June 2015

the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, INTERNET ADVERTISING, MARKETING AND INFORMATION SERVICES LAW AND POLICY

VENABLE SNAPSHOT

Received *Chambers USA* "Award of Excellence" for the top privacy practice in the United States

Named Two of the "Top 25 Privacy Experts" by *Computerworld*

"Winning particular plaudits" for "sophisticated enforcement work" – *Chambers and Partners*

Recognized by *Chambers Global* and the *Legal 500* as a top law firm for its outstanding data protection and privacy practice

ISSUE EDITORS:

Stuart P. Ingis
singis@Venable.com

Michael A. Signorelli
masignorelli@Venable.com

Ariel S. Wolf
awolf@Venable.com

ADDITIONAL CONTRIBUTORS:

Emilio W. Cividanes
ecividanes@Venable.com

David L. Strickland
dlstrickland@Venable.com

Julia Kernochan Tama
jktama@Venable.com

Kelly A. DeMarchis
kademarchis@Venable.com

Tara Sugiyama Potashnik
tspotashnik@Venable.com

Matt H. MacKenzie
mhmackenzie@Venable.com

Rob L. Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Chan D. Lieu
cdlieu@Venable.com

Introduction:

In this issue, we review several announcements in the regulatory space, including the Federal Communications Commission's initial guidance on enforcement of its Open Internet Order against broadband Internet access service providers, as well as the release of a draft "Privacy Risk Management Framework" by the National Institute of Standards and Technology. State legislatures across the country were active in the privacy space, with California alone passing and introducing several new measures. Also discussed in the June issue of the Download are key marketplace developments, including the dispensation of customer data in a bankruptcy action. Finally, we review regulatory and enforcement developments in the EU.

In this Issue:

Heard on the Hill

Anti-spoofing Bill Introduced in the House

On June 4, 2015, Representatives Grace Meng (D-NY), Joe Barton (R-TX), and Leonard Lance (R-NJ) introduced H.R.2669, the "Anti-Spoofing Act of 2015." H.R.2669 would amend 227(e) of title 47 of the U.S. Code, which prohibits "knowingly transmitting misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."[1] The bill would expand current law to prohibit so-called "spoofing" by anyone outside of the U.S. if the recipient is within the U.S. The bill also would add text messaging and Voice over Internet Protocol (VoIP) to the services covered by the law's prohibition.

The Federal Communications Commission ("FCC") would be required to issue regulations implementing the amendments to law made by the legislation within eighteen (18) months after enactment, and the new law would take effect six (6) months after the FCC's regulations are promulgated. H.R.2669 was referred to the House Energy and Commerce Committee, where it awaits further action. The sponsors introduced a similar version of the legislation in the previous session of Congress, and the measure ultimately passed the House of Representatives by voice vote on September 9, 2014.

Around the Agencies

Federal Trade Commission Updates FAQs on Endorsement Guides

The FTC recently updated its Frequently Asked Questions ("FAQ") page regarding its Endorsement Guides to provide guidance to endorsers and marketers regarding their disclosure obligations on new online platforms, such as social media.

The updated FAQs caution advertisers against soliciting endorsements on social networking platforms or through features that do not allow for a clear and conspicuous disclosure of the relationship between the endorser and the marketer. The FTC also reiterated its prior guidance that advertisers should use clear and unambiguous language when disclosing its relationship with an endorser. According to the FTC, such disclosures must be close to the claim to which they relate; they should not be hidden in footnotes or hyperlinks; they should be easy to find and easy to read; and if made during an audio advertisement, they must be presented in a manner that facilitates the consumers' comprehension of the disclosure.

The FAQ page also addresses advertisers' compliance obligations regarding the implementation of a program to train and monitor their network of bloggers and social media influencers. According to the FTC, the scope of an advertiser's training and monitoring program depends on the risk of harm to consumers in the event a blogger or social media influencer makes a deceptive statement. However, the FTC noted that all programs should include the following elements: 1) informing bloggers and social media influencers of the claims that they can make about the advertiser's products or services and those that they cannot make because they are unsubstantiated; 2) instructing bloggers and social media influencers on their responsibility to disclose their connection to the advertiser; 3) monitoring periodically the compliance of those endorsing its products and services with the above requirements; and 4) correcting any practices that do not comply with these requirements. The FTC also stated that endorsements must reflect the honest opinion of the endorser and that advertisers may not delegate their compliance obligations by hiring a service provider to assist with social media advertising.

Federal Communications Commission Issues Privacy Advisory

On May 20, 2015, the Enforcement Bureau of the Federal Communications Commission ("FCC") issued a public notice clarifying the FCC's position on enforcement of privacy protections for providers of broadband Internet access service.[2] The notice follows the FCC's decision in the Open Internet Order ("Order"), adopted February 26, 2015, which stated that the FCC would apply the customer privacy protections of Section 222 of the Communications Act (47 U.S.C. § 222) to broadband Internet access service, but would exercise forbearance from applying the FCC's previously-adopted Customer Proprietary Network Information ("CPNI") rules implementing § 222 to such service providers.[3] In noting that it was "not persuaded" that the CPNI rules are "well suited to broadband Internet access service," the FCC stated in

[1] 47 USC § 227(e); Truth in Caller ID Act of 2009, Pub. L. 111-331.

[2] FEDERAL COMMUNICATIONS COMM'N, DA 15-603, OPEN INTERNET PRIVACY STANDARD (2015), *available* at https://www.fcc.gov/document/isps-should-take-reasonable-steps-protect- privacy.

[3] In the Matter of Protecting and Promoting the Open Internet, Report and Order, FCC 15-24, ¶ 467 (2015).

the Order that "certain of those rules appear more focused on concerns that have been associated with voice service," and mentioned the fact that the rules do not address information such as web browsing history.

The May 20 public notice, which reiterates the FCC's decision to apply the "core customer privacy protections" of § 222 (and not the CPNI rules), called on broadband providers to take reasonable, good faith steps to protect consumer privacy. The notice states that the FCC may adopt implementing rules that are tailored to broadband providers, but that in the meantime the Bureau will focus on the reasonableness and good faith of a provider's steps to comply with Section 222, "rather than focus[] on technical details." Providers are instructed to employ "effective privacy protections in line with their privacy policies and core tenets of basic privacy protections." Going forward, the Bureau said it will provide formal and informal guidance on best practices for compliance and providers will be permitted to seek advisory opinions from the FCC to gain further insight.

Federal Communications Commission Adopts Order on Autodialed Telemarketing Calls

On June 18, 2015, by a vote of 3-2, the Federal Communications Commission ("FCC" or Commission") adopted a proposed Declaratory Ruling and Order ("Order" or "FCC 15-72") during an open meeting to clarify the Commission's interpretation of requirements set forth by the Telephone Consumer Protection Act ("TCPA") on autodialed or prerecorded telemarketing calls.[4] Prior to the open meeting, more than 20 petitions were submitted to the FCC, each requesting clarification concerning the Commission's interpretation of the TCPA.

The Order is expected to change the FCC's telemarking framework in several ways. First, the Order is expected to establish a broad definition of "autodialer" underscoring that an autodialer is "technology with the capacity to dial random or sequential numbers." The discussion among the Commissioners during the open meeting suggests that "autodialer" is expected to include technology with the future capacity to place autodialed calls and equipment that can send Internet-to-phone text messages. Second, the Order is expected to require companies placing autodialed calls to obtain the consent of the party that received the call rather than the intended recipient. The Order is also expected to clarify that consumers may revoke their consent "in any reasonable way at any time." Third, the Order is expected to reaffirm that the TCPA applies to autodialers sending text messages. Fourth, companies are expected to be allowed to place only a single autodialed call to a reassigned number without obtaining the new owner's prior consent. The Order is expected to clarify that the placement of more than one autodialed call to the reassigned number without receiving the new owner's consent is a violation of the TCPA. Fifth, it is expected that the Order will exempt from the prior consent requirement certain types of health calls (*e.g.*, vaccination shot reminders) and financial alerts (*e.g.*, bank account fraud alerts). The exemption is not expected to cover health or financial autodialed calls placed for marketing or debt collection purposes. Finally, the Order is expected to clarify that the TCPA does not prohibit telecommunications providers from providing consumers with technologies to block unwanted calls.

The FCC has not yet issued the full text of the Order nor indicated the expected date of its public release.

National Institute of Standards and Technology Releases Draft Privacy Risk Management Framework for Federal Information Systems

On May 29, 2015, the National Institute of Standards and Technology ("NIST") released a draft report entitled "Privacy Risk Management for Federal Information Systems," which sets forth a proposed privacy risk management framework ("Framework") for federal agencies that process personal information in federal information systems. In the draft report, NIST states that the Framework was developed to help address potential privacy risks associated with the increasing adoption of information technology by federal agencies, as well as encourage the use of certain vocabulary to further communication in and an understanding of this technology space. NIST is seeking public comment on the Framework until July 31, 2015.

The Framework contains two key components: (1) privacy engineering objectives, and (2) a privacy risk model. On privacy engineering, the Framework provides three objectives for engineers and system designers to consider when designing information systems. First, the "predictability" objective focuses on enabling reliable assumptions of stakeholders and achieving this through the processing of personal information by information systems. Second, the "manageability" objective is described as permitting granularity in the administration of personal information. Third, the "disassociability" objective is defined as providing for the processing of personal information or events without association to devices or individuals.

The privacy risk model recommends to federal agencies a process for calculating privacy risks posed by collection systems. The Framework states that the privacy risk model can help federal agencies determine the privacy risk of a data action in terms of likelihood and impact of a problematic data action, and emphasizes the importance of understanding that privacy risks are distinct from security risks when calculating privacy risk.

[4] Press Release, Federal Communications Comm'n, FCC Strengthens Consumer Protections Against Unwanted Calls and Texts (Jun. 18, 2015), *available* at https://www.fcc.gov/document/fcc-strengthens-consumer-protections-against-unwanted-calls-and-texts.

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST IR 8062, PRIVACY RISK MANAGEMENT FOR FEDERAL INFORMATION SYSTEMS (Draft) (2015), *available* at http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

In the States

Illinois Legislature Passes Bill to Update Breach Notification Law

On February 20th, 2015, Senate Bill 1833 was introduced in the Illinois Senate to amend and expand the scope of the state's Personal Information Protection Act ("PIPA"). On May 31st, the bill, which was originally drafted by Illinois Attorney General Lisa Madigan (D), passed both houses. SB 1833 was subsequently sent to Illinois Governor Bruce Rauner (R) for his consideration. As of late June 2015, it remained unclear whether Governor Rauner would sign the legislation.

Under Illinois' current breach notification law, PIPA requires notification to consumers of breaches of personal information, which includes Social Security numbers, driver's license numbers or state identification card numbers, and financial account numbers in combination with security codes necessary to permit access. Such types of information are commonly seen in state data breach notification laws across the country.

SB 1833 would expand the scope of information covered by PIPA. Specifically, SB 1833 would amend PIPA's definition of "personal information" to include: medical information; health insurance information; unique biometric data; geolocation information; consumer marketing information; home address, phone number, and email with mother's maiden name or month, day, and year of birth; and user name or email address along with a password that would permit access to an online account. The inclusion of this information, and in particular geolocation information and consumer marketing information, is a departure from data typically covered by state breach notification laws.

Additional components of the legislation would: obligate companies to inform the Illinois Attorney General of a breach; create data security requirements; and enumerate specific requirements for online privacy policies.

California Privacy Legislation Update

California's legislature has recently experienced a flurry of activity in the privacy space. The California Assembly passed A.B. 1116 on May 22, 2015. The bill places restrictions on the collection and use of recorded conversations by smart televisions. While the legislation would not create a private right of action, it would authorize civil penalties of up to $2,500 per violation. [6]

A.B. 83, which passed out the Assembly in early May, would amend California's Customer Records law to provide minimum security standards for retention of certain personal information. The bill states that "reasonable security procedures and practices" include, at a minimum, identifying reasonably foreseeable risks, maintaining safeguards to ensure the security of personal information, regularly assessing those safeguards, and evaluating and adjusting material changes that have an impact on the privacy or security of personal information. The bill also expands the definition of "personal information" to include any unique government-issued identification number, biometric information, geolocation data (including routes taken by a transportation service), signature, and online account log-in information.[7]

A.B. 259 passed out of the Assembly on June 1, 2015. The legislation would amend the Information Practices Act of 1977 to require that government agencies offer identity theft prevention and mitigation services for free for one year after they suffer a data breach.[8]

S.B. 178 passed the California Senate on June 3, 2015 and would require law enforcement to obtain a warrant or wiretap order to access electronic communication information, which includes "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device."[9]

New Jersey Enacts Law Limiting Access to Recorded Car Data

On May 12, New Jersey Governor Chris Christie signed an automobile data privacy bill into law. The law restricts access to recording devices in cars, which are similar to black boxes on airplanes. A recording device includes any electronic system in a vehicle that records data collected by the vehicles. The definition excludes personal devices that are in the vehicle.

Under the law, only the owner or the owner's representative can access and use the recorded data, unless one of the following exceptions apply: (a) the owner provides consent; (b) the data is retrieved pursuant to a search warrant; (c) the data is used to improve "safety, security,

[6] A.B. 1116, 2015-16 Leg. (Cal. 2015).
[7] A.B. 83, 2015-16 Leg. (Cal. 2015).
[8] A.B. 259, 2015-16 Leg. (Cal. 2015).
[9] S.B. 178, 2015-16 Leg. (Cal. 2015).

performance, operation, compliance with traffic laws, or traffic management…provided that the identity of the owner, operator or other occupant of the motor vehicle is not disclosed…"; (d) the data is used for diagnostics; (e) the data is accessed for certain emergency response purposes; or (f) the data is accessed pursuant to a discovery request.[10] The law also prohibits altering or deleting data on the device or destroying the device within two years of a crash that results in bodily injury or death. The law took effect immediately. A similar bill, introduced by U.S. Senator John Hoeven (R-ND) in the U.S. Senate, would provide restrictions on the access and use of recorded data at the federal level.

Pennsylvania Court Rejects Data Breach Class Action

On May 28, 2015, Pennsylvania State Judge R. Stanton Wettick Jr. rejected a proposed class action law suit against the University of Pittsburgh Medical Center.[11] The suit claimed that the hospital failed to protect employees' personal information that was compromised in a data breach.

According to the plaintiffs, confidential information including birthdates, Social Security numbers, tax and other financial information was compromised in a 2014 data breach. The plaintiffs asserted that because the provision of this personal information was mandatory for employment, failing to protect it was both negligent and a violation of an implied contract. The judge dismissed this argument, stating that both parties must have a "meeting of the minds" for an implied contract to exist.

Additionally, the judge stated that according to Pennsylvania's economic loss doctrine, the employees could not sue for damages because they incurred only economic losses from the breach, but sustained no personal or property injury. The judge stated that allowing plaintiffs to make a private cause of action to recover damages following a data breach would be overly burdensome to businesses and not in the public interest. Furthermore, citing the frequency of data breach occurrences, Judge Wettick asserted that allowing a private cause of action would trigger hundreds of thousands of lawsuits in the state, overwhelming the courts limited resources. The judge also cited precedent from the Pennsylvania State Legislature, stating that the legislature has decided against incorporating a provision in the state's Data Breach Act that would allow individuals to recover damages from a data breach.

Connecticut and Oregon Update Data Breach Notification Laws

On June 1, 2015, the Connecticut General Assembly voted unanimously in favor of legislation that would amend the state's data breach notification law. The bill, SB 949, is currently before Gov. Dannel P. Malloy, and, if he signs it, the bill will become effective on October 1st.

The bill would require any person that experiences a data breach that compromises the confidentiality of consumers' Social Security Numbers to provide at least one year of identity-theft prevention services to affected individuals and, if applicable, at least one year of identity theft mitigation services. Such services must be provided at no cost to affected individuals, and the notice sent to affected individuals must include all information necessary to enroll in these services. Additionally, the bill would require any person that experiences a data breach to report the breach to the attorney general's office within 90 days.

Connecticut's Attorney General has stated in a press release that the requirement to notify affected individuals within 90 days establishes an outside limit and that there may be circumstances in which delaying such notice for 90 days is unreasonable.[12] He further stated that his office will continue to bring enforcement actions against persons that unreasonably delay notifying individuals, even if notice is sent within 90 days. He also stated that the requirement to provide one year of identity theft protection services establishes a floor for the duration of such services. The Attorney General said that he will continue to seek more than one year's protection where circumstances warrant, and specifically, that he will continue to demand two years of identity theft protection where the breach involved highly sensitive information, such as Social Security Numbers.

On June 10th, Oregon enacted S.B. 601 amending the state's data breach notification statute. The new law will expand the statute's definition of "personal information" to include an individual's full name and any of the following:

- Biometric data that is used to authenticate the consumer's identity in the course of a financial or other transaction;
- A consumer's health insurance policy number or subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
- Information about a consumer's medical history, mental or physical condition, or about a health care professional's medical diagnosis or recommended course of treatment.

[10] A3579, 216th Leg. (N.J. 2015).

[11] *Dittman v. UPMC*, No. GD-14-003285 (Pa. Ct. Com. Pl., Allegheny Cnty., May 28, 2015).

[12] Statement of CT Attorney General Jepsen on Final Passage of Data Breach Notification and Consumer Protection Legislation, *available* at http://www.ct.gov/ag/cwp/view.asp?Q=566508&A=2341.

The new law also will add to the individual notification content requirements providing that the individual notice must advise consumers to report any suspected identity theft to law enforcement, including the Oregon Attorney General and the Federal Trade Commission. The new law will further add a requirement that the breached entity must notify the Oregon Attorney General of any breach involving more than 250 residents. Lastly, the new law will add an exemption to the individual notification requirement for covered entities that are subject to the breach notification requirements under the Health Insurance Portability and Accountability Act and that provide to the Oregon Attorney General a copy of the notice sent to the Department of Health and Human Services.

Marketplace

RadioShack Limits Data Sale Pursuant to Agreement with State Attorneys General

RadioShack recently curtailed its planned sale of customer data in a bankruptcy proceeding after concerns were raised by the Federal Trade Commission ("FTC"), dozens of state attorneys general, and some of the company's business partners.

After filing for bankruptcy earlier this year, RadioShack offered for sale a subset of its customer data, comprised of approximately 67 million records that included customer names, addresses, telephone numbers, email numbers, payment card numbers, and transaction histories. Thirty-eight state attorneys general, led by Texas Attorney General Ken Paxton, raised objections to RadioShack's plan to sell these customer data assets. In May, the attorneys general reached an agreement with RadioShack and acquiring company General Wireless to resolve the regulators' objections.[13]

Under the terms of the agreement, much of RadioShack's customer data will be destroyed. In particular, no payment card data will be sold. The acquiring company will obtain email addresses only for those customers who requested information from RadioShack within the past two years along with limited transaction data. These customers must receive clear and conspicuous prior notice of the transfer and an opportunity to opt out. With respect to the limited data that is sold, the acquiring company agreed to comply with RadioShack's privacy policy and not to sell the data to any other third party.

Before RadioShack's agreement with state regulators was announced, the Director of the FTC's Bureau of Consumer Protection ("BCP") also wrote a public letter to the court-appointed Consumer Privacy Ombudsman expressing concern about the planned sale of RadioShack's customer data in the bankruptcy.[14] Consistent with the views expressed by FTC staff in prior bankruptcy cases involving data sales, the letter cited provisions in RadioShack's privacy policies that stated that personally identifiable information would not be sold or rented to third parties and asserted that RadioShack's representations would likely be very important to many of the customers who provided such data. Recognizing that bankruptcy presents "special circumstances," the BCP Director stated that concerns about the data sale would be alleviated if (1) data was not sold as a standalone asset, (2) the buyer is engaged in substantially the same lines of business as RadioShack, (3) the buyer "expressly agrees" to follow RadioShack's privacy policy with respect to the acquired data, and (4) affirmative consent will be obtained for any material changes to the policy. Alternatively, the BCP Director suggested that customers' affirmative consent could be obtained prior to transferring the data.

Federal Court Dismisses VPPA Class Action

On May 15, 2015 the U.S. District Court in Massachusetts dismissed a potential class action lawsuit against the publisher of *USA Today*, Gannett Satellite Information Network, Inc., that alleged violations of the Video Privacy Protection Act ("VPPA").[15] The plaintiff alleged that the *USA Today* mobile app disclosed users' personally identifiable information ("PII") to a third party data company. Specifically, it was alleged that the disclosure of a user's device ID number, in combination with a video title, was a violation of the VPPA because the third party in question could potentially tie that information to other data in order to reidentify an individual. The court found that while the device ID could be considered PII, the user in question was not a subscriber to the publication because there was no payment of money, registration of information, periodic delivery, or other necessary elements of subscription involved in his use of the application.

The VPPA prohibits the knowing disclosure of information that identifies a consumer as having requested or obtained specific video materials or services from a video tape service provider ("VTSP"). The VPPA defines a consumer as any renter, purchaser, or subscriber of goods or services from a VTSP. Although the law was originally passed to cover brick-and-mortar video rental stores, courts have expanded

---

[13] Notice of Agreement Regarding Sale of Certain Personally Identifiable Information, *In re RadioShack Corp. et al.*, No. 15-10197 (Bankr. D. Del., filed May 20, 2015).

[14] Letter from Jessica L. Rich, Director, Bureau of Consumer Protection, Federal Trade Commission to Elise Frejka, Esq., Frejka PLLC (May 16, 2015).

[15] *Yershov v. Gannett Satellite Information Network, Inc., d/b/a USA Today,* case no. 14-13112-FDS (D. Mass. May 15, 2015).

the meaning of VTSP to include online video streaming services and mobile applications. The statue carries with it a private right of action, and a minimum of $2,000 per violation in damages.

The statute does not specifically define what types of information are considered PII, leaving the courts to give meaning to the term. A series of class action suits have been brought against content and streaming companies, all of which allege that a disclosure of anonymous numerical identifiers and video content information to third parties constitute a violation of the VPPA. However, the majority of these suits have been dismissed after the court, found that the numerical identifiers on their own were not enough to identify an individual. The *USA Today* decision, on the other hand, found that a device identifier could be considered PII under the statute, and dismissed the case based on a finding that the plaintiff did not qualify as a "consumer" under the statute. While courts have begun to come to a consensus regarding the status of anonymous identifiers under the VPPA, plaintiffs continue to bring suits under the VPPA, and this decision may embolden such claims.

International

FTC Settles U.S.-EU Safe Harbor Violations with Two Companies

The Federal Trade Commission ("FTC") recently announced two settlements with companies for violations of the U.S.-EU Safe Harbor Framework.

The Safe Harbor Framework is a streamlined means for United States' organizations to comply with the European Commission's Directive on Data Protection (the "Directive") which generally prohibits the transfer of personal data to non-European Union countries such as the U.S. that do not meet an "adequacy" standard for privacy protection as determined by the EU. Companies that join the Safe Harbor Framework must implement processes and procedures that extend the protections and obligations of the Directive to personal data collected from residents of EU member countries. These companies are also required to make public representations about their compliance with the Safe Harbor Framework and submit to a dispute resolution mechanism to resolve any complaints about their compliance. Deceptive misrepresentations about Safe Harbor compliance are enforceable by the FTC.

The FTC issued complaints against TES Franchising, LLC and American International Mailing, Inc. for allegedly false representations on their websites that their certifications under the Safe Harbor Framework remained current when the certifications had lapsed some years earlier. The complaint against TES also separately alleged a deceptive representation about TES' dispute resolution procedures. According to the complaint, the TES webpage represented that any disputes brought under the Safe Harbor Framework would be settled by an arbitration agency and contained additional terms about the costs and venue of such disputes. The FTC alleged that TES had actually agreed to have all disputes resolved by the European Data Protection authorities. Finally, TES also allegedly falsely claimed to be a licensee of the TRUSTe privacy program.

EU General Data Protection Regulation Moves Forward

On June 15th, the Council of Ministers in the EU reached consensus on a revised text of the proposed General Data Protection Regulation ("GDPR"). This clears another procedural hurdle for the GDPR, which continues its long march towards enactment.

The GDPR was introduced in 2012. It would replace the current European Commission Directive on Data Protection which has been in place since 1995. The current Directive provides a set of guiding principles to member countries, which are required to enact the principles into local law. This local enactment process allows countries to interpret provisions of the Directive in different ways. The proposed GDPR would be a top-down Regulation that all countries must accept as law, although there are places in the GDPR that would require individual countries to implement certain provisions via local law. The proposed GDPR is also highly proscriptive, containing hundreds of "articles" conferring legal obligations on companies that operate in the EU.

Most recently, the European Council agreed on a draft text, following separate draft texts approved by the European Parliament and the European Commission. This begins the next step of approval—the "trilogue" process—where all three draft texts must be reconciled and agreed upon. Once a final text of the GDPR is agreed upon, it can be adopted into law and supersede the current Directive once it comes into effect. Under the tentative timetable released for the trilogue, meetings will begin on June 24th with the goal of agreement on an overall roadmap for trilogue discussions. A second meeting, tentatively scheduled for July 14, is supposed to discuss the topics of the territorial scope of the GDPR and the treatment of international transfers of personal information.

At present, the three texts have wide discrepancies in a number of substantive areas. Although the timetable aims for agreement on a final text by the end of 2015, it is uncertain whether that goal is achievable.

About Venable's Privacy and Data Security Team

Venable's privacy and data security attorneys, pioneers in the field, provide an integrated approach to legal and business solutions in e-commerce, Internet advertising, financial services, homeland security and government surveillance, telemarketing and medical privacy. Our attorneys are well-versed in the evolving U.S., Canadian, European and Asian regulations governing our clients' businesses, and assist with drafting statutes and regulations. Our clients represent a variety of industries and are supported by Venable's renowned Legislative and Government Affairs, Advertising, IP and Communications Practices. Venable's Privacy and Data Security Practice is recognized in *Chambers Global* and the U.S. *Legal 500* and has won the *Chambers USA* Award for Excellence.

About Venable

An *American Lawyer* Global 100 law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

Venable's Privacy and Data Security Team serves clients from these office locations:

WASHINGTON, DC
t 202.344.4000

NEW YORK, NY
t 212.307.5500

SAN FRANCISCO, CA
t 415.653.3750

LOS ANGELES, CA
t 310.229.9900

BALTIMORE, MD
t 410.244.7400

TYSONS CORNER, VA
t 703.760.1600