own hotels, resorts and golf clubs, has ceded day-to-day control of his businesses to his sons. Critics have said that is not a sufficient safeguard.

This undermines democracy, the suit said, because Americans cannot be sure if Trump is acting in their best interest, or "international and domestic business dealings in which President Trump's personal fortune is at stake."

The suit said Trump had received millions of dollars in payments and benefits through leases of Trump properties held by foreign government entities, the purchase of condominiums in Trump properties, as well as hotel accommodations, restaurant purchases and the use of venues for events by foreign governments and diplomats.

Judge Messitte's action contrasts with that of U.S. District Judge George Daniels in Manhattan, who threw out the similar case filed by a nonprofit watchdog group, a hotel owner, a hotel events booker and a restaurant trade group.

Judge Daniels said the claims were speculative and that the U.S. Congress was the proper place to hold the president to account. WJ

(Reporting by Andrew Chung; editing by Will Dunham)

Related Filings:
Opinion: 2018 WL 1516306

See Document Section A (P. 21) for the opinion.