KRAMER LEVIN
KRAMER LEVIN NAFTALIS & FRANKEL LLP

Cybersecurity, Privacy and Data Protection
UPDATE

January 14, 2016

2015 — A Year in Review

As the close of 2015 marks a historic year for cybersecurity jurisprudence and lawmaking, this Update highlights key legal and policy developments in cybersecurity law that may impact important trends for 2016 and beyond. In addition to the passage of the Cybersecurity Information Sharing Act ("CISA") in the final days of 2015, federal and state regulators were active throughout the year in providing guidance to companies and individuals regarding data security practices. Key court rulings concerning the validity of the Safe Harbor agreement between the United States and the European Union as well as the FTC's enforcement power reshaped the cybersecurity landscape. Important rulings on law enforcement's ability to access and use electronically stored information are expected in the coming year. These decisions will no doubt impact the trajectory of cybersecurity and privacy issues in 2016.

Beyond Safe Harbor

In a landmark decision issued in October, the European Court of Justice — the highest court in the European Union — struck down the "Safe Harbor" data-transfer agreement between the EU and the United States. The Court's decision in *Maximilian Schrems v. Data Protection Commissioner* put pressure on the ongoing U.S.-EU negotiations to produce a new data-sharing agreement, which is expected to be completed in January 2016.

In December, the EU member states agreed to a new set of data protection rules called the General Data Protection Regulation ("GDPR"). Some of the key features of the new GDPR include the so-called "right to be forgotten"; a right to data portability that enables data subjects to transfer their personal data between services; mandatory data protection officers for the public sector, for large private enterprises, and in instances where core activities of a controller or processor consist of data processing requiring regular and systematic monitoring; and required notification to relevant national supervisory authority in the event of a serious data breach. Each member state will have two years to incorporate the provisions of the GDPR — which will come into force in 2018 — into their national laws. The GDPR will apply to any companies handling the data of EU citizens regardless of the location of the company. Liability will extend not only to data controllers (i.e., the companies deciding how and why to collect data) but also to service providers. The new data protection regime will carry heavy fines for rules violations.

Once implemented, the GDPR will have a significant impact on U.S. companies. Under the "right to be forgotten" rule, EU citizens will be able to request that data providers delete their data when there is no legitimate reason for retaining it. This rule will affect the business models of various companies that rely on consumer data. Companies will also have to expend significant resources to ensure compliance with various new rules. The GDPR specifies that companies may be fined up to 4 percent of their global revenue for violating data protection rules — an amount that could range in the billions of dollars for very large companies.

For more information on the *Schrems* decision, click **here**.

The FTC's Authority to Enforce Data Security

In August, the United States Court of Appeals for the Third Circuit unanimously affirmed the district court's

ruling in *FTC v. Wyndham Worldwide Corp.* that the Federal Trade Commission ("FTC") has the authority to regulate a company's data security practices under Section 5 of the FTC Act. The FTC Act broadly prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC suit, filed in 2012, stemmed from three separate data breaches between April 2008 and January 2010 that exposed over 600,000 Wyndham customers' payment card information to hackers.

In December, Wyndham reached a settlement with the FTC in which the company agreed to establish an information security program designed to protect customer and cardholder data. The company also agreed to conduct annual information security audits to ensure that it is in compliance with the Payment Card Industry Data Security Standard. Further, the company committed to enacting additional security measures, including creating firewalls between its corporate servers and those of its franchisees.

For more information on the *Wyndham* case, click **here**.

An Active Year for Federal and State Regulators

Throughout 2015, federal and state regulators continued to stress the importance of cybersecurity and the need for companies and organizations to have adequate protections against — and responses to — data breaches. In addition to conducting in-depth surveys of these threats, these regulators have also released an abundance of guidance providing recommendations on how corporate cybersecurity practices should be handled.

In April, for example, the U.S. Securities and Exchange Commission's ("SEC") Division of Investment Management released guidance to registered investment companies and advisors, highlighting cybersecurity as an "important issue." The guidance was designed to aid these companies and advisors in their efforts to both understand the nature and impact of cybersecurity threats and design and implement a strategy to prevent, detect and respond to these threats. In December, the SEC also solicited comment on new cybersecurity rules that, among other things, would require registered transfer agents to implement cybersecurity guidelines that would govern how the agents safeguard certain sensitive data and personally identifiable information.

In September, the SEC reached a settlement in an enforcement action against a registered investment adviser that failed to adopt proper cybersecurity protocols. According to the SEC, an unauthorized intruder gained access to the adviser's server, which contained the sensitive personally identifiable information of more than 100,000 individuals. The SEC determined that the adviser had violated the Commission's Safeguards Rule by failing to adopt written policies and procedures reasonably designed to safeguard its clients' personally identifiable information. The adviser agreed to adopt various cybersecurity measures and pay a civil penalty of $75,000 to the SEC.

Additionally, in November, the New York Department of Financial Services ("DFS") released a letter outlining proposed cybersecurity regulations for the financial institutions it regulates. In addition to initiating a dialogue among various state and federal regulators, the DFS intended the proposals to bolster cybersecurity defenses within the financial sector by requiring mandatory quarterly audits, multifactor authentication, comprehensive written policies and procedures, and more stringent requirements for cyber incident notification and the management of third-party service providers.

For more information on these regulations, click **here**.
For more information on these surveys, click **here**.

Key Data Security Cases

In September, a three-judge panel of the United States Court of Appeals for the Second Circuit heard arguments in Microsoft's appeal of the district court's ruling in *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.* The appeal concerned a 2013 search warrant that the Department of Justice served under the Electronic Communications Privacy Act ("ECPA") directing Microsoft to seize a suspect's digital documents. Microsoft objected to turning over certain data that it had stored in a data center in Dublin, Ireland. In April 2014, S.D.N.Y. Magistrate Judge Francis, who issued the warrant, denied Microsoft's motion to quash the warrant with respect to the data stored in Ireland. In July, Chief Judge Preska affirmed Judge Francis's ruling and held Microsoft in contempt for refusing to comply with the warrant. Microsoft subsequently appealed. The Second Circuit's decision will address the significant question of whether a U.S. law enforcement agency can compel a U.S. company to disclose electronic data that it has stored abroad.

In another likely precedent-setting case concerning law enforcement's ability to access electronically stored information, the Second Circuit, sitting *en banc*, also heard arguments last September in *United States v. Ganias*. In 2003, pursuant to a search warrant, the government seized and cloned three computer hard drives belonging to Stavros Ganias. At the time, the government had not been investigating Ganias and instead had obtained the warrant to acquire information responsive to an investigation of government contractors for which Ganias had performed accounting services. The government did not return the nonresponsive material, however, and instead retained the full cloned hard drives. Nearly two and a half years later, the government obtained an additional warrant to search Ganias' records for evidence of tax evasion, but — unable to access the records from Ganias — it returned to the hard drives cloned years earlier to conduct the search. The evidence obtained from this warrant was used to convict Ganias of tax evasion. Ganias appealed his conviction, arguing that the government's conduct violated his Fourth Amendment protection to be free from unreasonable searches and seizures. A Second Circuit panel agreed, vacating his sentence and ruling that the government's conduct had in fact violated the Fourth Amendment. The *en banc* ruling is expected to address whether the government's retention and subsequent search of the nonresponsive data violated Ganias' Fourth Amendment rights. Prior to the *en banc* hearing, Kramer Levin submitted an amicus brief on behalf of the Center for Constitutional Rights in support of Ganias.

In March, Target agreed to pay $10 million to settle a consumer class action lawsuit stemming from a 2013 data breach that affected at least 40 million credit cards. The settlement followed a Minnesota federal judge's December 2014 ruling that rejected Target's argument that the consumers could not establish any injury and allowed the case to proceed. Just last week, a different judge in the same court dismissed a class action brought by SuperValu shoppers alleging that they were harmed after hackers accessed the supermarket chain's payment systems. In this case, the judge found that the consumers' claims of possible future injuries were too speculative to give them standing. The judge distinguished this case from the Target class action, stressing that the Target consumers alleged facts reasonably suggesting that hackers had succeeded in stealing their data and using it for fraud. The SuperValu plaintiffs, on the other hand, identified only a single unauthorized charge affecting one person.

For more information on the *Microsoft* case, click **here**.
For more information on the *Ganias* case, click **here**.

If you have any questions or need additional information about this alert, please feel free to contact the authors below or any one of your Kramer Levin attorney contacts.

Samantha V. Ettari
E-Discovery Counsel
settari@kramerlevin.com
212.715.9395

Alan R. Friedman
Partner
afriedman@kramerlevin.com
212.715.9300

Arielle Warshall Katz
Associate
akatz@kramerlevin.com
212.715.9368

Erica D. Klein
Partner
eklein@kramerlevin.com
212.715.9205

Daniel Lennard
Associate
dlennard@kramerlevin.com
212.715.9396

Harold Robinson
Associate
hrobinson@kramerlevin.com
212.715.9547

Our Cybersecurity and Data Protection Practice

Kramer Levin's Cybersecurity, Privacy and Data Protection Practice is an interdisciplinary team of attorneys from the United States and Europe with litigation, regulatory, technology and compliance experience. Our team advises on the most cutting-edge technology and data security issues at every stage, representing clients ranging from entrepreneurial startup entities to multinational Fortune 100 companies in a variety of sectors. We help clients navigate the rapidly evolving and challenging privacy law landscape by providing practical strategies to identify and manage the legal and reputational risks associated with these emerging and dynamic issues. Many of our attorneys have served in senior positions in government, as prosecutors and trial attorneys, as counsel for congressional committees and as advisors in the development of EU law. **View more**.

OUR TEAM >