International Municipal Lawyers Association 2020 IMLA Virtual Annual Conference

Data Protection, Privacy & Cybersecurity for Local Government

September 29, 2020

Benjamin E. Griffith & Sven Kohlmeier

Introduction

This presentation reflects the perspectives of an American lawyer and a German Rechtsanwalt on data protection, privacy and cybersecurity for local government. This deep dive into the debate over data protection, privacy and cybersecurity can be traced to an evening of cigars and single-malt scotch at the World Jurist Association Congress in Barcelona where these two first met three years ago. Each has experience in these issues in the context of municipal governance, and each speaks the other's language to a fair extent.

There are key differences and similarities between the U.S. privacy laws and laws that reflect Germany's approach to data protection, the right of privacy and cybersecurity, and these differences are global in nature, transnational in scope and rooted deeply in history. The similarities reflect the closeness of the U.S.A. and Germany in the field of human rights, governmental oversight, individual freedom and the fundamental right of privacy.

Of Privacy and Power

Henry Farrell and Abraham Newman described themselves as intellectual doppelgängers when they first met in 2003 over a beer in Bonn, Germany. They recently published *Of Privacy and Power – The Transatlantic Struggle Over Freedom and Security* (Princeton Univ. Press 2019), a landmark book that plunges deeply into the geopolitical issues covered in this presentation, illustrating that ours is indeed an interconnected world. *Of Privacy and Power* provides a sobering picture of the different political, social and legal systems and internal norms from the business sector (one many would agree is dominated by Microsoft, Google, Amazon, a and Facebook) that have resulted in a closer, more pragmatic geopolitical relationship that transcends assumptions about the security-focused U.S. and the privacy-focused E.U..

Farrell and Newman describe a world influenced by public and private actors, political and commercial interests, and national and international debates. These debates that have been played out, and continue to do so, in the E.U. Parliament and the U.S. Congress over privacy and power, and they dominate the privacy-security discussion today. In doing so, these are fuel for the ongoing and heated contest that accompanies E.U.-U.S. interactions over privacy and security, which "have never reached a stable equilibrium" and are often far from discrete bargaining outcomes with a clear winner and clear loser. Id. at 172.

A Cross-National Alliance

Of Privacy and Power highlights the importance of a cross-national alliance for transatlantic politics over privacy and security. Farrell and Newman provide an objective basis for evaluating how best to safeguard privacy amidst the demands of global and domestic security post-9/11. Id. at 167. They also make a convincing case for the proposition that homeland security, domestic security, counterterrorism and interior policy are no longer confined within national borders, and that debates over privacy and civil liberties are now internationalized. Id. at 2, 95-97.

Transatlantic Tensions over national security and privacy protection

There are a number of relevant examples of how the transatlantic tensions between the United States and the European Union go well beyond simplistic depictions of the U.S. as Mars and the E.U. as Venus. Id. at 97.

A treasure trove of the many U.S.-E.U. interactions, relationships and transatlantic interdependence is contained in *Of Privacy and Power*. These are the forces and events that have led many to assume, incorrectly, that
►there has been an effective subordination of the E.U. to the U.S. national security state,
►the E.U. is holding the U.S. back from protecting the security of its citizens, or
►European officials are imperiling the safety of U.S. citizens because of a mindless attachment to abstract principles of privacy protection. Id. at 159, 164-169.

While these tautologies have at least some factual support in the popular political narratives of social media and political hacks, none are absolute and supported by a solid factual foundation. Many privacy-security debaters see this as a battle or a fight. On the contrary, it is far from a simplistic analogy that would characterize our transatlantic differences as a battle between warmongering Americans or lily-livered Europeans, or a fight between Europe and the United States that has not been contained within national borders.

Multinational Corporate Actors in the Debate

A number of complex digital travails in the courts in the U.S. and in the E.U. have put Microsoft, Google, Amazon and Facebook on their heels. One centers on the U.S. CLOUD Act and its political consequences in the E.U. during the final stages of the *United States v. Microsoft* data privacy litigation, Id. at 67, 167-168. Another focuses on the creation and then surprising invalidation of the Safe Harbor Agreement in *Schrems I* in which data privacy authorities and the E.U. courts could conceivably make it impossible for Facebook and Google to "require their customers to consent to their personal data being used to target advertising to them," thereby putting pressure on U.S. regulators "to make U.S. companies more responsive to European privacy concerns." Id. at 169. We will cover *Schrems* II in this presentation as well, a surprising development in the field of data protection that caught many by surprise.

There are also conflicts between European privacy laws and post-9/11 U.S. legislation requiring foreign carriers to transfer detailed information on passengers to U.S. Customs, leading ultimately to an international accord on Airline Passenger Data Sharing. Id. at 69. 93.

GDPR implementation

Of Privacy and Power takes us to the origin, purpose and intended result of implementation of the GDPR (and by extension Germany's more stringent version of it), as laudable but perhaps imperfect efforts to "minimize unwanted or unnecessary data collection and processing through privacy-by-design initiatives, opt-in requirements, and a right to date erasure (often referred to as the right to be forgotten). At the same time, it explicitly recognizes the transnational nature of data sharing, extending the legislation's scope to data concerning individuals based in the European Union regardless of whether or not data collection or processing occurs within the European Union. In other words, individuals based in the European Union enjoy extraterritorial protection of their rights." Id. at 168.

Is Big Brother Listening?

Ours is not simply a world beset with the looming threat of Big Brother listening to us and watching us through the Internet of Things (IOT) on which our internet-connected systems exist. Instead, it is a complex and pervasive decentralized architecture of private, public, quasi-public, domestic, and international systems, all busily gathering data on us, "intersecting in murky, complex, and sometimes invisible ways." Id. at 164.

While the State is certainly not gone, even as it continues to use data to go after terrorists, criminals and political opponents, there has been a radical transformation of the world that surrounds the State by the decentralized monitoring of internet browsing. The vehicles for this have included the ubiquitous use of GPS, cell phones with altitude sensor, behavior-predictive, biometric and facial recognition technology that "endlessly whisper information back to the mothership." Id. at 165.

Of Privacy and Power concludes that those in academia and policymaking positions "concerned with surveillance and privacy must learn how to map this shifting transnational environment if they hope to engage with its consequences for politics," as the line between public and private is being washed away. Id. at 165.

Facial Recognition Technology

Facial recognition technology is a form of artificial intelligence that matches faces and tracks people. According to Grand View Research, the size of the government "facial biometrics" market is expected to grow from $136.9 million in 2018 to $375 million in 2025. The rapid rise of facial recognition technology appears to have prompted a backlash at the state legislative level, municipal level and in the U.S. Congress. There are increasingly prominent privacy issues now being raised over the use of facial recognition monitoring to track people. Facial recognition technology maps faces in a crowd, compares them to a watch-list of images, suspects, missing people and persons of interest to law enforcement. Automated facial recognition enables police or other law enforcement agencies to monitor people's activity in public in a way they have never done before, capturing almost instantaneously the biometric data of thousands of people, all with profound consequences for privacy and data protection rights, which may not be adequately or sufficiently protected by the existing legal framework.

For example, at a pro-gun rights rally or a protest against gun violence, concerns may be raised that "the Government" could monitor and enter facial photos in a database that in turn could be used in unrestricted ways, such as scanning faces in large crowds in public places like streets, shopping centers, football games and other sports events, or concerts. The usefulness and value of this technology lies in how it helps with police investigations and crime deterrence.

"It does not require a great leap of logic to conclude that most people have a reasonable expectation that their faces will not be scanned in a public place and processed without their consent at a time when they are not the subject of wrongdoing. For those of us who live in a democracy and not in an authoritarian state, this is as it should be." David Gershgorn, *Microsoft Wants Congress to Regulate Facial Recognition*, July 13, 2018, Quartz, accessible at https://qz.com/1327920/microsoft-wants-congress-to-regulate-facial-recognition/

In 2012, the GAO reported that 41 states and the District of Columbia used face recognition technology to detect fraud in driver's license applications by ensuring an applicant does not obtain a license by using the identity of another individual and has not previously obtained licenses using a different identity or identities. See GAO, *Driver's License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*, GAO-12-893 (Washington, D.C.: Sept. 21, 2012).

Recent research has revealed that up to 50 agencies across the United States, including the FBI and the New York Police Department, have used facial recognition technology in some way, such as finding a fake ID, finding someone fraudulently stealing people's identities and using cameras in a public square to gather data in order to look for and apprehend a wanted fugitive. The U.S. Customs and Border Protection now uses facial recognition in many airports and ports of sea entry. At airports, international travelers stand before cameras and have their pictures matched against photos provided in their passport applications. CBP says the process complies with privacy laws, but it has still come in for criticism from the Electronic Privacy Information Center, which argues that the government, though promising travelers that they may opt out, has made it increasingly difficult to do so.

State, Local and Federal Government Bans on Facial Recognition Technology

On May 14, 2019, San Francisco adopted the "Stop Secret Surveillance" ordinance to became the first American city to ban its law enforcement agencies from using facial recognition systems and technology. The SF ordinance (full text of file # 190110 accessible at https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019) also requires city departments to disclose any surveillance technologies they currently use or plan to use, and to spell out policies regarding them that the Board of Supervisors must then approve. The ban does not affect personal, business or federal government use of facial recognition technology.

Other cities considering a similar ban include Oakland and Berkeley, California, and Somerville, Massachusetts, and the state legislatures of California and Washington are moving forward with proposed bans on facial recognition being used in body cameras, including a statewide ban on facial recognition and face surveillance as applied to public schools. A bill in the Massachusetts State Legislature would put a moratorium on facial recognition and other remote biometric surveillance systems.

On the federal level, S.847, the *Commercial Facial Recognition Privacy Act of 2019*, introduced during the current 116th Congress, would ban users of commercial face recognition technology from collecting and sharing data for identifying or tracking

consumers without their consent, although it does not address the government's uses of the technology.

FBI's Use of Facial Recognition Technology

For decades, fingerprint analysis was the most widely used biometric technology for positively identifying arrestees and linking them with any previous criminal record. However, beginning in 2010, the FBI began incrementally replacing the Integrated Automated Fingerprint Identification System (IAFIS) with Next Generation Identification (NGI). NGI was not only to include fingerprint data from IAFIS and biographic data, but also to provide new functionality and improve existing capabilities by incorporating advancements in biometrics, such as face recognition technology. As part of the fourth of six NGI increments, the FBI updated the Interstate Photo System (IPS) to provide a face recognition service that allows law enforcement agencies to search a database of criminal photos that accompanied fingerprint submissions using a photo of an unknown person—called a probe photo. The FBI began a pilot of NGI-IPS in December 2011, and NGI-IPS became fully operational in April 2015. See *Additional Work Remains*, infra, at https://www.gao.gov/assets/700/699489.pdf

NGI-IPS users include the FBI and selected state and local law enforcement agencies, which can submit search requests to help identify an unknown person using, for example, a photo from a surveillance camera. When a state or local agency submits such a photo, NGI-IPS uses an automated process to return a list of candidate photos from the database. The number of photos returned ranges from 2 to 50 possible candidate photos from the database, depending on the user's specification. According to the FBI, in fiscal year 2018, NGI-IPS returned about 50,000 face recognition search results to law enforcement agency. Id.

House Committee on Oversight and Reform

In a May 22, 2019 hearing before the House Committee on Oversight and Reform, entitled "*Facial Recognition Technology: Its Impact on our Civil Rights and Liberties,*" the Committee announced it was convened for the purpose of examining the use of facial recognition technology by government and commercial entities and the need for oversight on how it is used on civilians. Among the findings was the revelation that the United States Supreme Court has not directly ruled on the constitutionality of local, state or federal law enforcement use of facial recognition technology upon citizens, although we now see that there are potential questions under the First, Fourth and Fourteenth Amendments of the U.S. Constitution arising from government use of such technology.

Federal Agency Use of Personal Information

Federal agency collection and use of personal information, including face images, is governed primarily by two laws: The Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice (SORN) in the Federal Register.

Privacy Impact Statements under the E-Government Act of 2002

The E-Government Act of 2002 requires that agencies conduct Privacy Impact Assessments (PIAs) before developing or procuring information technology (or initiating a new collection of information) that collects, maintains, or disseminates personal information. The assessment helps agencies examine the risks and effects on individual privacy and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. OMB guidance also requires agencies to perform and update PIAs as necessary where a system change creates new privacy risks, for example, when the adoption or alteration of business processes results in personal information in government databases being merged, centralized, matched with other databases or otherwise significantly manipulated.

GAO Recommendations to FBI

In May 2016, the Government Accountability Office (GAO) found that the U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) could improve transparency and oversight to better safeguard privacy and had limited information on accuracy of its face recognition technology. GAO made six recommendations to address these issues. As of May 2019, DOJ and the FBI had taken some actions to address three recommendations—only one of which the FBI has fully implemented—but has not taken any actions on the other three. See GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

In GAO's May 2016 Report, it found that DOJ did not complete or publish key privacy documents for FBI's face recognition systems in a timely manner and made two recommendations to DOJ regarding its processes for developing these documents. These included privacy impact assessments (PIA), which analyze how personal information is collected, stored, shared, and managed in federal systems, and system of records notices, which inform the public about, among

other things, the existence of the systems and the types of data collected. While DOJ has taken actions to expedite the development process of the PIA, it has yet to take action with respect to the development process for system of records notices (SORNs). GAO continues to believe both recommendations are valid and, if implemented, would help keep the public informed about how personal information is being collected, used and protected by DOJ components. GAO also recommended the FBI conduct audits to determine if users of FBI's face recognition systems are conducting face image searches in accordance with DOJ policy requirements, which the FBI has done.

One of every two Americans already is captured in a face-recognition database accessible to law enforcement, according to a 2016 study at Georgetown Law. This data is mostly stored in the Federal Bureau of Investigation's Next Generation Identification Interstate System, which has about 411 million individual photos. In a May 2016 report, discussed below, the U.S. Government Accountability Office admonished the FBI for failing to disclose the extent to which it uses the technology, and to ensure privacy and accuracy.

In a June 4, 2019 letter from GAO to the U.S. Department of Justice, the status of these six priority recommendations made in May 2016 on use of facial recognition technology was laid out. See Testimony before House Committee on Face Recognition Technology, *DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, accessible online at https://www.gao.gov/assets/700/699489.pdf. See also GAO, *Priority Open Recommendations: Department of Justice*, GAO-19-361P (Washington, D.C.: Apr. 10, 2019) ("Additional Work Remains").

The House Oversight Chairman, Elijah Cummings, set the tone for the Committee's hearing:

> We need to do more to safeguard the rights of free speech and assembly under the First Amendment, the right to privacy under the Fourth Amendment, and the right of equal protection under the Fourteenth Amendment.

The former President of the National Organization of Black Law Enforcement Officers also emphasized the need for a high standard in this area of law:

> If you're going to develop this technology, it's going to have to meet a standard being articulated by the scientists and those in the legal community that are here. If it can't meet that standard, then there's no place for it in our society.

Among its key findings, the House Committee on Oversight and Reform found that facial recognition technology misidentifies women and minorities at a much higher rate than white males, increasing the risk of racial and gender bias. This is consistent with a particularly egregious example provided by the American Civil Liberties Union (ACLU), which recently ran a test of Amazon's facial recognition software and found it incorrectly misidentified 28 black members of Congress as criminals. MIT Researchers found that overall the software returned worse results for women and darker-skinned individuals. Amazon has disputed these findings. Similarly, in Maryland, police agencies have been accused of generally using facial recognition technology more heavily in black communities and to target activists — for example, police in Baltimore used it to identify and arrest protesters of Freddie Gray's death at the hands of law enforcement. Shirin Ghaffary, *San Francisco's facial recognition technology ban, explained,* May 14, 2019, VOX, accessible at https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained

Amazon's Marketing of Facial Recognition Technology

Amazon is moving forward with marketing facial recognition technology to police departments and helping the AI community behind the technology learn how to apply it. The Washington Post's national technology reporter, Drew Harwell, has pointed out the scope of this technology:

> These systems learn faces by looking at millions of them – that's how they pick out the differences between the width between eyes and how someone looks when they're grimacing, and all the different little micro expressions and little ticks that we have in our faces.

Mary Harris, *Amazon Encourages Police to Use Untested Facial Recognition Technology*, Slate.com, May 24, 2019, accessible online at https://slate.com/news-and-politics/2019/05/facial-recognition-police-officers-hillsboro-oregon-amazon.html.

Microsoft's ICE Contract

Microsoft came under scrutiny last year relating to its contract with ICE (U.S. Immigration and Customs Enforcement) that was alleged to provide facial recognition technology while the U.S. Government was separating families at the U.S. – Mexico border. After pitching its facial-recognition system in the summer of 2018 to ICE officials as a way for the agency to target or identify immigrants, a move that could shove Microsoft further into a growing debate over the industry's work with the government. A June 2018 meeting in Silicon Valley was revealed in emails as part of a Freedom of Information Act request by the advocacy group Project on Government Oversight, and the emails were published first in the Daily Beast, showing that ICE officials and Microsoft Web Services talked about

implementing the company's Rekognition face-scanning platform to assist with homeland security investigations. A Microsoft Web Services official who specialized in federal sales contracts, and whose name was redacted in the emails, wrote that the conversation involved "predictive analytics" and "Rekognition Video tagging/analysis" that could possibly allow ICE to identify people's faces from afar — a type of technology immigration officials have voiced interest in for its potential enforcement use on the southern border. Microsoft's president later clarified that it was only providing email, calendar, messaging and electronic storage services, but not facial recognition. Colin Lecher, *Microsoft says it doesn't work on ICE facial recognition and calls for regulation,* The Verge, July 13, 2018, accessible at https://www.theverge.com/2018/7/13/17568558/microsoft-ice-facial-recognition

Around the same time that Microsoft was explaining its contractual relationship with ICE, it also sought congressional support for a bipartisan, expert-led committee to draft regulations for facial recognition in July 2018. Microsoft's president, Brad Smith, emphasized that regulation was needed to lay the foundations for what the U. S. Government can and cannot do with the technology, to create safeguards for citizens against constant surveillance facilitated by the technology, and to effectively and proactively manage the technology to insure that it works for all, regardless of appearance or skin tone.

FTC Calls For National Privacy Law

On May 8, 2019, members of the Federal Trade Commission (FTC) called on Congress to enact a national privacy law that would regulate how large tech companies collect and handle user data, the most valuable currency in the internet economy, and also strengthen the FTC's ability to police violations and provide greater authority and resources to impose penalties. This call for federal legislation did not come in a vacuum, but took place following the FTC's year-long investigation into alleged privacy violations by Facebook and shortly before the FTC rendered a major decision, discussed below, that will provide guidance for future enforcement of online privacy and a blueprint for regulation.

Facebook's Woes With the Federal Trade Commission

Facebook's privacy practices were the subject of complaints filed with the Federal Trade Commission by a coalition of consumer groups and the Electronic Privacy Information Center. Ultimately, Facebook entered into a 2012 consent order in which it sought to put to rest charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. The 2012 settlement required Facebook to take several steps to make sure it lives up to its promises in the future, including giving consumers clear and prominent notice and obtaining consumers' express

consent before their information is shared beyond the privacy settings they have established.

The FTC had charged that Facebook had made privacy promises to American consumers but unfairly and deceptively failed to live up to them. "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users," according to FTC Chairman Jon Leibowitz, Chairman of the FTC, who asserted that "Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not." *Facebook Settles FTC Charges*, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep (Nov. 29, 2011)
These are the highlights of the charges that led to the 2012 consent order:

1. In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn't warn users that this change was coming, or get their approval in advance.
2. Facebook represented that third-party apps that users' installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data – data the apps didn't need.

3. Facebook told users they could restrict sharing of data to limited audiences – for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.

4. Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It didn't.

5. Facebook promised users that it would not share their personal information with advertisers. It did.

6. Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.

7. Facebook claimed it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't.

Under the FTC consent order, Facebook was barred from making any further deceptive privacy claims, was required to get consumers' approval before it changed the way it shared their data, and was required to obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years.

Specifically, the consent order barred Facebook from making misrepresentations about the privacy or security of consumers' personal information; required Facebook to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences; required Facebook to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account; required Facebook to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services; required Facebook to protect the privacy and confidentiality of consumers' information; and required Facebook, within 180 days, and every two years after for the next 20 years, to obtain independent, third-party audits certifying that it had a privacy program in place that met or exceeded the requirements of the FTC consent order, and to ensure that the privacy of consumers' information is protected. *FTC Decision and Order in the Matter of Facebook,, Inc.*, July 27, 2012, accessible at https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf

Facebook Friends and Cambridge Analytica

The FTC has on occasion been criticized as being toothless on privacy. Maybe that criticism was not fully merited, as political pressure is mounting for the FTC to take a tougher line against Facebook and other big tech companies. The ongoing FTC probe into Facebook's privacy missteps and investigation into Facebook's potentially problematic privacy practices took another twist and became even more complicated when reports surfaced that the personal data of tens of millions of Facebook users had ended up in Cambridge Analytica's hands during the 2016 Presidential Campaign of Donald Trump. Cambridge Analytica was a data firm that worked on the 2016 campaign of President Trump, and it shut down in 2018 amidst allegations about Facebook data and other questions about its political activities. It is just now coming to light that Facebook's personality-prediction app has gathered data from tens of millions of users and shared the information with Cambridge Analytica. Id. at A5.

Cambridge Analytica had secured political consulting work in the U.S. by promising to use data to profile and influence voters with political messages, and in this case the Facebook user data reached beyond users who downloaded the Facebook app to include data about their Facebook friends. The FTC investigation centered on whether this lapse in security violated the 2012 consent order under which Facebook had agreed to better protect user privacy. Id.

Ultimately, in a settlement that could exceed the previous record penalty for violating an FTC order and that is higher than what the EU could have sought under its privacy laws, the FTC endorsed a $5 Billion settlement with Facebook, subject to being finalized by the Civil Division of the U.S. Department of Justice.

Facebook Penalty is Set at $5 Billion, July 13, 2019, Wall Street Journal Weekend, at 1. The settlement is anticipated to tighten government restrictions on how Facebook treats user privacy, but the Democratic minority on the FTC was pushing for even tougher oversight. Id. Besides being over 200 times greater than the previous monetary fine leveled by the FTC, this settlement goes beyond financial ramifications. Facebook would be required to document every decision involving user data before introducing new products and monitor third-party apps to ensure they are not inappropriately tapping into consumer data. Facebook's top executives would be required to attest to Facebook's efforts to protect user privacy.

One of the issues that divided the three Republican commissioners from the two Democratic commissioners, fueled by the fact that Facebook was being perceived as a repeat offender, was the extent to which CEO Mark Zuckerberg should be held personally accountable for future missteps. Id. *Facebook is Staring Down a Record-Setting $5 Billion Fine*, July 15, 2019, USA Today, accessible at https://www.usatoday.com/story/money/2019/07/15/facebook-fined-5-billion-ftc-cambridge-analytica/39687137/ During earlier proceedings before the FTC, the three Republican commissioners were at loggerheads with the two Democratic commissioners on the appropriate punishment that should be meted out to Facebook and the role of executive responsibility. The Democratic commissioners suggested making the punishment strong enough to being home the message that a tech company violating privacy rules must change its behavior, and with big tech companies treating fines like a parking ticket and just the cost of doing business, the FTC should name top executives as financially liable parties and find out who at the top called the shots, and the fines should be painful. Cecelia Kang, *FTC Members Prod Congress on Privacy*, NYT Business, at B3, May 9, 2019; FTC Commissioners Back Privacy Law, NYT May 8, 2019, accessible online at https://www.nytimes.com/2019/05/08/business/ftc-hearing-facebook.html?auth=login-email&login=email

Amazon's Challenge: Children's Online Privacy Protection Act & Echo Dot

The children's smart-speaker market was graced with the presence of a colorful device called *Echo Dot* Kids Edition, marketed by tech giant Amazon, who played up the device as a simple way for youngsters to converse with Amazon's voice-activated virtual assistant, Alexa. Two advocacy groups found, however, that the device enabled children to divulge their names easily to Alexa, along with home addresses, social security numbers, and other intimate personal information. Parents experienced a cumbersome process as they sought to delete their child's personal details from the system. Natasha Singer, *Critics Assail Amazon Over Children's Privacy*, NYT Business at B3, May9, 2019; *Amazon Flunks Children's Privacy, Advocacy Groups Charge*, The New York Times, May 9, 2019, accessible online at https://www.nytimes.com/2019/05/09/technology/amazon-childrens-privacy-echo-dot-kids.html

A dozen advocacy groups filed an FTC complaint charging Amazon with violations of the Childrens' Online Privacy Act, a federal statute that protects the personal information of people under the age of 13. Among them were Campaign for a Commercial-Free Childhood and the Center for Digital Democracy. Amazon, they alleged, had failed to obtain verified consent from parents before collecting their children's voice recordings and kept those records unnecessarily after extracting the data to respond to the children. While Amazon says its Alexa device and its subscription service for children, Free Time Unlimited, comply with the Children's Online Privacy Protection Act, the advocacy groups said that once a parent purchases this device for his or her child, they are essentially ceding control of their child's data to a voice-activated device that lives in a home. Id.
Amazon says that before children's subscription services can be used on Alexa, the user must consent and provide a credit card number or a code number sent via text message by Amazon.

Amazon's Echo Dot kids device has come under scrutiny as a time when parents, advocacy groups and regulators consider voice recordings to be among the most sensitive types of children's data. This particular device records children's voice commands and uses artificial intelligence to respond. For example, children can ask the device to play music, answer questions, tell jokes or remember information they tell it, but advocacy groups charge that parents are not being provided with clear explanations of their data practices and clear instructions for deleting a child's information as soon as it is no longer needed to fulfill the service for which it was collected. Id.

The Echo Dot Kids Edition was tested by researchers by having a child ask Alexa to remember a made-up phone number, social security number, home address and phrases like "I am allergic to peanuts". When the researchers testing the device used parental controls to delete the voice recordings, Alexa still remembered and was able to repeat the personal information included in the recordings. In order to delete the underlying data, researchers had to contact Amazon Customer Service and ask to have the child's entire profile deleted. Amazon's executive response was that Amazon kept a child's voice recordings indefinitely by default, retaining them for the parent's review until the parent deletes them. Id.

In June 2019, Amazon came back on the market with a new version of Echo Dot Kids Edition, enlisting Family Online Safety Institute (FOSI) to help build FreeTime. According to Amazon:

> To access FreeTime on Alexa, verifiable parental consent is required. None of the Alexa skills included within FreeTime Unlimited have access to or collect personal information from children, and there are multiple ways to delete a child's profile or voice recordings. Parents can review and delete recordings

through the Alexa app or the Alexa Privacy Hub, and contact Customer Service to request deletion of their child's profile.

Jonathan Schieber, *Amazon revamps Echo Dot Kids Edition and FreeTime* (June 2019), accessible online at *https://techcrunch.com/2019/06/12/amazon-revamps-echo-dot-kids-edition-and-freetime/*

The Future of National Privacy Legislation in the USA?

With calls from the FTC, big tech giants and privacy advocacy groups, one would think that the time is ripe for the U.S. Congress to consider and act upon a reasonable proposal for a national privacy law to regulate the collection and handling of user data. But the devil is always in the details, and progress has stalled over disagreements on the details of such a national data privacy law, putting the USA even farther behind the EU in the global movement to curb the growing power of big tech companies. Id.

California Consumer Protection Act of 2018

The appeal of high standards for data protection has been a natural consequence of the EU date protection, EU market power, and EU negotiating strategies. This appeal was also a factor leading to California's enactment of the California Consumer Protection Act of 2018 (CCPA), which goes into effect on January 1, 2020. This state legislation incorporates the core concepts of the EU data protection regime into a GDPR-like state statute, including the following rights:

1. An individual's right to know what information a business has collected about him or her;
2. A right to "opt out" of allowing a business to sell one's personal information to third parties;
3. A right to deletion;
4. A right to data portability; and
5. A right to receive equal services and pricing from a business, even if one exercises his or her rights under the CCPA.

Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y. L. Rev. 1, 28 (2019), accessible online at https://paulschwartz.net/wp-content/uploads/2019/02/Schwartz_Global_Data_Privacy_the_EU_Way_2.pdf ("The EU had not set up a policy shop in Sacramento, California. It had not lobbied the state legislature or Governor to enact a GDPR-like law. Yet, somehow, the ideas of EU data protection made their way to the Golden State." Id. at 28)

The GDPR is automatically applied to all 27 member states of the European Union as of May 25, 2018, and includes the rights enumerated above. It is designed to protect the personal data1 of the approximately 508 million people in the EU and imposes new requirements on organizations that process data and are either established in the EU or, in some cases, established exclusively outside the EU> European Union (EU). After the Peoples Republic of China and India, the EU has the third largest geo-political population in the world. Widespread adoption of the GDPR is driven by its broad application within the EU and its territorial scope set out in Article 3, coupled with the spectre of heavy fines detailed in Articles 83 and 84.

On the other side of the pond, the United States has a different approach and substantially different culture with respect to individual rights and data privacy protection. The United States model has been criticized as "a patchwork of sector-specific laws that fail to adequately protect data" with no individual right to data privacy or date protection guaranteed in the U.S. Constitution.

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, and broadly applies to American companies. The International Association of Privacy Professionals reports that over half a million U.S. companies are likely impacted by the CCPA, which may also apply to those operating outside the U.S. too. Thus, the fact that a business does not have a physical location in California does not necessarily exempt it from its legal obligation to comply with the CCPA. Catherine Barrett, *Are the EU GDPR and the California CCPA Becoming the De Facto Global Standards for Data Privacy and Protection*? 15 Scitech Lawyer 24 (Spring 2019)

This brings us to the rampant privacy violations, obstruction of justice, data manipulation, disinformation campaigns and unprecedented wrongdoing at the highest level of government that allegedly took place as part of Russia's interference with the American electoral and political system documented in the recently concluded Mueller investigation.

The Mueller Report

The role of social media, data privacy concerns, and political wrongdoing came to light during the two year investigation by Special Counsel Robert Mueller, former Director of the Federal Bureau of Investigation. Mueller addressed Russian interference with the 2016 Presidential Election in his ten minute statement at the U.S. Department of Justice on May 29, 2019. During those brief remarks, which came at the time he resigned from the DOJ and returned to private live, Mueller summarized key indictments that had been secured by his investigative team in the Southern District of New York and the District of Columbia, along with the

principal findings of the over 440-page report based on a two year investigation. He described "multiple, systemic efforts" by Russian intelligence officers and Russian military officials to interfere with America's political system.

During the 2016 Election, Mueller emphasized – at least for those who have not yet taken the time to read the report – that "Russian intelligence officer who were part of the Russian military launched a concerted attack on our political system," in which they used "sophisticated cyber techniques to hack into computers and networks used by the Clinton campaign," "stole private information, and then released that information through fake online identities and through the organization WikiLeaks … designed and timed to interfere with our election and to damage a presidential candidate" while "a private Russian entity engaged in a social media campaign where Russian citizens posed as Americans in order to interfere with the election." *Justice News*, May 29, 2019, accessible at https://www.justice.gov/opa/speech/special-counsel-robert-s-mueller-iii-makes-statement-investigation-russian-interference.

With that opening for a discussion and evaluation of the American and German perspectives on data privacy, individual privacy and security, we come to the crossroads as we enter the complex, interdependent global arena.

At this somber crossroads, one cannot downplay the serious consequences and misfortunes that beset those people, companies and nations that may have become ensnared in unintended or perhaps intended violations of privacy rights, data privacy norms and data protection regulations. Nonetheless, one is tempted to ask the question that may have been overheard following the assassination of President Abraham Lincoln, perhaps as a cabinet member was consoling the President's grieving widow: "Other than that, how was the play, Mrs. Lincoln?"

Russia's Use of Social Media

The other shoe dropped on October 8, 2019, when the Senate Select Committee on Intelligence released a new report entitled, "Volume II: Russia's Use of Social Media." This is the second volume released in the Committee's bipartisan investigation into Russia's attempts to interfere with the 2016 U.S. election, and the full text of the report is accessible online at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

The report on Russia's Use of Social Media examines Russia's efforts to use social media to sow societal discord and influence the outcome of the 2016 election, led by the Kremlin-backed Internet Research Agency (IRA). The analysis draws on data provided to the Committee by social media companies and input from a Technical Advisory Group comprising experts in social media network analysis,

disinformation campaigns, and the technical analysis of complex data sets and images to discern the dissemination of disinformation across social media platforms. https://www.burr.senate.gov/press/releases/senate-intel-committee-releases-bipartisan-report-on-russias-use-of-social-media-

The report details how Russia took advantage of America's openness and innovation, exploiting American-bred social media platforms to spread disinformation, divide the public, and undermine democracy. Vice-Chairman Mark Warner emphasized that with the 2020 elections on the horizon,

> there's no doubt that bad actors will continue to try to weaponize the scale and reach of social media platforms to erode public confidence and foster chaos. The Russian playbook is out in the open for other foreign and domestic adversaries to expand upon – and their techniques will only get more sophisticated. …
>
> We also need to give Americans more control over their data and how it's used, and make sure that they know who's really bankrolling the political ads coming across their screens. Additionally, we need to take measures to guarantee that companies are identifying inauthentic user accounts and pages, and appropriately handling defamatory or synthetic content. It's our responsibility to listen to the warnings of our Intelligence Community and take steps to prevent future attacks from being waged on our own social media platforms." Id.

Key findings and recommendations of "Russia's Use of Social Media"

1. The Committee found that the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin. The Committee found that IRA social media activity was overtly and almost invariably supportive of then-candidate Trump to the detriment of Secretary Clinton's campaign.
2. The Internet Research Agency's (IRA) targeting of the 2016 U.S. election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society. While the IRA exploited election-related content, the majority of its operations focused on exacerbating existing tensions on socially divisive issues, including race, immigration, and Second Amendment rights.
3. The Committee found the IRA targeted African-Americans more than any other group or demographic. Through individual posts, location targeting, Facebook pages, Instagram accounts, and Twitter trends, the IRA focused

much of its efforts on stoking divisions around hot-button issues with racial undertones.

4. The IRA engaged with unwitting Americans to further its reach beyond the digital realm and into real-world activities. For example, IRA operatives targeting African-Americans convinced individuals to sign petitions, share personal information, and teach self-defense courses. Posing as U.S. political activists, operatives sought help from the Trump Campaign to procure campaign materials and to organize and promote rallies.
5. The Committee found IRA activity increased, rather than decreased, after Election Day 2016. Analysis of IRA-associated accounts shows a significant spike in activity after the election, increasing across Instagram (238 percent), Facebook (59 percent), Twitter (52 percent), and YouTube (84 percent). Researchers continue to uncover IRA-associated accounts that spread malicious content.
6. The Committee recommends social media companies work to facilitate greater information sharing between the public and private sector. Because information warfare campaigns are waged across a variety of platforms, communication between individual companies, government authorities, and law enforcement is essential for fully assessing and responding to them. Additionally, social media companies do not consistently provide a notification or guidance to users who have been exposed to inauthentic accounts.
7. The Committee recommends Congress consider ways to facilitate productive coordination and cooperation between social media companies and relevant government agencies. Congress should consider whether any existing laws may hinder cooperation and whether information sharing should be formalized. The Committee also recommends Congress consider legislation to ensure Americans know the source behind online political advertisements, similar to existing requirements for television, radio, and satellite ads.
8. The Committee recommends the Executive Branch publicly reinforce the danger of attempted foreign interference in the 2020 election. The Executive Branch should establish an interagency task force to monitor foreign nations' use of social media platforms for democratic interference and develop a deterrence framework. A public initiative to increase media literacy and a public service announcement (PSA) campaign could also help inform voters.
9. The Committee recommends candidates, campaigns, and other public figures scrutinize sourcing before sharing or promoting new content within their social media network. All Americans should approach social media responsibly to prevent giving "greater reach to those who seek to do our country harm."
10. The Committee recommends that media organizations establish clear guidelines for using social media accounts as sources to prevent the spread of state-sponsored disinformation.

These findings and recommendations are alarming in their specificity and gravity, and two of the recommendations provide particularly relevant guidance for privacy, security and data protection.

Recommendations for data security, data protection, and privacy

First, the report states that "[b]road, effective data security and privacy policies, implemented across the platforms and enforced by a tough, competent government regulator, are necessary to prevent the loss of consumers' data and the abuse of that data in election influence campaigns." In this connection, the report calls upon Congress to enact legislation that addresses this concern in three ways:

(1) The Federal Trade Commission must be given the power to set baseline data security and privacy rules for companies that store or share Americans' data, as well as the authority and resources to fine companies that violate those rules;
(2) Companies should be obligated to disclose how consumer information is collected and shared and provide consumers the names of every individual or institution with whom their data has been shared.
(3) Consumers must be given the ability to easily opt out of commercial data sharing.

Second, companies holding private information on Americans "also must do far more to protect that information from hacking." This must include "telecommunications companies that hold information about customers' communications, web browsing, app · usage and location. Too much of this information is held for too long, increasing the risk that it will be hacked. Besides strengthening their cyber security practices, companies can take steps to delete consumer information as soon as it is not absolutely necessary for business purposes."

The Privacy Paradox

Young people today in comparison to Baby Boomers represent what may be the largest generational divide since the early days of Elvis Presley and his swivel-hipped introduction to America and the world on the Ed Sullivan Show. Loosely defined as GenX and Millennials, young people provide large amounts of personal information as they open up their private lives online. All of this digital treasure trove is swept up by commercial and governmental entities, while the older generation of Baby Boomers look on in amazement as they see a vast public intrusion into the individual lives through almost unaccountable internet access to highly sensitive personal information.

Before we get into the national characteristics and history of the people of America and Germany in this context, let us consider as a threshold matter the privacy differences between these age groups, not to mention the racial, ethnic, gender, religious and socioeconomic differences. These are differences that, for better or worse, may have an outcome-determinative impact on how people present their private lives in an online context.

Digital or online privacy can be rationally evaluated from many perspectives, but for our purposes, let us consider evaluating it in terms of a perceived inability on the part of many internet users to manage their own online privacy and to control the privacy of and access to their personal information. This remains a major unresolved issue, and not just an issue in the context of social media communications.

The attention we give to online privacy, moreover, can be affected by such negative experiences on the internet as viruses, misrepresented purchases, identify theft, request for bank details, spam and inadvertently reaching a porn website.

We can gain a better understanding of these issues in a thoughtful analysis entitled "*A New Privacy Paradox: Young People and Privacy on Social Network Sites,*" an August 17, 2014 presentation by Grant Blank, Gillian Bolsover, and Elizabeth Dubois to the American Sociological Association, accessible at https://poseidon01.ssrn.com/delivery.php?ID=746089005127104068002118096121019000058054059002002048118072114011067111068115069074003063123097024005008124013084065106102010039032060058020113093029029020085101110010036010118099076099117078011067094103031103123082007095115097089021117126109022096090&EXT=pdf. This presentation concludes that young people are much more likely than older people to have taken action to protect their privacy on (social network sites). Id. at 23. This is despite the inadequacy of controls for users as they seek to meet their diverse privacy needs. Id. at 30.

Fake News and Computational Propaganda

Computational propaganda is the automated dissemination of fake news, propaganda and other forms of junk news, particularly the polarizing type that grew like a wildfire during the 2016 U.S. Presidential Election and appears to have increased in intensity since that time. Misinformation and disinformation can be disseminated online, often leading many to conclude that fake news may well have led to Donald John Trump's victory in the race for President, but the jury is still out on that issue. Social media platforms in key battleground states like Michigan, Pennsylvania, West Virginia, North Carolina and Wisconsin may well have

spawned enough junk news to neutralize if not surpass legitimate professional news. *Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?* The Computational Propaganda Project, March 26, 2017, accessible at https://comprop.oii.ox.ac.uk/research/working-papers/junk-news-and-bots-during-the-u-s-election-what-were-michigan-voters-sharing-over-twitter/

Junk News in the 2017 German Federal Presidency Election

In the 2017 German Federal Presidency Election, junk news made up a large proportion of information shared by Twitter users, with right-wing sources being the most shared junk news sources. Given the Alternatif für Deutschland's far-right traffic, candidate Albrecht Glaser received a disproportionate amount of Twitter activity given the far right share of voter support.

Junk news and other forms of computational propaganda at sensitive times in public life can lead to a rapid spreading of online disinformation, one of the top 10 perils to society identified by the World Economic Forum. Junk News and Bots, supra at 1.

Deliberate manipulation of non-factual, sensational information online, coupled with the online media's less rigorous journalistic standards and practices, the absence of fact-checking and the absence of content derived from reliable sources, provide unique weapons for state and non-state political actors who thrive on publishing misleading, deceptive or false information purporting to be real news regarding culture, economics or politics. This perverse phenomenon is weaponized and made more potent by political bot, dissemination algorithms and other vehicles to spread content that is extremist, masked commentary, sensationalist and other forms of fake news.

For example, in the weeks running up to the German elections in 2017, a right-wing group "Reconquista Germanica" was called out by *Der Spiegel* for declaring a "war of memes" on the German government. Its tools were disinformation and political bots aimed at ginning up support for AfD and targeting Chancellor Angela Merkel. *Junk News and Bots*, supra at 2. A network of automated Facebook accounts was formed to have steered 31 pro-AfD secret Facebook groups.

As far back as November 2016, Angela Merkel warned the Bundestag about the influence social bots and digital information could have on the formation of public opinion. *Junk News and Bots*, supra at 2. The major parties, SPD, CDU/CSU, Bündnis 90/Die Grünen and Die Linke, disavowed use of social bots in elections and voiced disapproval over their use, while the right-wing AfD trumpeted that it would "consider the use of social bots for elections," a statement it later walked back.

This has made computational propaganda a hot political issue in Germany, leading to public concerns of election meddling and voter manipulation. *Junk News and Bots*, supra at 2. Defamatory and junk news content can now lead to fines being levied on social networking companies under the recently enacted Netzwerkdurchsetzungsgesetz (NetzDG).

At the other end of the spectrum are concerns over undue burdens on freedom of expression. Junk News and Bots, supra at 2. The right-wing oppositional party, AfD, is dominant on Twitter. Junk News and Bots, supra at 5. Along with social networking sites like Facebook, Instagram and Sina Weibo, Twitter has proven to be the favorite late night and early morning political trumpet of the U.S. President, whose "Tweet storms' have found a reliable audience in what he calls "my base." In reality, and particularly during the run-up to the 2016 Presidential election, the code-driven tools of computational propaganda were prevalent on Twitter and other social networking sites. The massive manipulation of opinion through such social media, coupled with autonomous agents and algorithms, have exposed a very concrete risk of shaping ideological viewpoints through manipulation of conversations, demobilizing opposition, and generation of false support. *Computational Propaganda in Germany: A Cautionary Tale*, accessible at https://comprop.oii.ox.ac.uk/uncategorised/computational-propaganda-in-germany-a-cautionary-tale/, at 3.

These are the modern weapons being used by state and non-state political actors to spread disinformation, engage with citizens and influence political outcomes. Id. at 3.

During the Bundeswahlen 2017, massive right-wing currents were evident and likely had an impact on public discourse. Id. at 3. The rise of right-wing populist movements in Germany has come on the heels of the European Sovereign Debt Crisis, Eurocrisis Salvation politics, the perception of a crumbling Eurozone, the European refugee debate and anti-immigration sentiment, all problems not limited Germany. The 2017 elections in Germany have resulted in a pluralistic, multiparty parliament that will now drive political decisions for the next four years. Id. at 5. The pivotal role of Germany is European politics is seen starkly in its perceived position as the economic powerhouse of Europe and the last defenders of the liberal West. Id. at 5.

These are some of the factors that have made Germany a vulnerable target for manipulation, distortion and misdirection of public opinion. Id. at 5. That public opinion has been tampered with by fake news sites, hate speech, political and social bots, terminology confusion and misconceptions, trolling, self-enforcing opinion and amplification through algorithms, just as Chancellor Angela Merkel warned in her annual budget address in late November 2016.

Data Privacy and a CLOUD of Uncertainty

One of the most recent analyses of data privacy and privacy protections came in a 2018 case before the United States Supreme Court. The differences in the German and American perspective on privacy were highlighted in an Amicus Curiae brief filed by Gesellschaft Für Freiheitsrechte (GFF) in support of Microsoft in *United States v. Microsoft Corporation,* No. 17-2 (U.S.). https://www.supremecourt.gov/DocketPDF/17/17-2/28727/20180122153932882_17-2%20bsac%20Gesellschaft.pdf (hereinafter GFF Amicus Brief).

Procedurally, federal law enforcement agents in 2013 obtained a warrant from the Southern District of New York requiring Microsoft to disclose all e-mails and other information associated with the account of one of its customers. The warrant directed Microsoft to disclose to the Government the contents of a specified e-mail account and all other records or information associated with the account to the extent that the information was within its possession, custody, or control. It so happened that Microsoft determined after being served with the warrant that the account's e-mail contents were stored in a sole location, its datacenter in Dublin, Ireland, and Microsoft moved to quash the warrant with respect to the information stored in Ireland, a member state of the European Union.

The question before the United States Supreme Court was whether 18 U.S.C. § 2703 authorized a court in the United States to issue a warrant that compels a U.S.-based provider of email services to disclose data stored outside of the United States, in this case Germany. GFF supported Microsoft in seeking to have enforcement of the warrant denied. In the Microsoft case, we were provided with a meaningful explanation of how Germany's history from World War II through 1989 had created in her society "a strong sense of the need for the protection of individual privacy—even while providing a way for society to protect itself from crime and terrorism."

GFF provided a clear picture of the legal background for Germany's recognition of the right to data protection as a fundamental right incorporated into the German Constitution and reflected in the E.U.'s constitutional standards for data protection:

In Germany, it is understood as the right to informational self-determination and the right to the confidentiality and integrity of information technology systems which both derive from the general right to privacy contained … the German Basic Law. The scope, explicitly determined by the German Federal Constitutional Court, rests on two principles. First, on the understanding of an individual as a self-determined human being living in a free society. Second, it takes into consideration modern developments in technology which, on the one hand, widen the possibilities of privacy, but at the same time open new ways of breaching privacy, which in turn leads to unpredictable risks to individual liberty. Therefore, it is crucial for individuals to be able to estimate where their data goes and who can access that

data. Considering the omnipresence of information technology systems and the rising amount of circulating data and networking systems, the State is required to protect its citizens in order to assure that their data remains confidential. As such, under German (and E.U. law), when a data subject entrusts his / her data to a service provider, the data subject does not lose their data privacy rights. GFF Amicus Brief at 3.

> The E.U. aims to set a high standard of data protection in all Member States. For this reason, it implemented the General Data Protection Regulation ("GDPR"), which will apply from May 25, 2018 and will regulate questions precisely like the one at issue in order to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. GFF Amicus Brief at 4.

GFF also made it clear that cross-border cooperation was an essential ingredient for an effective fight against crime and terrorism, and that there must be a careful balance between the right to data protection and the need for security. In short, the right to confidentiality and integrity of information technology were not absolute rights, but were

> limited by competing interests, e.g., where national security is at stake. By way of the principle of proportionality it is to be ensured that national security and data protection as a precondition for a free and democratic society are accomplished at the same time. GFF Amicus Brief at 4.

GFF emphasized that the need for cross-border cooperation was one of the underpinnings for the negotiations by the E.U. and the U.S.A for the 2003 U.S.-European Union Agreement on Mutual Legal Assistance (MLAT), ensuring their ability to collaborate on procedures for processing data and exchanging information, and that this also applies to cooperation between Germany and the United States under the 2006 U.S.-Germany Supplementary Treaty to the Treaty between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matter. "Taking into account the fundamental need for protection of personal data, the foreign access to German or European personal data is only conceivable with the restrictions of formalized procedures" like those established in the E.U. and Germany. GFF Amicus Brief at 4-5.

The core of GFF's argument for quashing the warrant was that neither Microsoft nor any other U.S. company should be required to "produce data hypothetically stored in Germany would force the addressee of that warrant to violate German and European Union (E.U.) law" while circumventing existing international treaties. That argument was an eloquent, if not disturbing, reminder of the historical context of the right of privacy and experience of German citizens relating to the behavior of government toward them:

> GFF comes before this Court with a perspective that is, perhaps, distinct from the American perspective of data privacy. The understanding of data protection and the importance of this right for German society has developed from first-hand experience with a long and stony path of human rights violations and abusive behavior by the government towards its citizens. During two brutal dictatorships—the Nazi regime from 1933 to 1945 and in this context especially the communist German Democratic Republic (GDR) from 1949 to 1989/90—Germans had to deal with steady governmental surveillance and profound violations of their human rights. GFF Amicus Brief at 6.
>
> These experiences opened the eyes of the German society to the fact that unlimited government access to personal data can have the gravest consequences for the person concerned and can be the beginning of the end of individual freedom. It was, after all, the registers of residents and punch card systems that enabled the Nazi regime to carry out their genocide with such notoriously cruel efficiency. Germans also experienced the Nazis' systemic surveillance and terror, forcing people to betray their neighbors by informing the secret police ("Gestapo") about any "deviant" behavior or the abode of persecuted individuals, which led to the known horrible consequences. GFF Amicus Brief at 6.
>
> Having survived the worst, the people of the former East Germany again found themselves in a situation of pain when the communist GDR established another regime of fear based on unlimited government surveillance. Under the communists, homes were tapped, literally millions of individuals were monitored, and lives were destroyed and even taken. Again the State used neighbors, friends and even family members to spy on its citizens in order to get as much information as possible. For forty years Germans had to fear that their best friends and family were potential informants for the GDR national security agency ("Stasi"). GFF Amicus Brief at 6-7.
>
> This history has created in German society a strong sense of the need for the protection of individual privacy—even while providing a way for society to protect itself from crime and terrorism. Situations like the Nazi or communist past cannot be allowed to happen again. Privacy protections are now guaranteed by the German Constitution and consistently protected by the jurisdiction of the highest court in Germany, the Federal Constitutional Court of Germany. GFF Amicus Brief at 7.

The Supreme Court thus had before it the clear issue of whether, when the U.S. Government has obtained a warrant under 18 U.S.C. § 2703, a U.S. provider of e-

mail services must disclose to the Government electronic communications within its control even if the provider stores the communications abroad. 583 U.S. ___, 138 S. Ct. 356, 199 L.Ed.2d 261 (2017). The Court, however, found that an intervening law had been enacted by the U.S. Congress on March 23, 2018, the Clarifying Lawful Overseas Use of Data Act (The CLOUD Act of 2018), which amended the Stored Communications Act, 18 U.S.C. § 2701 et seq., under which the subject warrant had been issued. The CLOUD Act granted the U.S. Government access to data held by U.S. firms in offshore data centers, the overall effect of which was to "widen the net of U.S. government surveillance to include both domestic and international targets … [while weakening] the due process mechanisms that typically constrain government overreach." ***Of Privacy and Power***, supra at 67.

The CLOUD Act's pertinent provision stated:

"A [service provider] shall comply with the obligations of this chapter to 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." CLOUD Act § 103(a)(1).

The Supreme Court concluded that "no live dispute remains between the parties over the issue with respect to which certiorari was granted," that a new warrant had replaced the original one, and the case was dismissed as moot. *U.S. v. Microsoft Corp.*, 138 S. Ct. 1186 (U.S. April 17, 2018).

The CLOUD Act of 2018 not only provided a means to access data held abroad by U.S.-based companies, it also created "incentives for other jurisdictions to make executive agreements with the United States over data transfer." ***Of Privacy and Power***, supra at 168. A similar regulatory measure in the form of the E.U.'s E-Evidence Regulation is now under consideration with the European Union, Id. at 168, providing the foundation for a possible E.U.-U.S. framework agreement which would facilitate "the reciprocal transfer of criminal data between the E.U. and the U.S.." Id. at 168.

Importance of Data Privacy Law: GDPR and Lessons Learned

The United States has virtually conceded the E.U.'s preeminent position on data privacy law in the global economy. The E.U. (including its strongest member, Germany) has taken the lead in recognizing the importance of data privacy law in that global digital economy. Paul M. Schwartz, Global Data Privacy: The E.U. Way, 94 N.Y. Law Review (2019).

The United States has listened, observed and hopefully learned from the E.U. as the E.U. raised the bar for privacy laws worldwide by enacting the GDPR (General Data Protection Regulation). With the adoption of the GDPR, effective May 28, 2018, this cornerstone of E.U. law in the area of data protection bestowed on the E.U. the role of the World's Privacy Cop, chiefly responsible for the protection of the fundamental right to privacy.

This E.U. view of the right of privacy as a fundamental right is in sharp contrast to the United States' view of data and information privacy as a consumer interest. That said, some of the tech giants have begun to preach the gospel of Privacy. Daisuke Wakabayashi and Brian X. X. Chen, *Google Says it has Found Religion On Privacy*, NYT Business, May 8, 2019, at B3. Google's shift in attitude on privacy comes from the company that probably knows the most about our digital lives.

Collaboration Between E.U. and U.S.

Equally significant, there have been growing calls for the United States to adopt its own comprehensive privacy legislation that would require all business to accept responsibility for how their data impacts data processing and thereby create consistent and universal protections for individuals and society as a whole.

With Europe having earned the reputation of the "world's toughest watchdog of Silicon Valley technology giants" as it moves deeper into the regulatory battleground we call the internet, Adam Satariano, *As Europe Polices Silicon Valley Titans, Critics Demand a Guard for Free Speech*, NYT May 6, 2019, at 1, the United States has undertaken a collaborative and innovative process with the E.U. to negotiate terms for international data transfers from the E.U..

This is a major step that will have a lasting impact on the legitimate expectations of privacy in the commercial world, the governmental sector and the private sector. This approach was quite different from earlier suggestions that the E.U. was acting in a unilateral fashion and exercising de facto influence over other nations through its sheer market power. On the contrary, the E.U. and the United States have engaged in bilateral negotiations to meet the GDPR's flexibly applied requirement of "adequacy" for international data transfers. Id. A more detailed discussion of the "adequacy" requirement under the 1995 Directive on Data Protection, the precursor to the GDPR, is set forth below. Id.

Evolution of the "Adequacy" Requirement and E.U.-U.S. Relations

Adequacy can be met by a nation's law as a whole, by a sub-territory within a nation, or by the terms of a specific data transfer, under both the 1995 Directive on Data Protection and the GDPR. The E.U.'s ability to determine adequacy was coupled with the ability of its regulators to exercise data embargo power, that is, to block data transfers if they were found without adequacy of protection. Global Data Privacy, supra at 11. Specifically, Article 45 of the GDPR provides an adequacy test for transfers of data outside of the E.U., setting forth a laundry list of facts that must be considered in assessing the adequacy of protection:
The rule of law; respect for human rights and fundamental freedoms; relevant legislation and its implementation; data protection rules; professional rules; and security measures. Global Data Privacy, supra at 12.

The Safe Harbor and The Privacy Shield

With respect to the E.U.'s relations with the United States concerning the adequacy requirement, the U.S. has never formally requested an adequacy determination from the European Commission. The E.U. and the U.S. have nonetheless developed two avenues for voluntary private sector compliance. These are the Safe Harbor (2000 to 2015) and the Privacy Shield (2016 to present). Both were bilateral agreements based on a streamlined list of substantive E.U. principles for U.S. companies to follow voluntarily.

At the time the Safe Harbor was agreed upon on 2000 by the Commission of the E.U. and the U.S. Department of Commerce, there were not enough votes in Congress to enact a E.U.-style privacy law, but the U.S. Government successfully negotiated an arrangement that allowed U.S. companies to voluntarily accept the Safe Harbor as a practical means of protecting E.U. citizens' data while allowing the E.U. to safeguard the economies of its member states. Id. at 18.

Key Principles of the Safe Harbor

The Safe Harbor contained seven key principles of data privacy law:
1. Notice
2. Choice
3. Onward transfer
4. Security
5. Data Integrity
6. Access, and
7. Enforcement.

While these principles can also be found in different versions and iterations of U.S. Privacy Law, the Safe Harbor incorporated them into a single document that expressed the concepts in a way that reflected E.U. data protection law. Id. at 19.

The Schrems Decision

Amidst growing controversy over whether the Safe Harbor met the adequacy standard as adjudged by the E.U. Commission, the Court of Justice of the European Union (CJEU) voided the Safe Harbor agreement in an October 2015 decision, *Schrems v. Data Protection Commissioner*, Case C-362/14, 2015 E.C.R.650 para. 73, Id. at 19n.112, ultimately finding that the Safe Harbor fell short of the Data Protection Directive's Requirements in light of the European Charter. The CJEU interprets EU law to make sure it is applied in the same way in all EU countries, and settles legal disputes between national governments and EU institutions.

One must take into account the then-current controversy over Edward Snowden's leaks regarding the U.S. National Security Agency. It was in this context that the CJEU. found that the Safe Harbor permitted "national security, public interest or law enforcement requirements" to have primacy over the data protection principles of the Safe Harbor transnational agreement, and that the Safe Harbor permitted public authorities "to have access on a generalised basis to the content of electronic communications" in a way that compromised "the essence of the fundamental right to respect for private life" guaranteed by Article 7 of the Charter.

The *Schrems* decision in short constitutionalized the "adequacy" standard for protection required for transfer of personal data from the E.U., as compared to the "equivalency" of protection required between E.U. member states. Following negotiations for a successor agreement, the E.U. and the U.S. Department of Commerce formalized the Privacy Shield which was finally approved by the E.U. Parliament in July 2016, with implementation beginning August 1, 2016.

The Privacy Shield adopts substantially the same seven principles found in the Safe Harbor and further enhances transatlantic data privacy norms. It delegates organizations to "respond expeditiously to complaints regarding compliance with the Principles, places liability on a Privacy Shield organization for damages from onward transfers to a third party who processes that personal information in a way inconsistent with the principles. Id. at 21.

It also increased an individual's ability to access his or her personal data while it limits the availability of consent as a basis for data processing to safeguard against individuals being pressured to make choices to their detriment. The United States through the Office of the Director of National Intelligence agreed that the U.S. intelligence apparatus would not engage in mass surveillance of data transferred under the Data Shield, thereby addressing the CJEU's concerns in *Schrems* about the U.S. engaging in indiscriminate mass surveillance of E.U. data. Finally, there will be periodic reviews of the E.U. Commission's adequacy finding, with a mechanism built into the Privacy Shield for transatlantic consultations. Id. at 21.

Schrems II

Schrems II was decided by the European Union Court of Justice on July 16, 2020. The key holdings in the CJEU Schrems II ruling 7-16-20 Case C-311/18 were the following:

1. The focus of the ruling was on the governmental privacy sphere and the adequacy determinations which have supremacy. The ruling ruling puts a spotlight on the compelling need for the United States to develop a national privacy law.
2. As the Advocate General stated in point 148 of his Opinion, the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.
3. If the recipient of personal data to a third country has notified the controller, pursuant to Clause 5(b) in the annex to the SCC Decision, that the legislation of the third country concerned does not allow him or her to comply with the standard data protection clauses in that annex, it follows from Clause 12 in that annex that data that has already been transferred to that third country and the copies thereof must be returned or destroyed in their entirety. In any event, under Clause 6 in that annex, breach of those standard clauses will result in a right for the person concerned to receive compensation for the damage suffered.

These are the highlights of the Press Release No. 91/20 issued by the Court of Justice of the European Union, Luxembourg, 16 July 2020, Judgment in Case C-311/18, in the matter of Data Protection Commissioner v Facebook Ireland and Maximillian Schrems:

First, the Court of Justice invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield However, it considered that Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries as valid.
Second, the General Data Protection Regulation1 ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection.
Third, according to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection.
Fourth, in the absence of an adequacy decision, such transfer may take place only if the personal data exporter established in the EU has provided appropriate

safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.
Fifth, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards.

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data is transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/5205 ('the Safe Harbour Decision'), the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court of Justice, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment').6 Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the EU to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1). 2 Article 45 of the GDPR. 3 Article 46(1) and (2)(c) of the GDPR. 4 Article 49 of the GDPR. 5 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 p.7).
6 Case:C-362/14 Schrems see also Press Release No. 117/15.
2010/87.7
Taking the view that the outcome of Mr Schrems's complaint depends, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court in order for it to refer questions to the Court of Justice for a preliminary ruling. After the initiation of those proceedings, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield8 ('the Privacy Shield Decision').

By its request for a preliminary ruling, the referring court asks the Court of Justice whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses in Decision 2010/87, what level of protection is required by the GDPR in connection with such a transfer, and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raises the question of the validity both of Decision 2010/87 and of Decision 2016/1250.
In today's judgment, the Court of Justice finds that examination of Decision 2010/87 in the light of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision. However, the Court declares Decision 2016/1250 invalid.
The Court considers, first of all, that EU law, and in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court adds that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR.
Regarding the level of protection required in respect of such a transfer, the Court holds that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter. In those circumstances, the Court specifies that the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.
Regarding the supervisory authorities' obligations in connection with such a transfer, the Court holds that, unless there is a valid Commission adequacy decision, those competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the EU has not itself suspended or put an end to such a transfer.
Next, the Court examines the validity of Decision 2010/87. The Court considers that the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court adds, depends on whether the decision includes effective mechanisms that make it possible, in practice, to

ensure compliance with the level of protection required by EU law and that transfers of Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100). 8 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016 L 207, p. 1). personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court finds that Decision 2010/87 establishes such mechanisms. In that regard, the Court points out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former.

Lastly, the Court examines the validity of Decision 2016/1250 in the light of the requirements arising from the GDPR, read in the light of the provisions of the Charter guaranteeing respect for private and family life, personal data protection and the right to effective judicial protection. In that regard, the Court notes that that decision enshrines the position, as did Decision 2000/520, that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court adds that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities.

As regards the requirement of judicial protection, the Court holds that, contrary to the view taken by the Commission in Decision 2016/1250, the Ombudsperson mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to

those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On all those grounds, the Court declares Decision 2016/1250 invalid.

Statement of U.S. Secretary of Commerce: Privacy Shield

The U.S. Secretary of Commerce Wilbur Ross submitted a "Statement on *Schrems* II Ruling and the Importance of EU-U.S. Data Flows" in a press release on July 16, 2020, addressing the July 16 ruling by the Court of Justice of the European Union in the *Schrems II* case. Specifically, he addressed the protections, if any, afforded by the E.U.-U.S. Privacy Shield.

"While the Department of Commerce is deeply disappointed that the court appears to have invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield, we are still studying the decision to fully understand its practical impacts," said Secretary Wilbur Ross. "We have been and will remain in close contact with the European Commission and European Data Protection Board on this matter and hope to be able to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments. Data flows are essential not just to tech companies—but to businesses of all sizes in every sector. As our economies continue their post-COVID-19 recovery, it is critical that companies—including the 5,300+ current Privacy Shield participants—be able to transfer data without interruption, consistent with the strong protections offered by Privacy Shield."

The United States participated actively in the case with the aim of providing the court with a full understanding of U.S. national security data access laws and practices and how such measures meet, and in most cases exceed, the rules governing such access in foreign jurisdictions, including in Europe.

The Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. Today's decision does not relieve participating organizations of their Privacy Shield obligations.

Data Privacy as a Generally Accepted Transnational Law Concept

There is a growing consensus among many nations that "data privacy" has become a generally accepted concept as developed and applied to the rapidly emerging body of transnational law. This is true whether one addresses "data protection" in the

context of the E.U.'s body of law concerning personal data collection, processing and transfer, or "information privacy" as that term is used in the United States. Id.

Regulating Content on the Internet

While more and more governments in Europe are seeking to regulate the most toxic, corrosive, inflammatory and harmful material on the internet by imposing either new laws or regulatory restrictions on online material, an increasing number of governments in other parts of the world are already moving ahead with stricter oversight of the internet through such actions as (1) shutting off access to social media sites in Sri Lanka after coordinated terrorist attacks left hundreds dead, (2) enacting restrictions on tech companies in New Zealand and Australia after the March 2019 massacre of 50 people at two mosques where the accused gunman used social media to amplify his message of hate, (3) exercising new powers to suppress digital content in India, and (4) enacting new laws to curtail false or misleading information in Singapore.

Network Enforcement Act: Growing Concerns Over Suppression of Free Speech

These and other efforts to restrict of suppress online material and content are rapidly giving rise to concerns over suppression of free speech and excessive restrictions on freedom of expression. For example, consider Germany's enactment of what is considered by many to be the world's strictest hate-speech law, the Network Enforcement Act (NetzDG).

The German Network Enforcement Act (NetzDG) was passed by the German Parliament in 2017 and implemented in early 2018, and since that time has faced much criticism from many quarters over potentially damaging and undermining the freedom of the press and freedom of expression. Shortly after the law went into effect in early 2018, Joerg Rupp, a political activist and social worker in the eastern German town of Malach, posted a tweet with altered lyrics to a German song, "The Anarchist Pig", to which he added derisive words about Chancellor Angela Merkel and asylum seekers. His twitter account was blocked and deactivated within hours for violating Twitter's terms of service by publishing offensive material. Rupp argued that his tweet was satire and that he was attempting to use the language of right-wing groups to show their cruelty.

Others including the research director of the Alexander Von Humboldt Institute for Internet and Society in Berlin dispute arguments that the Network Enforcement Act has triggered undue or widespread blocking of online content. They discount fears from some that internet providers are being required to moderate speech, a task more appropriately left to the courts or public institutions. Id.

Nonetheless, there are concerns over a growing risk that internet providers in the face of political pressure will take the path of least resistance and be forced to clean up their social media platforms by taking down content. Twitter for its part issued a statement that "freedom of expression is our fundamental guiding principle" and that there must be an appropriate balance struck between keeping people safe online and "preserving their inalienable human rights, and protecting the nature of a free, open internet." Id.

Potential Suppression of Free Speech

In a surprising example of potential suppression of free speech on the eve of elections for the European Parliament scheduled to take place from May 23 to 26, 2019, and based on its interpretation of the German Network Enforcement Act, Twitter temporarily blocked accounts of Germany's Jewish weekly newspaper Die Judische Allgemeine and Berlin SDP member Sven Kohlmeier after they had issued tweets containing criticism of the far-right populist Alternative for Germany (AfD) party. As its stated reason for shutting down the twitter accounts, the now global online social networking service said the tweets contained "misleading information on elections" and violated German laws aimed at combatting agitation and fake news in social networks.

The Judische Allgemeine tweet contained a link to an interview to the news agency DPA given by Israel's ambassador to Germany, Jeremy Issacharoff, in which he said he avoided all contact with the AfD because of that party's dubious stance on the Holocaust. In Sven Kohlmeier's tweet, he had commented on the decision by the AfD's Berlin branch to keep the politician Jessica Blessmann in the party, after Blessman had come under fire in 2018 for photos that emerged of her posing in front of wine bottles with a portrait of Adolf Hitler on the label. Such bottles are illegal in Germany.

In one of Mr. Kohlmeier's tweets that triggered a complaint, he asked "just how extreme-right do members have to be to be thrown out of the AfD?" He contested Twitter's temporary blocking action on the ground that his tweet did not break any of Twitter's rules. Both Kohlmeier's account and the account of Judische Allgemeine were restored on the afternoon of May 13, 2019.

According to Philipp Peyman Engel, the head of the online edition of the Judische Allgemeine, "the fact that Twitter tolerates anti-Semitic hate tweets but blocks messages from the only Jewish weekly newspaper in German is completely incomprehensible to U.S." Sven Kohlmeier stated in the multimedia online platform rbb24 that he saw the blocking of his Twitter account as a deliberate campaign to prevent freedom of speech. Kohlmeier said the rules were being abused by some users who reported accounts publishing opinions opposed to theirs and got them blocked. *Twitter Suspends Jewish Newspaper, SPD Politician for anti-AfD Tweets*,

DW Breaking World News, Deutsche Welle, May 13, 2019.

European Privacy Standard of 2014: Right to be Forgotten

The 2014 standard that gave rise to the Right to be Forgotten allows people to petition Google to remove search results about themselves, but it has sparked criticism for blocking legitimate material. In 2018, Google was ordered to stop listing search results about a Dutch doctor reportedly suspended for poor care of a patient according to The Guardian.

Such incidents, according to Wikipedia founder Jimmy Wales, represent a warning and that Europe's regulatory efforts may Balkanize the internet, with available online content changing based on a person's location.

Removal of "Harmful" Material from the Internet

The E.U. standards are having an impact beyond Europe. According to human rights groups, the public backlash against internet tech companies is at risk of being used as a pretext for censoring speech. Internet Without Borders, which tracks internet freedom globally, warns that the E.U.'s activities in this area normalize the removal of content. According to IWB's executive director, "freedom of expression relies solely on the possibility your content won't be suppressed arbitrarily."

In April 2019, the British Parliament proposed broad new laws to remove "harmful" content from the internet, including material supporting terrorism, inciting violence, encouraging suicide, disinformation, cyber bullying and inappropriate material accessible to minors. Over 17 nations have cited the spread of "fake news" when adopting or proposing new internet restrictions. According to Freedom House, a pro democracy group tracking government internet policies, these nations include Egypt, Kenya and Malaysia. *As Europe Polices Silicon Valley Titans*, supra. Moreover, 120 nations have now enacted data privacy laws styled and patterned after the European Standard, and GDPR-based principles of data portability and the "right to be forgotten", measures that are having a decided impact on laws outside Europe.

Extraterritorial Reach of the "Right to be Forgotten"

"The right to be forgotten" allows a person to ask that links to websites, news, and databases be taken down, or de-referenced, if the requestor considers the information "old, no longer relevant, or not in the public interest." The "right to be forgotten" purports to restrict people's ability to control what information is available about them on the internet. Some see it as mandating the deletion of truthful and accurate information, thereby limiting free expression. Others question whether the law can or should apply beyond the EU's 28 member states. The

extraterritorial reach of this law was recently litigated in the ECJ in a case brought by Google against the data protection watchdog for France, CNIL.

Google vs CNIL (C-507/17), Court of Justice of the European Union

Google in this case challenged a €100,000 fine from France's data protection regulator (CNIL), which had ordered Google to delist material across its global domains, based on the right to be forgotten principle. Google argued that global delisting impinged on free speech and would in effect be a way to enforce EU privacy standards in countries without similar laws. CNIL as the privacy watchdog for France imposed this fine on Google in 2016 for refusing to to delist sensitive information from internet search results globally upon request, based on the "right to be forgotten".

Google took its fight to the French Council of State which subsequently sought advice from the European Court of Justice. On September 24, 2019, the European Court of Justice handed down a landmark ruling in favor of Google that limited the reach of the online privacy law known as "right to be forgotten" and clarified the that law's geographical scope. Carl Schonander, Digital Policy Outlooks, Oct. 9, 2019, *European Court of Justice 'right to be forgotten' ruling likely to be relitigated - Love it or hate it, it's clear that whether the EU can apply the GDPR's "right to be forgotten" globally is in question*, accessible online at https://www.cio.com/article/3444605/european-court-of-justice-right-to-be-forgotten-ruling-likely-to-be-relitigated.html

Effectively this ECJ ruling means that Google's delisting of search results that concern EU citizens should apply only to the 28 member states of the EU, and that Google will not have to impose a global block on searches for information about EU citizens who invoke the "right to be forgotten".

The case is the first major ruling clarifying the geographical scope of the right to be forgotten principle, which since 2014 has allowed EU citizens to request delistings of information they deem to be inaccurate, inadequate, irrelevant, or excessive.

The ECJ acknowledged the relevance of non-EU law but suggested that the EU Parliament could impose global de-referencing. In ¶59 of its opinion, the ECJ noted that that "it should be emphasized that numerous third States do not recognize the right to de-referencing or have a different approach to that right." In ¶58, however, the ECJ said that the EU Parliament in fact has the "competence" (authority) to oblige search operators to "de-reference" right to be forgotten requests on all of its versions of its search engine. Id.

The ECJ did suggest, moreover, that if the GDPR had been written differently, the ECJ potentially could have found that the right to be forgotten applies to non-EU

domains. In its ruling, the ECJ did not limit the reach of the right to be forgotten on public policy grounds or international law grounds, but on the ground that the GDPR does not require global de-referencing. Its conclusion was thus appropriate since the GDPR does not provide for a balance between the right to privacy and the right to freedom of information of internet users outside the EU. Thus, while the ECJ did find that there is currently no obligation under EU law for global de-referencing, that might change if the EU law is amended. Id.

It appears that the ECJ has invited regulators to push the envelope to obtain global de-referencing. In its reaction to the ECJ ruling, the French data protection authority (CNIL) said that a "supervisory authority, and so the CNIL, has the authority to force a search engine operator to delist results on all the versions of its search engine if it is justified in some cases to guarantee the rights of the individual concerned." The stage appears to be set for this issue to be relitigated. Id.

Many see the September 24, 2019 ECJ ruling as a victory for Google and internet activists against a French effort to force the company and other search engines to take down links globally. See "*Right to Be Forgotten' Privacy Rule Is Limited by Europe's Top Court*, accessible at https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html.

The ECJ decision specifically noted that the "operator of a search engine is not required to carry out a de-referencing on all versions of its search engine" in order to comply with the GDPR's "right to be forgotten." As a practical matter, this may mean that when search engines like Google grant a de-reference request under the GDPR, they will not have to de-list search results that appear in non-EU domains. The search engines, however, are still required to discourage EU citizens from accessing those non-EU domains. Id.

This ruling limits the reach of the right to be forgotten to EU internet domains such as de. or fr., and in that sense it is a positive public policy development. It may also be considered positive from an international relations standpoint insofar as it prevents the EU's "right to be forgotten" from being applied extraterritorially, which would have strained the transatlantic relationship and the EU's relations with other countries as well.

In holding that Google does not have to apply the right to be forgotten globally, this ECJ decision will have broad implications for the regulation of the internet. In holding that the privacy rule cannot be applied outside the European Union, the ECJ effectively limited the geographical reach of the right to be forgotten.

US tech companies do not often win in the ECJ these days, and the right to be forgotten ruling was a win. It is nonetheless clear that whether the EU can apply

the right to be forgotten or right to erasure globally will be relitigated. It is safe to say that, at least for now, the ECJ ruling may influence courts around the world about the enforceability of GDPR.

Press release 112/19 regarding the ECJ ruling in *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)* appears at https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf

Eva Glawischnigh-Piesczek v Facebook Ireland Limited

In a new hit to high tech giants and free-speech advocates, the ECJ handed down a decision on October 3, 2019, in which it considered worldwide applicability of EU law as permissible. Former Green Party chairwoman Eva Glawischnig-Piesczek, an Austrian lawmaker, sued Facebook in Austria to remove what she considered a libelous news story that could be viewed by user worldwide. The Austrian court ruled in her favor, but requested the opinion of the European Court of Justice. Zachary Evans, *EU Court Rules Member States Can Force Facebook to Remove Content Worldwide,* National Review, Oct. 3, 2019, accessible online at https://www.nationalreview.com/news/eu-court-rules-member-states-can-force-facebook-to-remove-content-worldwide/

The ECJ's judgment in Case C-18/18 *Eva Glawischnigh-Piesczek v Facebook Ireland Limited*, is different from the right to be forgotten ruling of September 24, 2019, because it involves content that has been found by a national court to be illegal. The ECJ ruled that individual member states can force Facebook to remove content worldwide if it contravenes their laws. Its ruling in essence allows one country or region to decide what Internet users around the world can say and what information they can access. Facebook argued that the ECJ ruling undermined the longstanding principle that one country does not have the right to impose its laws on speech on another country. The ruling does say, however, that national courts can issue injunctions with "worldwide effects," i.e., beyond the EU. This has led some to conclude that even though the September 24, 2019 ECJ ruling on the right to be forgotten did not result in that case in the extraterritorial application of EU law, the ECJ is open to such extraterritoriality in the future. Id.

The ECJ ruling enables one EU member state to issue an order that could be used to remove social media posts by users around the world, even though what is considered unlawful in one country might not be considered unlawful in a different jurisdiction. *Facebook to be subject to tougher controls after EU court ruling,* The Guardian, Oct. 3, 2019, accessible online at https://www.theguardian.com/technology/2019/oct/03/facebook-faces-tougher-controls-after-eu-ruling.

The decision also raises questions about how material found to be unlawful in one country will be identified by Facebook or other social media sites without searching through the posts of all its users. It also makes it clear that Facebook will be subject to tougher controls over online content now that the social media giant can be ordered by member states in the EU to remove defamatory material worldwide. Predictably, the ruling was condemned by free speech organizations for imposing restrictions on online comments. Id.

Press Release 128/19 regarding the ECJ ruling of Oct. 3, 2019 in Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, appears at https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190128en.pdf.

Privacy as a Fundamental Right

Google has an unfortunate history of intensive online data collection arising from what some have characterized as an aggressive collection of user data, similar in some respects to the embarrassing scandals that rocked the Facebook world in recent years, leading to Facebook CEO Mark Zuckerburg's declaration in a recent company conference that "the future is private" and Facebook is "shifting its products to more intimate communications." *Google Says it has found Religion on Privacy*, supra.

Ours is a world increasingly defined by digital technology, and privacy is "not merely a luxury; it is a fundamental right," as recently noted by Google's Chief Executive, Sundar Pichai. *Privacy Should Not Be a Luxury Good*, NYT Op-Ed May 8, 2019 at A25. Pichai emphasized Google's core philosophy to make privacy a reality for everyone: "Privacy must be equally available to everyone in the world."

Addressing growing concerns over how people's personal information is used and shared, Pichai touched on the personal nature of privacy and how people define privacy in their own way:

"To the families using the internet through shared devices, privacy might mean privacy from one another."
"To the small business owner who wants to start accepting credit card payments, privacy means keeping customer data secure."
"It the teenager sharing selfies, privacy could mean the ability to delete that data in the future."

There is a paramount need for people to be given "clear, individual choices around how their data is used," as Pichai noted in his May 7, 2019 conference remarks that echoed similar views expressed at the time the GDPR went into effect. Id. at A25.

For example, while a paid product like YouTube Premium includes an ads-free experience, the regular version of YouTube can be viewed in Incognito mode, allowing the user to browse the web without linking any activity to the user. Google CE Pichai put it in perspective: "To make privacy real, we give you clear, meaningful choices around your data ... while staying true to two unequivocal policies: that Google will never sell any personal information to third parties; and that you get to decide how your information is used." Id.

Among the new privacy features Google recently unveiled are the following:
One-click access to privacy settings from all of Google's major products;
Auto-delete controls that allow the user to choose how long data will be saved;
A Two-factor authentication built into Android phones as a security key;
"Federated Learning" developed by Google's A.I. Researchers that allow its products to "work better for everyone without collecting raw data from your device" through which a Google keyboard can recognize and suggest new words after people begin typing them, without Google ever seeing anything you type.

Google is thus providing its users with more control over their data and making it more difficult to track their online activities. Users will be permitted to navigate Google's maps and search for information in Incognito mode and will be allowed to delete web and app activity history automatically after 3 months and 18 months, respectively.

Turning now to data privacy under German law, let us take a close look at the Bundesdatenschutzgesetz (BDSG), the German Federal Data Protection Act. This has now been translated by the German Ministry of the Interior into English and is accessible online at https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf

German Federal Data Protection Act

The German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (English), referred to as The German Federal Data Protection Act, has separate provisions for data processing in the public and private sectors. On 27 April 2017, the German Parliament passed the BDSG in order to make use of the opening clause provided for in the EU General Data Protection Regulation (GDPR).The GDPR marks the first step toward adapting German law into the provisions of the EU General Data Protection Regulation.

In addition, Germany has special privacy provisions for electronic information and communication services (telemedia) and yet another set of privacy rules for the providers of services that transmit electronic signals. All these laws apply to some

extent to the providers of online services. Through these laws Germany transposed European Union (E.U.) Directives 95/46 and 2002/58, albeit in a very complex and differentiated manner. Some German experts find that this complexity interferes with the requirement of transparency in that it keeps consumers from being aware of their rights and from exercising them.

In keeping with the Directives, Germany generally prohibits the collection and use of personal data unless the law specifically permits this or the data subject has given his or her informed consent. German law also follows the Directives on issues relating to rights and remedies of data subjects, security requirements, restrictions on location data, minimization of data, and safeguards against transmitting personal data to third countries with lesser standards of protection. The German provisions, however, often call for the balancing of competing interests and the application of the principle of proportionality. These provisions have resulted in an extensive and varied case law.

In Germany, data protection has constitutional dimensions that flow from the guarantees of human dignity and personhood. From these, the Federal Constitutional Court (FCC) crafted the right of informational self-determination that permits the processing of personal data only if authorized by statue or by consent of the data subject. In 2008, the FCC expanded these principles by articulating a constitutional guarantee of the confidentiality and integrity of IT systems. In 2010, the FCC struck down a German law transposition of the E.U. Data Retention Directive, for violating the principle of proportionality and the individual's rights of personhood.

Germany has a Federal Data Protection Agency and sixteen state data protection agencies. These often act in concert when making recommendations on how the consumer may navigate safely through the Internet. In addition, German experts often discuss the data protection problems that arise from the widespread collection of data by search engines and social media, and the use of these data to profile the data subject for commercial purposes. Although German law prohibits these practices unless informed consent has been given and although German law applies to any collection of data on German soil, Germany cannot enforce these laws against global players.

I. Legal Framework

Privacy in online services is in part governed by the data protection provisions of the German Telemedia Act (TMA) (§§ 11–16). This Act regulates electronic information and communication services (hereafter telemedia service providers) irrespective of whether their services are gratuitous or fee-based, thus applying to search engines, news groups, chat rooms, and social media. The Federal Data Protection Act (FDPA) also applies to these online services, except where the TMA more specific provisions. In addition, the privacy provisions of the

Telecommunications Act (TCA) (§§ 87–116) apply to various technical aspects of telemedia activities.

Germany transposed the European Union (E.U.) Data Privacy Directive (Directive 95/46) through the TMA as well as the FDPA, making use of the Directive's permission to enact sector- specific legislation. German also made use of the Directive's permissible "margin for maneuvering" by crafting some detailed legal concepts that are not contained in the Directive but adhere to its spirit.

The German legislation also deviates from the wording of the Directive but not its meaning by adhering to pre-existing German terminology and concepts. In particular, the
German legislation distinguishes between data collection, processing and use i nstead of employing the term "data processing" for all these activities, as is done in the Directive. In addition, the German FDPA retained its pre-Directive structure of having separate rules for the public and private sectors, as well as general provisions that apply to both sectors. Of these, only the private sector rules (FDAP §§ 27–38a) and the general provisions (§§ 1–11) apply to telemedia service providers.

Germany transposed the e-privacy Directive (Directive 2002/58) primarily through the Telecommunications Act. Germany had transposed the E.U. Data Retention Directive in sections 113a and 113b of the Telecommunications Act, but the Federal Constitutional Court voided these provisions as unconstitutional, and German politicians have since then been unable to agree on how to reword these provisions, while the E.U. Commission initiated proceedings against Germany's tardiness. Germany transposed Directive 2009/136 only in part through amendments to the Telecommunications Act. In particular, Parliament could not reach an agreement on the transposition of the all-important "cookie provision".

Germany has a long history of data protection. Like the United States, Germany became aware in the late 1960's of the need to protect the privacy of individuals against the data collection capabilities of electronic data processing. In 1970, the German State of Hesse enacted
the first Data Protection Act and several German states shortly followed this example. In 1977, Germany enacted the first Data Protection Act at the federal level.

German data protection developed a new dimension in 1983, with the *Census Decision* of the German Federal Constitutional Court (FCC). In this decision, the Court held that the individual has a constitutional right to "informational self-determination." The decision prohibits the handling of personal data unless specific statutory authorization is given or the data subject consents (see below, section IV).

In 1990, a new Federal Data Protection Act incorporated these constitutional requirements.

The Act of 1990 is still in effect today, albeit after numerous amendments. Now, as at the time of enactment, the FDPA has aimed at protecting against the abuse of data processing by requiring that governmental data processing be based on specific statutory enabling legislation, while the consent of an individual is generally necessary to permit data processing in the private sector. There is, however, a strong feeling that the complexity of the German legislation is detrimental to its effectiveness.

In addition to the Federal Data Protection Act, the German states (Länder) have data protection acts. These, however, are not very relevant to online privacy, because they regulate the public sector of the states, whereas the regulation of private sector activity is governed primarily by federal law. Some of the states have explicit data protection guarantees in their constitutions, yet these also are of little consequence for online data protection.

II. Current Law: Federal Data Protection Act

A. General Principles

The privacy provisions of the FDPA address data controllers, that is entities that process (in German parlance, collect, process, and use) personal data. The controllers are required to register with the pertinent state authority, and this also applies to telemedia service providers. Registration is required in particular for controllers who transfer data to others or conduct market research. They must always register even though other controllers can avoid registration if they appoint an internal data protection official.

Telemedia service providers may collect and use personal data only to the extent that the law specifically permits or the data subject has given his consent. Moreover, to the extent that the law permits the collection of data for specified purposes, these data may not be used for other purposes, unless the data subject has consented to other uses. The law recognizes two types of special purpose data: contract data (*Bestandsdaten*) and utilization data (*Nutzungsdaten*) (see below, Personal Data). For all other types of personal data, particularly content data, consent is required in accordance with sections 28 through 30 of the FDPA, a set of stringent provision, particularly with respect to advertisements.

B. Consent

According to section 13 of the TMA, the controller must inform the user of the extent and purpose of the processing of personal data, for any consent to be valid. Consent may be given electronically, provided the data controller ensures that the user of the service declares his consent knowingly and unambiguously, the consent

is being recorded, the user may view his consent declaration at any time, and the user may revoke consent at any time with effect for the future. These principles live up to section 4a of the FDPA, which requires consent to be based on the voluntary decision of the data subject. Consent, however, is not always required. Many statutory exceptions allow for the use of data without consent, for various business-related purposes.

C. Transparency

According to TMA section 13(1), the telemedia service provider must inform the user at the beginning of the contractual relationship of the extent and purpose of data collection and use, also on whether the data will be processed outside of the European Union. If the provider intends to use an automated process that will allow the identification of the user, then this information has to be provided when data collection commences, and the user must at any time have access to this instruction.

This provision of the TMA has been interpreted as applying only to contract and utilization data, thus leaving content data under the governance of Section 4(3) of the FDPA. The latter provides that the controller must inform the data subject of the identity of the data controller, the purpose of the collection, processing, and use of the data, and the categories of intended recipients if this is not foreseeable for the data subject. This information must be provided when the data are first collected.

D. Personal Data

The FDAP defines personal data as "individual pieces of information about personal or factual circumstances about an identified or identifiable human being." This definition applies to all the data handled by telemedia service providers irrespective of whether the data are governed by the FDPA or the TMA. Different rules on consent requirements, however, apply to different categories of data.

Contract data (Bestandsdaten), as defined in the TMA, are the data that are required to establish, develop, or change a contractual relationship with a telemedia service provider. Contract data are to be collected sparingly, in order to live up to the principle of data minimization. They may be used only for the intended contractual purpose and must be deleted once they are no longer needed. This use is statutorily permitted. The user's consent, however, is required if the service provider wants to use these for other purposes, such as advertising or market research; a specific agreement from the data subject is required for these uses. The provisions on contract data apply whenever a relationship is established by an online registration. They apply therefore, to Facebook and other social media.

Utilization data are the personal data that a telemedia service provider may collect and use to facilitate use of the service and for accounting purposes. The service provider may use these data to create user profiles for market research and

advertising, unless the user objects after having been duly informed. The thus-created profiles must be identified by a pseudonym, and the identity of the user may not be revealed.

Other data, particularly content data, fall under the consent requirements of sections 28 through 30 of the FDPA, if they are collected by online service providers. In their current form, these provisions were introduced through the 2009 reform of the FDPA, and their complexity is legendary. Generally, they allow certain commercial uses of data, including "list-making" and "scoring," albeit under numerous safeguards. Section 29 deals with data collection and storage for a controller's own business purpose and for the purpose of disclosure of the data to third parties, including for the purpose of direct marketing. Such activities are permitted to some extent without the data subject's consent, yet the competing interests must be balanced, and the data subject must be notified of the purpose of the processing.

It has been stated that section 29 of the FDPA is not well-suited to online activities as facilitated by current internet technology that allows the collection of information from websites and the downloading of large quantities of data. Section 29 requires a scrutiny of the permissibility of data processing in each individual case to ascertain circumstances, such as a protection-worthy interest in preventing the data processing, and the public availability of the data. In addition, the law requires random checks of the continued suitability of ongoing operations.

There has been much discussion of whether IP addresses are personal data, and the majority opinion considers them to be always personal data when they are fixed IP addresses that identify a specific computer. If they are movable IP addresses that are assigned by the access provider every time the user logs in, then they are personal data only if the service provider has enough information to actually identify the user, which will usually be the case.

E. Sensitive Data

The FDPA defines sensitive data according to Directive 95/46 as those relating to race, ethnicity, political opinions, religious or philosophical beliefs, or health or sex life. Consent must be expressed specifically in order to permit the collection and use of such data. Moreover, controllers of such data must undergo an examination of their operations as required by Directive 95/46.

F. Profiling

Germany has been averse to the profiling of personally identifiable data subjects since the *Micro Census Decision* of the Federal Constitutional Court in 1969, and the data protection laws guard against profiling in various ways, among them the insistence that data only be used for the purpose for which they have been collected. The TMA, however, allows the creation of profiles with data that have

been rendered anonymous (see below, Anonymity). The FDPA also allows the use of some data for market-related purposes. To the extent that they involve profiling, various safeguards, including the informed consent of the data subject, would be necessary. Profiling without the consent of the data subject is at the heart of the German dislike for the "Like" button of Facebook (see below, Data Protection Authorities).

The specter of large-scale profiling through web-crawling and the use of Facebook was raised in June 2012, when it became known that Schufa, a German credit rating agency, was exploring the possibility of enhancing its profiles on the creditworthiness of individuals with these means. German official reaction was largely negative, finding the project offensive if not illegal; even the German IT industry association, Bitkom, suggested that not everything that was doable should be done and worried about consumer confidence in the Internet.

G. Smartphones and Geo Data

Germany transposed article 6 of Directive 2002/58 concerning traffic data in section 96 of the TCA and the Directive's article 9 on other location data in article 98 of the TCA. Both types of data are highly sensitive, and unless there is consent for further processing, these data may be collected and used only to the extent that they are required. They must be deleted or made anonymous. as soon as they are no longer needed. If they are to be used for marketing purposes or for connection to smartphone applications, special forms of consent and notifications are required.

German scholars are of the opinion that programs such as "Facebook Places" violate German law if the mobile phone user logs in. In that case, the location of the user is to be construed as personal data that may be collected and used only if there is consent. There also is established case law that the creation of movement profiles of a person is illegal. Scholars also are of the opinion that the use of radio-frequency identification technology is of questionable legality in view of the potential to create moving profiles and that the current statutory provisions may not provide enough privacy protection.

Google Street View has come under considerable attack in Germany, resulting in the intervention of the data protection agencies and in much litigation. The outcome of this struggle is that Google may take pictures of the street view of houses, but it must blot out identifiable house numbers upon request. In Berlin, the Consumer Protection Ministry decreed that Google could start its picture taking only after the residents had an opportunity to voice their objections. The dwellings and gardens of these citizens had to be rendered totally unrecognizable by Google.

In August 2010, the Federal Council (the Chamber representing the states in the bi-cameral federal legislature) proposed legislation that would have further restricted the collection of data through photographs by introducing a legally binding right of

objection. In December 2010, the Federal Minister for the Interior, together with Bitkom the German industry association for information technology, responded with a counterproposal that recommended self- regulation, as long as certain well-established principles were not violated.

H. Protection of Minors: Klicksafe

Germany has no age-specific privacy provisions. Many of the states, however, provide educational programs to make young people aware of the online attacks on privacy. In Hamburg, for instance, the Data Protection Commissioner published a brochure entitled "You Won't Get My Data," that has suggestions on how to include online privacy education in the school curricula. German organizations also participate in the E.U.-wide initiative "klicksafe." The media authorities of the states also provide and coordinate programs to protect young people from the dangers of the Internet, particularly illegal content.

I. Technical Security

Section 9 of the FDPA requires extensive technical organizational measures to ensure the overall integrity of IT systems that are being used for the processing of personal data, and these requirements live up to article 17 of Directive 95/46. The German provisions, as well as the Directive, call for a proportional interpretation of security requirements, by tailoring the need for security to the risk inherent in specific operations. Additional provisions on technical security are contained in sections 107 and 109 of the Telecommunications Act.
Section 13 of the Telemedia Act requires controllers to install the necessary technical and organizational measures to ensure that:

- the user may terminate the relationship at any time;
- data will be automatically erased or blocked if required by law;
- the use of the service will not become known to third parties;
- data on the use of several telemedia by one user can be accessed separately, except that they can be combined for accounting purposes; and
- data collected under a pseudonym cannot be combined with data personally identifying the user.

In August 2009, Germany introduced a security breach notification requirement that obliges controllers to notify the data subject if data were unlawfully transmitted or otherwise became known to third parties. This requirement was modeled after U.S. law and is intended to increase consumer confidence in automated systems.

According to the German provisions, notification is required only if the security breach threatens to cause serious impairment of the rights or the protection-worthy interests of the data subject. In November 2009, the E.U. promulgated Directive 2009/136, which requires notification of any type of security breach that led to the

destruction, loss, or alteration of data, irrespective of the impairment caused thereby. Germany has not as yet transposed this provision.

J. Anonymity

Rendering data anonymous is a general principle of German data protection law, to be employed whenever feasible so as to minimize the proliferation of data. Data may also be placed under a pseudonym so as to preserve anonymity. These devices allow the data subject to retain control over his data while giving the controller greater possibilities for use and transmittal of the data. When data have become anonymous, they are no longer personal data and can therefore be freely used for market research. They become personal data again if the controller has the possibility of identifying the data subject. It appears that services are available in Germany that facilitate anonymity by allowing the user to communicate over an IP address that differs from his or her own.

Telemedia service providers are required to use pseudonyms for the collection of certain data. For utilization data, the controller must use "pseudonymization" in order to be allowed to create profiles for market research (see above, Personal Data). With regard to contract data, the telemedia service provider must make it possible for the data subject to use the service and pay for it under a pseudonym, and he must also inform the data subject of this option. The law provides, however, that the provider must make "pseudonymization" possible only to the extent that it is technically feasible and can be reasonably expected. This is one of the many "balancing and weighing" clauses that exist in German data protection law.

K. Rights and Remedies of Data Subjects

The privacy rights and remedies of telemedia users are governed to a large extent by the FDPA. The Act imposes duties of notification on the data controller (§§ 4(3) and 33). He must notify the data subject on the types of data that are being collected, the source of the data, the purposes for which data are collected, and to whom they are disclosed.

For the data subject, the Act grants rights of access (§ 34) and rights to effect correction, erasure, and blockage (§ 35). The right to demand erasure often becomes an issue when a user leaves a social medium. Users often waive the right of erasure in standardized terms of contract. It appears that this is currently permissible according to German law. Even if erasure were to be carried out, data are being transmitted to third parties in many different ways in social media, so that erasure often does not fulfill its purpose.
Data subjects may enforce their rights through the judicial remedies provided in civil and commercial law. Injunctive relief as well as damages can be claimed. It appears, however, that damages for pain and suffering are not available for data protection violations in the private sector.

In Germany, the data protection authorities are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers must first be lodged with the company's in-house data protection official. Germans believe in self- regulation of the private data processing sector, yet it has been suggested that this German solution is not compatible with E.U. requirements.

L. Sanctions

Contraventions of the various duties of the TMA are administrative offenses that are punishable with a fine of up to €50,000. This applies to transgressions such as the failure to erase data or to keep them anonymous. Most violations of the FDPA are also administrative offenses. Some are punishable with a fine of up to €50,000, whereas the more serious ones, such as the processing of data without having obtained consent, are punishable with a fine of up to €300,000. Criminal sanctions are available for conduct involving intent to harm others or to make a profit.

M. Cross-Border Application

In keeping with article 4 of Directive 95/46, the law of the seat of the controller applies to data processing occurring in Germany if the controller resides in another Member State of the European Union. German law applies, however, if such an E.U.-resident controller carries out data processing in Germany through a German subsidiary or establishment. German law also applies for any data processing occurring in Germany that is carried out by a controller who resides outside the European Union.

According to these principles, German law applies to an online search engine or social medium if it places a cookie on a German personal computer. Enforcement of German law, however, can rarely be achieved against foreign controllers.

On the transmittal of data to other countries, Germany also differentiates between recipient countries that are E.U. or EEA members and third countries. Transfers to the latter generally require assurances that the third country has an E.U.-compatible standard of data privacy. Transfers to E.U./EEA countries are often, but not always, governed by the same provisions of German law that apply domestically.

The issue of applying German law to the collection of German data by controllers in third (non-E.U.) countries is addressed in the ongoing controversy over whether Facebook qualifies as a E.U.-domiciled controller because of its corporate address in Ireland. Many German experts are of the opinion that Facebook use in Germany, in particular the use of the "Like" button, is subject to German law and therefore

prohibited on the grounds that the data are ultimately transmitted to the United States, which does not have an E.U.-compatible data protection standard.

N. Data Retention

As mentioned above, Germany has not as yet transposed E.U. Directive 2006/24, on data retention. If Germany eventually were to comply with this mandate, the German practices and rules on rendering data anonymous might have to be changed (see above, section II(J).

III. Role of Data Protection Agencies

Germany has a Federal Data Protection Commissioner and sixteen state data protection authorities, one for each German state. The Federal Commissioner's primary function is the supervision of data processing by the federal government, whereas the state authorities are in charge of overseeing data protection in the public sector of their state on the basis of state law, and data protection in the private sector of their state on the basis of federal law. In a decision of 2010, the European Court of Justice held that the date protection agencies of some of the German states agencies are not independent enough from the state governments; this judgment will lead to institutional reforms in some of the German states.

The state authorities oversee the activities of private data controllers and require them to register with the authority or to appoint an internal data protection official in accordance with federal law. The state authorities also offer assistance to the public, yet complaints against controllers who reside in Germany should at first be brought to the in-house data protection officials (see above, Rights and Remedies). The sate authorities publish biannual reports on their activities. In addition, the state authorities cooperate in the Düsseldorfer Kreis, a periodic conference that publishes resolutions on important data protection issues for the private sector.

In 2009, the Düsseldorfer Kreis recommended standards for the tracking of internet users by search engines, such as through Google Analytics. As a result of these efforts, Google changed its program code through "IP masking," thus collecting the data in an anonymous manner. Nevertheless, Google is still viewed as being in violation of German law for its tracking practices.

In 2011, the Düsseldorfer Kreis published a resolution on data protection in social media. It admonished social media, stating that German law applies to their activities even if they have a subsidiary in another E.U. member state, and it emphasized that transparency and informed consent are required to make the use of social plug-ins on German personal computers permissible. The resolution, however, adopted a somewhat conciliatory tone by approving of self-regulatory efforts by social media companies.

On the same issue, however, the data protection agency of Schleswig Holstein has taken a more pronounced view, particularly on the "Like" button of Facebook. The agency advised public and private providers of websites that the "Like Buttons" and other social plug-ins violated German law and that German private and public entities should not have a presence on Facebook. In addition, the agency has taken three German enterprises to court for their presence on Facebook. The cases are still pending.

IV. Court Decisions

The Federal Constitutional Court [FCC] shaped German data processing law by subjecting it to the constitutional guarantees of human dignity and free development of one's personality. In 1969, the Court held in the *Micro Census Decision* that it is contrary to human dignity to catalog and register an individual and that there has to be a sphere into which no one can intrude and where the individual can enjoy solitude.

In 1983, the FCC issued its famous *Census Decision* [*Volkszählungsurteil*]. According to the Court, the right of informational self-determination derives from the guarantees of personhood and human dignity of the Constitution, and it generally grants the individual the power to decide about the disclosure of his personal data and their use. The Court allows exceptions from this principle only if there is an overriding public interest and if this is explicitly stated in specific statutory provisions. In addition, the constitutional protection requires that data processing activities live up to the principle of proportionality and give the individual procedural remedies and protections. Moreover, data may not be stored indefinitely for undefined future purposes.
In 2008, the FCC issued a decision on online searches by public authorities. The Court created a new constitutional right that guarantees the integrity and confidentiality of IT systems. Consequently, the Court held that online searches by the public authorities require a search warrant. Although the decision addresses the public sector, it may also create duties for the private sector, because the German Constitution is interpreted to the effect that fundamental rights must be observed by the private sector.

In 2010, the FCC referred to the data retention prohibition of the *Census Decision* when it issued a decision on data retention which struck down the German transposition of Directive 2006/24. In addition, the decision of 2010 found that the statutory provisions had violated the secrecy of telecommunications.

The courts of ordinary jurisdiction also have contributed much to the interpretation of data protection law. They are called upon on a daily basis to apply the principle of proportionality and to balance competing interests, such as privacy versus technical feasibility or freedom of expression. There is a flood of cases that limit the right to informational self- determination.

A decision of the Federal Court of Justice (Bundesgerichtshof) of 2009 explains that informational self-determination has to be balanced with other rights, in that case with freedom of speech. A teacher had requested an injunction against an Internet portal that published student evaluations of her performance. The portal had a registration requirement that included naming the school, along with a user name and password. The Court held that providing information on the teacher was permissible, because it was provided to a circle of persons with an interest in the information. The Court also mentioned that individuals have fewer privacy protections in their professional sphere.

In May 2012, the Federal Court of Justice balanced the right to be forgotten with the public's right to know, by rejecting a request from two murderers to enjoin an Austrian Internet
portal from retaining an article on them in its online archive. The plaintiffs had been convicted of murder in 1990. The Court first obtained an advisory opinion from the European Court of Justice that confirmed German jurisdiction over the case due to the plaintiff's close connection to Germany. On the merits, the German Court held that under the circumstances of the case, the public's right to know outweighed the interests of the complainants to be shielded from publicity.

V. Public and Scholarly Opinion

Germans are avid users of the Internet and of social networks. Some 75% of the German population uses the Internet; close to one half of them use it on mobile telephones or tablet computers. The use of search engines has become indispensable to many Germans, and Google has an 85% market share in Germany. Some 55% of Germans are active users of social media, with Facebook usership reaching 28% of the population.

Opinions on the need for online privacy protection range from asserting that privacy has become an out-of-date concept to viewing the assault on privacy in online services as a serious problem. Many scholars are of the opinion that developments in technology and user patterns have created a new reality that is not adequately addressed by German law. This is perceived as being particularly true for the numerous applications that are used on smartphones and through which enormous amount of data are processed, often for the purpose of profiling. A recurring theme in this discussion is the compensatory nature of search engine and social media use, the fact that these services are not "free," that there is a consideration to be paid in the form of released information of monetary value.

The German discussion of online privacy is multifaceted; it addresses the constitutional tension between privacy and freedom of information, makes practical suggestions for users and for future technological development, emphasizes education, and recommends law reform. Most writers take a balanced view by recognizing that online services, be they search engines or

social media, contribute to the proliferation of knowledge and empower people to express themselves. Moreover, some writers advise against overly strict German regulation of its domestic providers on the grounds that enforcing high standards in Germany will hurt German firms when they are competing with providers in other countries.

On technical developments, Dirk Heckmann, the author and editor of a renowned commentary on Internet law, favors the development of privacy settings by default that would minimize the disclosure of personal data while also offering transparency and assistance. On user behavior, Frank Koch, a practicing attorney, makes several recommendations, including the frequent deletion of cookies while surfing, the frequent change of pseudonyms when using social media, the de-activation of the geo-localization function of smartphones when not needed, frequent reputation management, using of information posted by German data protection authorities on how to better protect privacy, and the use of search engines such as Ixquick that do not collect user data. He believes that these measures would not only protect the user, but also would favor the growth of innovative, small service providers who would be given a better chance if the data collections of the large, oligopolistic providers were less complete.
Phillip Gröschel, a youth protection official for a for social media service provider, emphasizes the need for education, to empower the individual to discern the complexities of the issue. Indra Spieker, a law professor, shares his view that users are not aware of the threats to their privacy; she would favor clearer statutory rules instead of the current practice of balancing and weighing of competing interests. Ultimately, she recognizes the inevitable tension between the right to information and the right to privacy. Legally speaking, she decries the imbalance in power between the network and the user.

A somewhat unconventional idea for law reform comes from Jochem Schneider, an attorney, who would not require informed consent for the processing of all data. He would limit stringent privacy protections to data relating to the home and the intimate sphere of life. He argues that the categorical insistence on a consent requirement for all personal data is responsible for the complexity of German data protection law, which has to create many statutory exceptions. Moreover, he finds that German data protection law, as written, violates the constitutional guarantee of freedom of expression, which therefore has to be inserted into the statutory law through judicial interpretations.

VI. Pending Reform

In June 2011, the German states had introduced draft legislation to transpose the cookie provision of Directive 2009/136, restating article 5(1) of that Directive almost verbatim. However, this draft did not become law, because the federal government is of the opinion that a transposition of the Directive that follows its wording would not be technically feasible without subjecting the user to constant pop-ups. The

federal government intends to await a European solution and also favors self-regulation by the telemedia service providers.
Many German experts view the proposed E.U. Data Protection Regulation148 favorably. Among them is the German Federal Data Protection Commissioner, who finds that the reform proposal has a chance of improving the current legal situation, in particular vis-à-vis service providers from non-E.U. member countries. He also hopes that industry interests will not succeed in watering down the proposed standards.

Thilo Weichert, the Data Protection Commissioner of Schleswig-Holstein formulated these expectations as to what the proposed E.U. Regulation may accomplish as follows:

Perhaps data transmission to the United States is no longer possible; traffic data can be analyzed only to a limited extent. The user must be better informed, particularly as to his options on the release of data. The collection of data of third persons, as for instance, through address books, must be restricted, if not completely prohibited. Proper consent procedures must be provided for facial recognition. On the granting of information on existing data and their erasure, clear European guidelines exist that Facebook has not observed as yet. Overall, Facebook must considerably improve their standardized terms of contract and consumer protection. You see: there is a multiplicity of demands – technical, organizational, and legal. Facebook must make major efforts.

Some Germans, however, oppose the proposed E.U. Regulation for violating the E.U. subsidiarity principle and for potentially lowering German data protection standards, as well as for giving up constitutional sovereignty over the issue.

VII. Concluding Remarks

Germany has invented the right of informational self-determination, and German law appears to be effective in restricting the processing of personal data by the private sector, at least by domestic providers. Germany, however, shows some understanding of commercial interests. This is demonstrated by the allowance of the use of personal data in some situations, for instance when it is possible to render that data anonymous for market research purposes, instead of requiring their deletion. German law also takes a pragmatic approach to imposing data protection requirements by balancing protective requirements with their feasibility. Balancing is also required to reconcile competing fundamental rights, such as freedom of expression, with privacy interests. The courts are frequently called upon to weight these competing interests, and they do not always decide in favor of privacy.

German law, however, suffers from its complexity and from many broad concepts that stand in the way of certainty and predictability. There is also much concern

that the existing laws are not adequate to deal with the technical and societal changes that have been brought through globalization, the increased use of search engines, smartphone applications, and social media and the resulting proliferation of personal data that are disclosed by the data subjects themselves.

For these reasons, like their American counterparts who are interested in comprehensive legislation on data protection, many German lawyers welcome the development of a European Regulation on data protection.

The Future of Cybersecurity?

We conclude this presentation on a cautiously optimistic note. The American Bar Association House of Delegates has now formally adopted and will submit to the U.S. Congress and state and local governments a narrowly tailored set of recommendations that address Disinformation and its negative impact on the electoral process. This addresses foreign interference in federal and U.S. elections and calls for specific legislative measures to prohibit false, deceptive or misleading statements, information or practices by a foreign principal or its agent, regarding the time, place or manner of voting or interfering with electoral process.

The ABA 2020 Disinformation Resolution and accompanying Report

The ABA Cybersecurity Legal Task Force, with substantial input and collaboration from many ABA Sections, Divisions and Standing Committees, submitted a Resolution on Disinformation to the ABA House of Delegates for adoption at its August 3, 2020 meeting. Also submitted as a companion was a Civic Education Resolution that urges federal and state governments and private sector entities to promote digital literacy, civic education, and public awareness to build societal resilience to domestic and foreign malign disinformation operations. The following discussion focuses on the Disinformation Resolution.

Foreign Interference in federal and U.S. elections: This resolution addresses foreign interference in federal elections. It calls for the U.S. Congress to "preserve and protect each American citizen's right to vote in federal elections by enacting legislation that prohibits the use of false, deceptive, or misleading statements, information, acts, or practices by a foreign principal or its agent (as defined in 22 U.S.C. 5 §611(a)-(c)), regarding the time, place, or manner of voting, to interfere with voting, registering to vote, vote tabulation, or vote reporting (hereinafter "electoral processes"). In addition to federal elections, this resolution urges state, local, territorial, and tribal legislatures to "preserve and protect the right to vote in U.S. elections by enacting legislation that prohibits the use of false, deceptive, or misleading statements, information, acts, or practices by a foreign principal or its agent, regarding the time, place, or manner of voting, to interfere with electoral processes.

Transparency in campaign advertising: This resolution further urges the U.S. Congress to "enact legislation regarding paid political campaign advertising that requires meaningful transparency concerning the entity that paid for a communication and requires consistent disclaimer and attribution requirements for all media, including television, radio, print, and Internet-based/digital media.

Disinformation affecting electoral processes: This resolution also urges social media companies to "take immediate steps to address the spread of disinformation affecting electoral processes in U.S. elections by: 1) Identifying and either labeling or removing, as appropriate, accounts that: a) Are used by a foreign principal or its agent engaged in communications or actions to interfere with electoral processes, including efforts to suppress voter turnout or attempts to deceive viewers into thinking the account belongs to a U.S. entity or national; b) Disseminate false, deceptive, or misleading content to interfere with electoral processes; or c) Are used by bots or other technology to post automated false, deceptive, or misleading content to interfere with electoral processes; 2) Making their terms of service or rules consistent with the foregoing recommendations; 3) Reporting to the public periodically about the results of the efforts to identify, label, or remove certain accounts; and 4) Educating users to beware of disinformation campaigns and deceptive practices that could interfere with electoral processes.

Funding to address emerging technological threats: Finally, this resolution urges federal, state, local, territorial, and tribal governments to identify and respond to emerging technological threats to electoral processes in U.S. elections by providing adequate funding and resources to: 1) Enable the sharing of information among election officials, governments, academia, nonprofit organizations, and the private sector to identify and combat emerging technological threats to electoral processes; 2) Facilitate responses, such as government guidelines, training, and public awareness education, to such emerging technological threats; 3) Promote government, private sector, and academic research on such emerging technological threats; and 4) Develop enhanced administrative, physical, and technical safeguards and technologies to deter, detect, and respond to such emerging technological threats.

The following is a recap and summary of the detailed Report submitted with the Disinformation Resolution.

Report Accompanying Disinformation Resolution

In furtherance of the ABA's strong support for free, fair, and impartial elections, the Disinformation Resolution targets the spread of false, deceptive, or misleading statements, information, acts, or practices, amplified by the use of technology and social media, all of which threatens the integrity of elections, which form the

foundation of our democracy. Immediate action is required across government and the private sector to protect the 2020 elections as well as future elections.

This is the second of three cybersecurity resolutions that address interference in U.S. elections:

First, the ABA House of Delegates at the 2020 ABA Midyear Meeting unanimously adopted Resolution 118, which focused on election cybersecurity and protection of the entire "election process," including election management by private sector companies.

Second, this Disinformation Resolution urges the U.S. Congress, state and local legislatures, and social media companies to act to protect voting and other core electoral processes in U.S. elections.

Third, as a companion to the Disinformation Resolution, a Resolution urges federal and state governments and private sector entities to promote digital literacy, civic education, and public awareness to build societal resilience to domestic and foreign malign disinformation operations.

The Disinformation Resolution is narrowly tailored to focus on foreign interference with the core electoral processes (voting, voter registration, vote tabulation, and vote reporting) that can be exploited to undermine the integrity of U.S. elections. It proposes necessary and achievable steps that government and private sector companies should take, while respecting the proper balance of interests under the First Amendment. Toward that end, the Resolution focuses on speech tied to the time, place, or manner of voting, which can be regulated by the U.S. Congress under the Constitution. Moreover, the specific proposals in the Resolution are consistent with substantial analysis and research and represent election reforms for which there is widespread consensus.

I. Threats to Voting in U.S. Elections

The Intelligence Community's 2019 Worldwide Threat Assessment identified "online influence operations and election interference" as a global threat and concluded that "[o]ur adversaries and strategic competitors probably already are looking to the 2020 US elections as an opportunity to advance their interests. More broadly, US adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere."

False, Deceptive or Misleading Information: One of the key approaches to such election interference is through the use of false, deceptive, or misleading

statements, information, acts, or practices. Today's technology makes it possible both to corrupt otherwise legitimate messages, and to facilitate the spread of false, deceptive, or misleading statements or information. Several terms and frameworks have emerged to describe information that is false, misleading, or deceptive, with perhaps the most common being the term "disinformation." Disinformation is widely defined as the purposeful dissemination of false information intended to mislead or harm, although it can also consist of true facts, pieced together to portray a distorted view of reality. Misinformation, on the other hand, is generally understood as the inadvertent sharing of false information that is not intended to mislead or cause harm.

The Disinformation Resolution focuses on the following:

Threats to U.S. electoral processes involving disinformation come from three sources: (i) foreign actors, (ii) domestic actors, and (iii) bots.

1. Malign Foreign Influence Operations Are Targeting U.S. Electoral Processes

Malign foreign influence operations include covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic

institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives. Such actions can pose a threat to national security and violate federal law.

The U.S. Department of Justice (DOJ) Cyber-Digital Task Force Report (July 2018) concluded that elections are a "particularly attractive target for foreign influence campaigns because they provide an opportunity to undermine confidence in a core element of our democracy: the process by which we select our leaders." The Report describes the types of foreign influence operations that use disinformation to interfere with U.S. elections:

► Cyber operations can target election infrastructure or the power grid or other critical infrastructure in order to impair an election.

► Operations aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even simply spreading disinformation suggesting that such manipulation has occurred) could undermine public confidence in election results.

► Covert influence operations, including disinformation operations, are designed to influence public opinion and sow division. Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation or divisive messages. They could

seek to depress voter turnout among particular groups, encourage third party voting, or convince the public of widespread voter fraud to undermine confidence in election results.

► These operations could be reinforced by the use of "bots," which are automated programs that can expand and amplify social media messaging and bolster desired narratives.

►The most well-documented example of foreign attempts to influence elections comes from Russia. Volumes of evidence establish that Russian cyber operations targeted election infrastructure in the U.S. in order to undermine the integrity and availability of the 2016 elections.The significance of those efforts was further emphasized in February 2018, when 13 Russian nationals and three Russian companies were indicted for allegedly conducting what they called "information warfare against the United States," with the stated goal of "spread[ing] distrust towards the candidates and the political system in general."

A report by the Center for Strategic and International Studies (CSIS), *Beyond the Ballot*, named the tactics "new generation warfare," in which Russia used a combination of propaganda channels to maximize the effectiveness of its disinformation campaigns. Exploiting social media platforms is effective because attribution is difficult.

Russia is the largest, but not the only, foreign threat. U.S. intelligence agencies and law enforcement have expressed concern "about ongoing campaigns by Russia, China and other foreign actors, including Iran, to undermine confidence in democratic institutions and influence public sentiment and government policies."

The risk of foreign interference in U.S. elections remains at critical levels. The DOJ Cyber-Digital Task Force concluded that "[f]oreign cyber-enabled and other active efforts to influence our democratic processes, including our elections, demand an urgent response."

2. Domestic Actors Are Creating and Amplifying Disinformation Designed to Interfere with U.S. Electoral Processes

Common Cause and the Lawyers' Committee for Civil Rights Under Law observed in a report that "[d]eceptive election practices occur when individuals, political operatives, and organizations intentionally disseminate misleading or false election information that prevents voters from participating in elections."

These tactics often target traditionally disenfranchised communities – communities of color, persons with disabilities, persons with low income, eligible immigrants, seniors, and young people. These "dirty tricks" often take the form of flyers or

robocalls that give voters false information about the time, place, or manner of an election, political affiliation of candidates, or criminal penalties associated with voting. Today, with a majority of Americans receiving information via the Internet and social media platforms like Facebook and Twitter, and given the viral nature of such communication tools, the potential is greater than ever that these tactics will deprive even more voters of the right to vote.

The CSIS *Beyond the Ballot* report observed that "[p]erhaps the most dangerous aspect of social media is the ease with which stories can be amplified in both intensity and reach. Russian troll farms have greatly contributed to amplifying divisive messaging on both sides of already contentious issues in the United States in the hopes of instigating more examples of deceptive election practices and intimidation, including distributing flyers with bogus election rules, flyers advertising the wrong election date, deceptive online messages, and robocalls with false information.

CSIS concluded that domestic audiences contribute to the spread of disinformation, and these "'unwitting amplifiers' — unknowingly falling for and spreading propaganda — play a large role in fueling the Russian propaganda machine and giving legitimacy to certain claims made by Russian state-sponsored media, inauthentic domains, and fake online accounts. Increasingly, domestic voices are actually the originators of content repurposed by Russia."

Domestic and foreign interference can affect the outcome of elections. Control of state legislatures has hung in the balance in states with razor-thin vote margins in recent elections. Carefully targeted interference in only a small number of key precincts where the vote is very close can sway entire elections.

3. Bots Are Disseminating False Information About U.S. Electoral Processes

Bots constitute a major instrument in the dissemination of false, deceptive, or misleading news, including around elections. Bots include "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks." 'Political bots' have been identified as disseminating news around elections.

For example, in spreading disinformation about the coronavirus, Russia is attempting to interfere in the 2020 elections by raising concerns about the health risks to voters entering crowded public polling stations and to election workers, many of whom are elderly volunteers, who may be reluctant to perform their responsibilities. Researchers at Carnegie Mellon University found that nearly half of the Twitter accounts spreading messages on the social media platform about the coronavirus pandemic are likely bots.

II. Protection of Voting and Addressing Interference in Electoral Processes

The Disinformation Resolution consists of five measures narrowly tailored to protect electoral processes by combating the spread of disinformation and addressing interference in U.S. electoral processes. Before discussing those five measures, it is important to note:

► **Narrowly Tailored**: The Disinformation Resolution does not focus on disinformation campaigns broadly – a complex undertaking for future consideration. Instead, it is narrowly tailored to address interference with the election franchise and focuses on core electoral processes – voting, registering to vote, vote tabulation, and vote reporting – that can be exploited to undermine the integrity of U.S. elections.

►**Layered Approach**: The Disinformation Resolution identifies essential, achievable steps that should be taken immediately by Congress, state and local governments, election officials, social media companies, and private sector entities to reduce the risks to U.S. elections. Such a layered approach is needed, because unlike other nations, the U.S. has no centralized, nationwide election authority. The election process in the U.S. is highly decentralized and it is run state-by-state. More than 9,000 jurisdictions of varying size administer the country's elections, with voters casting ballots in 185,000 precincts. On the other hand, election administration and management systems are centralized — run by only a few companies nationwide that work for multiple states. Private companies play an integral role in elections, from manufacturing voting machines and developing software to designing ballots and hosting results websites.

A. The Resolution's Five Measures

(1) ABA urges the U.S. Congress to enact legislation to preserve and protect each American citizen's right to vote in federal elections.

There is an urgent and compelling need for Congress to take action to combat interference in U.S. elections. State and federal lawmakers should create effective laws that protect voters from false, deceptive, or misleading election practices and voter intimidation by foreign principals or their agents so that these schemes do not undermine the integrity of elections.

The first Resolved clause urges Congress to protect each American citizen's right to vote in federal elections by enacting legislation that prohibits the use of false, deceptive, or misleading statements, information, acts, or practices by a foreign principal or its agent (as defined in 22 U.S.C. §611(a)-(c)), regarding the time, place, or manner of voting, to interfere with core electoral processes (voting, registering to vote, vote tabulation, and vote reporting).

Voting is a fundamental Constitutional right. It is a central aspect of the U.S. Constitution, amendments, and federal laws. Constitutional amendments guarantee and protect the right to vote. Article 1 of the Constitution gives states the responsibility of overseeing elections. Constitutional amendments have been enacted and federal laws to protect voting rights have been passed since then. Constitutional Amendments: 15th Amendment: gave African-American men the right to vote in 1870; individual's right to, and integrity in, the vote. Moreover, Congress has a paramount interest in protecting federal elections and ensuring that they are fair and impartial; the Resolution follows the well-established approach that Congress has followed over many years of enacting statutes that protect federal interests. The 19th Amendment: ratified in 1920, gave American women the right to vote; 24th Amendment: ratified in 1964, eliminated poll taxes; 26th Amendment: ratified in 1971, lowered the voting age for all elections to 18.

The first Resolved clause thus addresses interference with federal elections and is limited to interference by foreign principals or their agents. Furthermore, it focuses on core electoral processes – voting, voter registration, vote tabulation, and vote reporting. The terms in the first Resolved clause are used historically in various statutes. Whether any statement, information, act, or practice is false, deceptive, or misleading depends on the facts and context of the situation. Federal agencies have defined some of these terms in the course of their enforcement of various statutes. Their work, as well as civil and criminal cases, have produced a body of law about what these concepts mean.

False, deceptive, or misleading statements or information can take many forms. Legislators, prosecutors, law enforcement, and judges routinely make judgments about their meaning based on the facts. Furthermore, with respect to analyzing technology aspects of content on digital media, researchers have developed methodology and approaches to detect and analyze false, deceptive, and misleading content.

(2) ABA calls on state and local governments and legislatures to enact legislation to preserve and protect the right to vote.

States have broad authority to pass laws to protect the right to vote. State and local governments are not limited to time, place, or manner of voting; they have broader authority. This second Resolved clause refers to U.S. elections; there is no limitation on state and local legislatures protecting state and local elections or federal elections.

Congress and some states have attempted to address deceptive election practices, but few laws have been passed that directly address this type of conduct. *The Deceptive Election Practices and Voter Intimidation* report by Common Cause and

the Lawyers' Committee for Civil Rights Under Law documents the need for states to enact laws to address interference in elections.

(3) Changes to legal requirements for paid political campaign advertisements are needed to provide transparency concerning the source of digital advertising and to identify each entity that paid for a communication on Internet-based/digital media.

Paid advertisements were central to the disinformation campaign launched by Russia during the 2016 election. The third Resolved clause will address this problem by enhancing disclosure requirements for political ads on online platforms. The ABA urges Congress to enact legislation regarding paid political campaign advertising that requires meaningful transparency concerning the entity that paid for the communication and requires consistent disclaimer and attribution requirements for all media, including television, radio, print, and Internet-based/digital media. By focusing on transparency, the Resolution will help to ensure that political advertising hosted by all types of media, including television or radio, providers of cable or satellite television, or online platforms, is not directly or indirectly purchased by a foreign principal or its agent.

Federal campaign finance law sets forth disclosure and disclaimer requirements for certain types of political campaign advertisements. The term disclaimer refers to an

attribution statement that appears on a campaign-related communication. The Federal Election Campaign Act (FECA), 52 U.S.C. § 30101 *et seq.,* sets forth disclaimer requirements, providing that certain political campaign communications contain attribution statements. At least states require some type of disclaimer statement to accompany political advertisements. Typically, disclaimer statutes cover advertisements made through long-established media forms, such as printed publications, television, and radio. Many statutes, however, are either ambiguous or silent regarding disclaimer requirements for political advertisements made via the Internet. More than a dozen states have explicitly addressed disclaimer requirements for online political advertisements. A handful of states impose no disclaimer requirements on political advertising, regardless of the medium through which it is conveyed.

Generally, the U.S. Supreme Court has upheld the constitutionality of such transparency requirements, determining that they serve the governmental interests of informing the electorate, deterring corruption or its appearance, and facilitating enforcement of the law.

The U.S. Supreme Court's relevant case law informs the constitutional bounds of any legislation to change the federal disclaimer and disclosure requirements. Regarding disclaimer requirements, the Court has upheld the constitutionality of current FECA disclaimer requirements in *McConnell v. FEC*, 540 U.S. 93, 230-31

(2003), and again in *Citizens United*, 558 U.S. at 367 (2010). In upholding the current requirements, the Court emphasized how disclaimers provide critical information about advertising sources so that the electorate can more effectively judge the arguments they hear. Hence, the Court signaled that should Congress enact additional disclaimer requirements, a reviewing court is likely to uphold such requirements to the extent they are substantially related to the informational interests of the electorate. In Congress, the Honest Ads Act, S. 1356, was introduced to help prevent foreign interference in future elections and improve the transparency of online political advertisements.

(4) ABA urges social media companies to take immediate steps to address interference with the right to vote in U.S. elections.

Social media companies' policies on disinformation are evolving and have been enforced unevenly or in an *ad hoc* fashion. In the fourth Resolved clause, the ABA proposes reasonable and appropriate measures that social media companies should take to address election interference. The proposal urges a series of voluntary steps rather than adopting mandatory measures. Thus, the ABA urges social media companies to avoid governmental content regulation by demonstrating that they can adopt meaningful policies to combat the spread of disinformation and consistently implement them. Social media companies have a broad scope to address election problems. They are doing more now, but immediate action is required to address the problem of interference in elections in a comprehensive manner.

The Resolution proposes steps that are framed around the observations of various organizations that have examined the issue in depth (discussed in Section II.C. below). More specifically, the Resolution urges social media companies to: 1) Identify, and either label or remove, as appropriate, accounts that: a) Are used by a foreign principal or its agent engaged in communications or actions to interfere with electoral processes, including efforts to suppress voter turnout or attempts to deceive viewers into thinking the account belongs to a U.S. entity or national; b) Disseminate false, deceptive, or misleading content to interfere with electoral processes; or c) Are used by bots or other technology to post automated false, deceptive, or misleading content to interfere with electoral processes. 2) Make their terms of service or rules consistent with the foregoing recommendations; 3) Report to the public periodically about the results of the efforts to identify, label, or remove certain accounts; and 4) Educate users to beware of disinformation campaigns and deceptive practices that could interfere with electoral processes.

By virtue of its global reach, social media messaging pervades elections. Social and political discourse can easily be distorted. Foreign principals and their agents have no role in U.S. elections. As detailed in the 2018 criminal indictment of Russian

military officials, foreign principals can establish hundreds of accounts online with stolen or fictitious identities.

"Deepfake" videos can portray or depict candidates saying and doing things they never said or did. For-profit firms in the U.S. and worldwide can be hired to spread disinformation to promote discord on the domestic front. Unwitting Americans can be manipulated to both spread the false information and attend election rallies and protests.

Finally, specific platforms (*e.g.,* WhatsApp and Instagram) may be selected as preferred vehicles because they are widely used and have a broad scope, based on their usage by millions of Americans every day.

Asking social media companies to identify, and label or remove, as appropriate, accounts used by foreign principals or their agents to interfere with electoral processes avoids the controversy that might accompany a Congressional mandate to take down false, deceptive, or misleading content. Yet, the proposed Resolution sends a direct signal to social media companies to address this issue by either removing or labelling suspect material, thus striking an appropriate balance between protecting voting and free speech.

Researchers have documented the serious and increasing problem of the use of bots in disseminating false, deceptive, and misleading content about elections. In the interest of promoting transparency, the ABA also urges social media companies to report periodically on the results of their efforts to either label or remove accounts so their experiences can be used to develop further reforms, if necessary.

Finally, the fourth Resolved clause urges a widespread education program to inform citizens about the manipulation and misinformation potential of the technology they use every day. All Americans need to develop a healthy skepticism about the information they consume and learn how to weigh the veracity of reports, posts, feeds, photos, videos, audio content, infographics, and statistics within appropriate contexts.

(5) Governments should provide adequate funding and resources to identify and respond to emerging technological threats to electoral processes.

Historically, the U.S. has experienced shocks from unexpected events, in some cases leading to tragic results. COVID-19 is only the latest example. Cyber threats and resulting data breaches, as well as the Russian interference with the 2016 election, are other examples. The root cause of all of them was lack of preparation.

Deepfakes: Many of the risks we face today arise from scientific and technological threats. One currently emerging threat to elections is the phenomenon of "deepfake"

videos and images produced by artificial intelligence (AI) systems. Attackers using AI can produce video images of politicians or celebrities appearing to say things that they never really said. Deepfakes could influence opinions and resulting voter behavior. How can the U.S. better prepare for emerging threats? The fifth Resolved clause is designed to help identify and address possible harm to electoral processes from sources and vulnerabilities we know little or nothing about yet. Steps that should be taken to address emerging threats include information sharing, education, and research into new threats. Finally, governments should fund responses to these threats, including for new safeguards to deter, detect, and respond to cyber attacks.

B. The Resolution Builds on Leading Reports

The recommendations in the Resolution are consistent with substantial analysis and research by professionals who have addressed the issues in depth. The Disinformation Resolution builds on the consensus that has emerged among government officials, academia, and leading organizations as to what must be done to ensure the integrity of U.S. elections.

Conclusion

Cybersecurity is a professional responsibility that all legal professionals, whether in the public sector or private sector, must accept as an ethical and professional obligation. Amidst a multitude of laws, regulations and conventions, some domestic and many international in scope and application, we must recognize and understand the duties that are imposed upon corporations, state actors, and individuals to safeguard and protect valuable, sensitive and/or proprietary data.

Privacy laws – and the expanding expectation of privacy rights – are proliferating and must be heeded, with drastic consequences for failing to do so.

The genie has long since gotten out of the bottle. Technology is now with us. That technology must be used responsibly. Each of us face difficult legal, regulatory and even political issues with regard to data protection, privacy and cybersecurity. We can and should take a proactive and formative role in giving careful consideration to these issues as we gain a foundational understanding and, hopefully, the ability to tackle them within a fact-based, logically informed and legal framework.