GIBSON DUNN

The Stored Communications Act and Trends in Data Privacy: What Companies Need to Know in 2021

March 2, 2021

Presented By:
Michael Holecek
Eric Vandevelde
Lisa Zivkovic

Agenda


1
THE ELECTRONIC COMMUNICATIONS ACT (AND STORED COMMUNICATIONS ACT)
2
THE SCA'S DISCLOSURE PROHIBITIONS
3
THE SCA'S ACCESS PROHIBITIONS
4
QUESTIONS

GIBSON DUNN

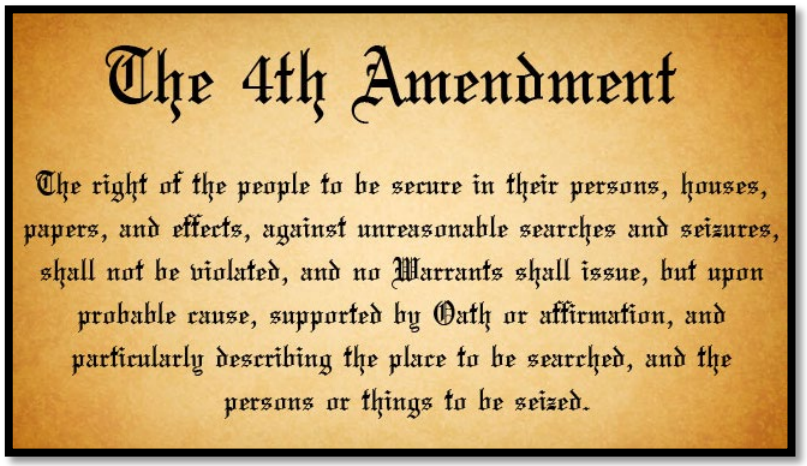
The Electronic Communications Act (and Stored Communications Act)

ECPA – Protecting the Privacy of Our Citizens

- The ECPA was *intended to extend Fourth Amendment protection to electronic communications data*.
  - "[I]f Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will *gradually erode as technology advances*." (House Report, supra, at p. 19, fns. omitted.)

ECPA – Protecting the Privacy of Our Citizens

- The ECPA was *intended to extend Fourth Amendment protection to electronic communications data*.



- The Senate Committee observed that "computers are used extensively today for the storage and processing of information," and yet because electronic files are "subject to control by a third party computer operator, *the information may be subject to no constitutional privacy protection*" absent new legislation. (Sen. Rep., supra, at p. 3; accord, House Rep., supra, at pp. 16-19.)

The Electronic Communications Privacy Act of 1986 ("ECPA")

- The SCA is **Title II of the three-title ECPA**.
  - The ECPA also includes the **Wiretap Act** (18 U.S.C. §§ 2515, *et seq*.), which protects the real-time interception of electronic communications in transit.
  - Title III of the ECPA (18 U.S.C. §§ 3121, *et seq*.) **regulates government use of pen registers** and other similar surveillance devices.

The Stored Communications Act

- The SCA seeks to protect ***communications in storage***, while "protecting the Government's legitimate law enforcement needs."
  - ***Disclosure prohibitions*** make it illegal for certain technology providers to disclose information.
  - ***Access prohibitions*** limit third parties' ability to access electronic communications without sufficient authorization.

Illegal to Disclose Information – *Facebook, Inc. v. Wint*, 199 A.3d 625, 627 (D.C. 2019)

- The District of Columbia Court of Appeals found that the ***plain text of the SCA forecloses Facebook from complying with criminal defendant's subpoena***, reversing trial court's order holding Facebook in civil contempt for refusing to comply with subpoenas served by appellee Daron Wint.

Facebook, Inc. v. Wint – Background Information

- Appellee was charged with murder in DC Superior Court.

- Before trial, he filed an ex parte motion asking the trial court to authorize defense counsel to ***serve subpoenas on Facebook for records***, including the ***contents of communications***, relating to certain accounts.
  - Wint argued the SCA would be unconstitutional, if SCA were interpreted to preclude Facebook from complying with the subpoenas.

- Facebook objected, arguing that the ***SCA prohibits Facebook from disclosing such information*** in response to a criminal defendant's subpoena.

Facebook, Inc. v. Wint – SCA Is Not Unconstitutional

- **Ruling:** Court held that the SCA is **not unconstitutional** and ***prohibits providers from disclosing covered communications in response to criminal defendants' subpoenas***.
  - Structure of the SCA and authority from other jurisdictions support this conclusion.
  - Legislative history and SCA do not contain any explicit reference to subpoenas by criminal defendants.
  - SCA does not prohibit subpoenas directed at senders or recipients rather than providers.

Facebook v. Superior Court (Touchstone) – 7-Factor Test

- Issue: Whether criminal defendant has a *constitutional right to obtain social media records* from a social media provider.

- Court Ruling: The California Supreme established a *seven-factor balancing test* to determine whether the subpoena was supported by good cause (evaluating such factors as whether the materials can be obtained from a different source, the defendant's need for the materials, and third-party privacy interests).

Facebook v. Superior Court (Touchstone) – 7-Factor Test

- Background:
  - Defendant Lance Touchstone, charged with attempted murder, sought victim's Facebook posts and private messages – instead from the victim himself –, believing the content of such communications to provide helpful exculpatory evidence in preparing for trial.
  - Facebook moved in the Superior Court to quash Touchstone's subpoena on the basis of the SCA, which prohibits an ECS from disclosing the contents of people's communications in the absence of certain exemptions, such as consent.
  - Defendant argues that his constitutional right to a fair trial trumped SCA privacy protections.
  - Trial court denied Facebook's motion to quash, the Court of Appeal reversed, and the California Supreme Court granted Touchstone's petition for review.

Facebook v. Superior Court (Touchstone) – 7-Factor Test

- Court Ruling: The California Supreme Court remanded the case for renewed analysis of whether the subpoena was supported by good cause by employing a *seven-factor balancing test* to determine the existence of good cause:

1. Plausible justification for acquiring documents from a third party?
2. Is material adequately described and not overly broad?
3. Is the material reasonably available to the entity from which it is sought (and not readily available to the defendant from other sources)?
4. Would production violate a third party's confidentiality or privacy rights?
5. Is defendant's request timely or premature?
6. Would the time required for production necessitate an unreasonable delay of defendant's trial?
7. Would production place an unreasonable burden on the third party?

GIBSON DUNN

The SCA's Disclosure Prohibitions (18 U.S.C. §§ 2702–2703)

SCA Key Distinctions

- The SCA's disclosure prohitions framework rests on a few key distinctions.

  - Electronic Communication Services ("ECS") vs. Remote Computing services ("RCS")
  - Content vs. Non-Content
  - Governmental Request vs. Non-Governmental Request

Distinction 1: ECS vs. RCS

- ECS providers include "any service which provides to users thereof the ability ***to send or receive*** wire or electronic communications." 18 U.S.C. § 2510(15).

- RCS providers offer "the provision to the public of ***computer storage*** or processing services by means of an electronic communication." 18 U.S.C. § 2711(2).

- Not mutually exclusive - many service providers offer services qualifying as both ECS and RCS. *See, e.g., Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 980–81 (C.D. Cal. 2010).

- Each particular communication is measured to determine whether a provider is acting as an ECS or an RCS is measured. *See In re U.S.*, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009).

Why the ECS vs. RCS Determination Matters

- Both ECS and RCS are <u>prohibited from disclosure</u> of content *absent an applicable exception*.

- The government can only obtain certain content (stored for less than 180 days) from ECS with a warrant, but it can obtain the same content from an RCS with a subpoena and notice to the user. 18 U.S.C. § 2703(a).

Distinction 2: Content vs. Non-Content

- Content includes "*any wire, oral, or electronic communication*, includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).
  - Courts construe "content" *broadly*—for instance, a court recently held that Instagram Stories are "content." See, e.g., *Facebook, Inc. v. Pepe*, __ __ A.3d __, 2020 WL 1870591, at *4 (D.C. Jan. 14, 2020).
- Non-content is divided into two categories: 1) "basic subscriber information" ("BSI"); and 2) other non-content.
  - BSI includes the identity of subscribers, their relationship to the provider, and basic connection records, as well as non-content that relates to a specific user. 18 U.S.C. § 2703(c)(1)-(2).

Why the Content vs. Non-Content Distinction Matters

- **Disclosure of content** by an ECS or RCS provider is ***prohibited*** (unless an exception applies).

- But an ECS or RCS provider ***may freely disclose*** **non-content** in many instances (except to the government).

Distinction 3: Non-Governmental vs. Governmental Disclosure

- The SCA's bars on disclosure are **not absolute** – they are subject to ***exemptions*** and ***compelled disclosure frameworks,*** depending on whether the disclosure would be to a private entity or a government entity.

  - **Non-content** may be ***freely disclosed to non-governmental entities***. 18 U.S.C. § 2702(c)(6).

  - **Content** may be disclosed ***only if one of the exemptions are met***. *See, e.g., O'Grady v. Superior Court*, 139 Cal. App. 4th 1423 (2006).

Social Media Communications and Lawful Consent Exception

- **Consent** exception is **key exception** to prohibition against disclosing content of communications by ECS/RCS.

- **Key issues:**
  - Whether communications that are ***sent to numerous recipients*** are considered **private** and outside the lawful consent exception.
  - Whether providers ***must disclose*** any communication pursuant to a subpoena that is authorized under state law.

Facebook v. Superior Court (Hunter) – Scope of Lawful Consent

- Court ruled that **posts made public on social media** can fall under the *lawful consent exception*.

- However, this exception does **not extend** to social media communications that were limited to even a large group of people.

Facebook v. Superior Court (*Hunter*) – Background

- Lee Sullivan and Derrick Hunter, charged with murder, weapons offences, and gang activity, sought private ***posts from victim's Facebook and Instagram accounts*** and ***from victim's then-girlfriend's Instagram and Twitter accounts***.

- Defendants argued that posts accessible by large group of users are considered public because social media users "lose[] control over dissemination once the information is posted," and can have **no reasonable expectation of privacy**.

- Tech providers moved to quash subpoenas and trial court denied motions.

Facebook v. Superior Court (Hunter) – Scope of Lawful Consent

- Court ruled that **posts made public on social media** can fall under the *lawful consent exception*. However, this exception does **not extend** to social media communications that were limited to even a large group of people.

- **Key inquiry** is whether social media users ***took steps to limit access to the information*** in their posts. "Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has."

Other Exceptions Permitting Disclosure:

- **9 exceptions**: The SCA allows providers of an RCS or ECS to disclose the contents of a communication (18 U.S.C. § 2702(b)):
  - To an addressee or intended recipient of such communication
  - With lawful consent of the originator or an addressee or intended recipient
  - To a person authorized to forward such communication to its destination
  - As may be necessary to perform the service or to protect the rights or property of the provider of that service …
- 18 U.S.C. § 2702(c) sets out **7 exceptions** to the statute's general bar on the disclosure of non-content.

Permissive Disclosure?

- Can a provider be *compelled* to disclose where an exception applies?
  - When an ***exemption applies***, the statute says that a provider "**may**" disclose content and non-content. 18 U.S.C. § 2702(b)–(c).
  - Providers in *Hunter* argued that where an exemption applies, the SCA affords provider discretion to decline to comply with a valid state subpoena. *Facebook v. Superior Court (Hunter).*
  - Court ruled that providers are ***compelled to disclose information pursuant to a valid state subpoena***, where the lawful consent excepted was satisfied. *Facebook v. Superior Court (Hunter); see also, Negro v. Superior Court (2014).*

Governmental Disclosure – Content

- One of the 9 content disclosure bar exceptions permits disclosure "as otherwise authorized in section . . . 2703." 18 U.S.C. § 2702(b)(2).
  - The government can obtain content from an **ECS provider** that has been in electronic storage **for 180 days or less** only by obtaining a warrant. 18 U.S.C. § 2703(a).
  - The SCA allows the government to obtain content from an **ECS provider** that has been in electronic storage **for more than 180 days** with less stringent requirements.
  - The government can obtain content from an **RCS provider** with (1) a warrant, (2) notice to the user *and* an administrative subpoena, *or* (3) notice to the user *and* a court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Governmental Disclosure – Non-Content

- SCA's general non-content disclosure bar also contains an exemption permitting disclosure "as otherwise authorized in section 2703." For non-content, section 2703 says:
  - The government can obtain **BSI** through an administrative subpoena (but the government does not need to notify the user).
  - The government can obtain **other non-content** with (1) a warrant, (2) a court order, (3) consent of the user, or (4) a formal written request for certain limited information relevant to a law enforcement investigation concerning telemarketing fraud. 18 U.S.C. § 2703(c)(1).

Extraterritorial Scope of SCA – Does the SCA Apply to Data On Foreign Servers?

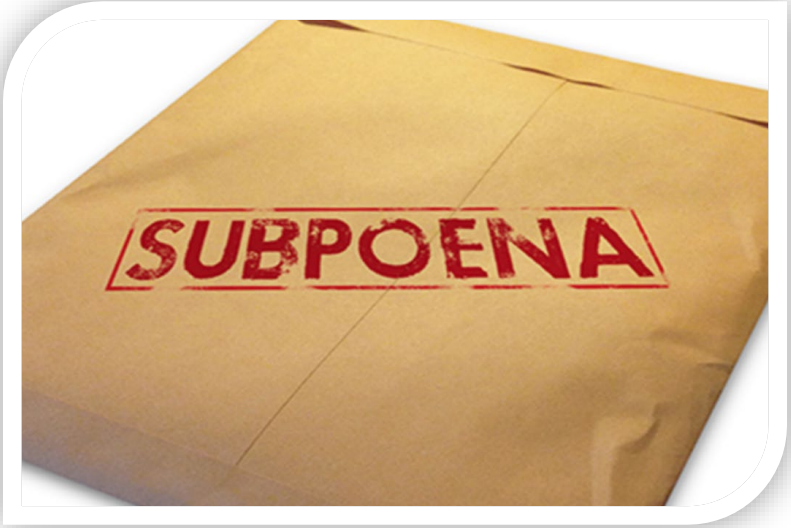
- Prior to the enactment of the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") on March 23, 2018, courts were split as to ***whether the search warrant provisions*** of the SCA are applied extraterritorially when search warrants seek data stored on foreign servers.
  - The Second Circuit in *Microsoft v. US* quashed the search warrant for data stored on an Irish server, ruling that the location of the "seizure" would be in Ireland and the ***search warrant provisions of the SCA do not extend extraterritorially***. *In re Warrant to Search a Certain E-mail Account Controlled and Maintained By Microsoft Corporation v. United States (The Microsoft-Ireland Case),* 829 F.3d 197 (2d Cir. 2016).
  - The EDPA in *Google v. US* found that there was ***no extraterritorial application of the search warrant provisions*** of the SCA because no seizure occurred until law enforcement accessed data in the US. *In re Search Warrant No. 16–960–M–1 to Google*, 275 F.Supp.3d 605, 619 (E.D. Pa. 2017).

Extraterritorial Scope of SCA – CLOUD Act

- The CLOUD Act amends the SCA – service providers must "preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*."

What To Do When You Receive a Civil Subpoena?

- Are you an ECS or RCS?
- Which entity received the subpoena – subsidiary or parent?
- Determine whether communications were stored electronically.
- Consider SCA protection – including privacy settings and configurations.
- Determine whether any exceptions apply.
- Consider how GDPR (and other international data protection laws) are implicated.



- What do you need to disclose about the legal process when disclosing records?
- Consider potential liability (discussed below).

Potential Liability Under the SCA

- The SCA provides a **private right of action** to anyone "aggrieved by any violation" engaged in with a "knowing or intentional state of mind." 18 U.S.C. § 2707(a).
  - But "[a] good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization" or "a request of an investigative or law enforcement officer" "is a complete defense." 18 U.S.C. § 2707(e).
- **Statutorily-provided remedies**:
  - Minimum damages of $1,000;
  - Actual damages and disgorgement of profits, if greater than $1,000;
  - Injunctive or declaratory relief;
  - Litigation costs and attorneys' fees;
  - Punitive damages, ""[i]f the violation is willful or intentional."

GIBSON DUNN

The SCA's Access Prohibitions (18 U.S.C. § 2701)

Criminal Liability for Unauthorized Access

- Section 2701 **criminalizes** "***intentionally access[ing]***" or "***intentionally exceed[ing]*** an authorization to access" an ECS provider "facility" resulting in "obtain[ing], alter[ing], or prevent[ing] an electronic communication within that facility.

- Violations may result in a fine or up to **5 years' imprisonment** (and 10 years' imprisonment for subsequent violations).

GIBSON DUNN

Questions?

Questions

Michael Holecek

333 South Grand Avenue, Los Angeles, CA 90071-3197 USA

Tel +1 213.229.7018
MHolecek@gibsondunn.com

Michael Holecek is a litigation partner in the Los Angeles office of Gibson, Dunn & Crutcher, where his practice focuses on complex commercial litigation, class actions, labor and employment law, and data privacy—both in the trial court and on appeal. Mr. Holecek has first-chair trial experience and has successfully tried to verdict both jury and bench trials, he has served as lead arbitration counsel, and he has presented oral argument in numerous appeals. Mr. Holecek has also authored articles on appellate procedure, civil discovery, corporate appraisal actions, data privacy, and bad-faith insurance litigation.

In 2017, Mr. Holecek was selected by the Carl & Roberta Deutsch Foundation as a 2017 HALO Award winner for his work on behalf of domestic-violence survivors. He was also honored as a winner of Gibson Dunn's Frank Wheat Memorial Award for his commitment to pro bono work.

Mr. Holecek serves on the Board of Directors of Family Violence Appellate Project, a nonprofit organization dedicated to providing free legal representation to domestic violence survivors.

Mr. Holecek was recognized in *The Best Lawyers in America*® 2021 Ones to Watch in Mass Tort Litigation/Class Action.

Mr. Holecek earned his law degree with high honors from the University of Chicago Law School in 2011. While at Chicago, he was a member of the *University of Chicago Law Review*. Mr. Holecek was runner-up in the Hinton Moot Court Competition and winner of the Karl Llewellyn Cup and the Thomas R. Mulroy Award for Excellence in Appellate Advocacy. He was a Kirkland & Ellis Scholar and was elected to the Order of the Coif.

Mr. Holecek graduated *magna cum laude* from Rollins College in 2001 with a bachelor's degree in Political Science and a minor in Fine Art.

Before attending law school, he founded and served as Managing Director of ERA Real Estate, the second largest residential real estate network in the Czech Republic.

Mr. Holecek is admitted to practice in the State of California.

Eric D. Vandevelde

333 South Grand Avenue, Los Angeles, CA 90071-3197 USA

Tel +1 213.229.7186
EVandevelde@gibsondunn.com

Eric D. Vandevelde is a litigation partner in Gibson Dunn's Los Angeles office and a member of its White Collar Defense & Investigations, Privacy, Cybersecurity and Data Innovation, Intellectual Property, and Crisis Management practice groups. He is a former federal prosecutor and an experienced trial and appellate attorney. He has significant first-chair trial experience and a deep technical computer/software engineering background, having obtained a degree in Computer Science from Stanford University and worked as a software engineer in Silicon Valley and Latin America. Mr. Vandevelde has been selected by Chambers USA in the area of White-Collar Crime & Government Investigations, has been repeatedly recognized as a "Super Lawyer" by Super Lawyers Magazine, and was named one of the Top 20 Cyber/Artificial Intelligence Lawyers in California by The Daily Journal. Mr. Vandevelde's practice focuses on white collar and regulatory enforcement defense, internal investigations, and technology-heavy civil litigation matters, often involving computer/software-related trade secrets, copyrights, patents, and other intellectual property. He routinely handles consumer protection investigations by state and federal regulators, including state Attorneys General and District Attorneys, as well as the Federal Trade Commission (FTC), into allegedly unfair, unlawful, and deceptive practices. Eric is on the forefront of cryptocurrency issues and related regulations, handling investigations for major crypto exchanges involving the Securities and Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), and Office of Foreign Assets Control (OFAC). Eric has also represented clients in some of the highest-profile, highest stakes cases in the country concerning government and law enforcement demands for corporate data and assistance in connection with criminal and national security-related investigations.

From 2007 to 2014, Mr. Vandevelde served as an Assistant U.S. Attorney in the U.S. Attorney's Office for the Central District of California. He was Deputy Chief of the Cyber & Intellectual Property Crimes Section, supervising one of the nation's largest teams of federal prosecutors dedicated to investigating and prosecuting computer hacking and intellectual property offenses. He was the lead prosecutor on numerous high-profile cyber-crime investigations, including cases involving corporate espionage, theft of trade secrets, APTs (advanced persistent threats), botnets, distributed denial of service attacks, SQL-injection attacks, and other sophisticated cyberattacks. Mr. Vandevelde handled the prosecution of several infamous hacking groups that infiltrated dozens of government and corporate servers around the world. Other matters included the prosecutions of a nationwide identity theft ring involving millions of dollars in fraudulent cash withdrawals; importers and distributors of counterfeit pharmaceuticals, electronics, and other consumer goods; a hacker of cellular telephone payment systems; a hacker who infiltrated the website of a publicly traded company to post false press releases in an attempt to manipulate the company's stock price; and executives at an aircraft parts supplier for selling fraudulent electronics, including to the U.S. military. Mr. Vandevelde also successfully prosecuted numerous traditional white collar cases as part of the Major Frauds Section, including healthcare fraud, mortgage fraud, investment fraud, tax fraud, and government procurement fraud cases, as well as some of the largest Ponzi scheme cases in Southern California. While at the U.S. Attorney's Office, Mr. Vandevelde first-chaired complex financial fraud, intellectual property, and cybercrime-related cases, and mentored junior prosecutors in numerous other trials. Mr. Vandevelde successfully argued multiple appeals before the Ninth Circuit. He also trained new prosecutors regarding electronic surveillance and data privacy issues. For his work with the government, Mr. Vandevelde received numerous awards and commendations from federal agencies, including the FBI, Secret Service, IRS, and U.S. Postal Inspection Service.

Mr. Vandevelde graduated from UCLA School of Law, Order of the Coif. After law school, he clerked for the Honorable A. Howard Matz, United States District Judge, Central District of California.

Lisa V. Zivkovic

200 Park Avenue, New York, NY 10166-0193 USA

Tel +1 212.351.3961
LZivkovic@gibsondunn.com

Ms. Lisa V. Zivkovic, Ph.D is an associate in the New York Office of Gibson, Dunn & Crutcher. She is a member of the Firm's Privacy, Cybersecurity and Data Innovation, Technology Transactions, and Litigation Practices Groups.

Ms. Zivkovic advises a wide range of clients, including technology, financial services, data aggregation and analytics, vehicle, and telematics companies, on new and complex legal and policy issues regarding global data privacy, cybersecurity, artificial intelligence, Internet of Things, and big data. Her practice focuses on assisting clients with data breach response and planning, cyber fraud, cloud computing, as well as government investigations and regulatory compliance with state, federal, and international privacy regulations, including the California Consumer Privacy Act, EU General Data Protection Regulation, Gramm-Leach-Bliley Act, Federal Trade Commission Act, Electronic Communications Privacy Act, Children's Online Privacy Protection Rule, and other proposed laws.

Ms. Zivkovic completed her Doctor of Philosophy in the history of data privacy in the United States and Europe. Her dissertation, entitled "Reconciling the European and America Approaches to Privacy Law: A Historical and Legal Analysis of Privacy Law and Data Communications Technology in the United States and Europe, 1978-2018," is a comparative history of technology and legal history of data privacy in the United States and Europe. By virtue of examining the technological architecture of the Minitel, France's precursor to the Internet, and the Internet, and the surrounding legal regimes of both communication network systems, Ms. Zivkovic's dissertation reveals that the privacy regimes in the US and Europe are not irreconcilable and certain concepts, such as the right to privacy and paying for services with access to personal data, were salient concepts to both networks in their early days. Her scholarship and by extension her practice emphasize the importance of understanding the underlying technology to inform her analysis of the law and policy. She has also published recently on the subject. Pursuant to winning the Tradafir Writing Competition, her article, entitled "The Alignment Between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protec the Data Subject," was published in University of Iowa's College of Law's Transnational Law & Contemporary Problems Journal. She also completed a legal externship in the Bureau of Internet and Technology at the Office of the New York Attorney General.

Ms. Zivkovic received her Doctor of Philosophy from New York University and her Juris Doctor from Fordham University School of Law in 2018. At New York University, she served as Assistant Editor for the Professional Peer-Review Journal, *French Politics, Society & Culture*. At Fordham Law, she was a Decennial Fellow at the Center of Law and Information Policy and a member of Fordham Law's *Urban Law Journal*. She received her Bachelor of Arts and Science from Princeton University, where she did an exchange with the Institut D'Etudes Politiques de Paris, Sciences-Po, graduated *magna cum laude,* and was a two-time prize winner for Best Undergraduate Thesis.

Ms. Zivkovic is admitted to practice in the State of New York and the United States District Court for the Southern District of New York.

Ms. Zivkovic is the Young Privacy Professional of the International Association of Privacy Professionals' New York KnowledgeNet Chapter, as well as a member of the New York State Bar Association.