NEW YORK CITY BAR

RECOMMENDATIONS RESPECTFULLY SUBMITTED TO THE TRUMP ADMINISTRATION REGARDING INFORMATION TECHNOLOGY AND CYBER LAW

The Information Technology and Cyber Law Committee of the New York City Bar Association is honored to provide our recommendations relating to the subject matter of our committee for the Trump Administration's consideration.

I. CYBERSECURITY: ESTABLISHING NORMS

a. Establishing Cybersecurity Norms

We urge the new administration to continue to enhance United States governmental efforts to participate in and advance worldwide cybersecurity. In particular, we urge you to work with private stakeholders to develop norms of cybersecurity. These stakeholders include private providers of networks and internet functionality, financial institutions, hardware manufacturers, software providers, and other developers and providers of Information Communication Technology ("ICT"). These various stakeholders around the globe have extensive experience in dealing with cyberattacks and often bear the brunt of attacks by state and/or criminal actors. As the speed of change in cyberspace—including cyberwarfare, cyberespionage and cybercrime—vastly outstrips the speed of most governmental institutions to identify and counter such threats, it is important that cybernorms be developed in coordination with those who have firsthand and varied experience in this realm.

b. Consequences for Cybercrimes

In addition to developing norms for detection and prevention, norms must also be developed concerning punishment for engaging in cyberwarfare and other cybercrimes. In so doing, we urge the administration to carefully consider the impact of private stakeholders' ability to strike back with their own cyberattacks in real time. Such countermeasures may seem expedient, appear confined to the particular concerned entities and might exact a toll from the initial cyberattacker that includes a disincentive for the cyberattacker to strike that particular target in the future. On the other hand, mistaken attribution could escalate an already tense internet space teeming with cyberattacks, and could devolve into cyberwars between otherwise "respectable" internet citizens.

c. Overreach

While efficiency and effectiveness requires that public, private and government sectors all work in coordination, law enforcement and other government agencies should not be authorized to plant "backdoors" or other surreptitious means of access into private companies, networks and devices. Such activities limit trust between the private and public spheres and inhibit the establishment of norms of conduct.

Recommendations:

1. Cybersecurity concerns and the establishment of norms of conduct might be addressed globally by trusted institutions that transcend any particular government or private interests. The Centers for Disease Control and Prevention ("CDC") may serve as a good model. Such a group can monitor and facilitate the sharing of information concerning denial of service attacks, botnets, malware, hacking and other evolving forms of cyberwarfare. This would strengthen the ability of all actors to resist such attacks. A global model similar to the CDC would maximize efficiencies and ensure that government agencies, private enterprise and other stakeholders have access to relevant information in a timely and efficient manner. However, one significant challenge with respect to cybersecurity that does not arise in the public health context is that some participants in such a forum might also be responsible for the very cyberhacking activities that the forum was intended to combat.

2. We also urge further study of the risk factors that might escalate a cyberskirmish into a war in the physical world. A well-placed cyberattack would have the potential to impact infrastructure or take lives every bit as effectively as traditional weapons of warfare.

II. INFRASTRUCTURE

a. Cybersecurity as part of Physical Infrastructure

Physical infrastructure is increasingly dependent on technology and, therefore, on the security of those technological functions. As such, investment in the country's infrastructure must include cybersecurity infrastructure. All aspects of our lives are increasingly dependent on technology, including transit and many facets of transportation, drinking water, waste management, schools, energy, commerce and communication. Indeed, the U.S. Department of Homeland Security's website lists various sectors which require infrastructure upgrades and maintenance, including the Information Technology Sector.[1] Strengthening U.S. cybersecurity infrastructure is critical to maintaining our power grids, communications bases and transportation hubs.

[1] *See* https://www.dhs.gov/information-technology-sector and https://www.dhs.gov/critical-infrastructure-sectors (last visited Feb. 13, 2017).

Recommendation:

1. Include cybersecurity infrastructure in all infrastructure plans and allocations because this investment is crucial to national security and to the continued functioning and development of our towns, cities and communities.

b. Economy, Education and Infrastructure

To support a thriving economy and economic growth, both domestically and internationally, the U.S. must promote a robust workforce ready for the 21st century.

i. Broadband Regulation

For the U.S. workforce to remain competitive, the federal government must work toward minimizing barriers to broadband service, expanding access to broadband connectivity for schools and public libraries, and promoting educational opportunities centered on technological literacy.

Literacy should remain an objective at both the local and federal level. To this end, there must be robust investment in urban and rural broadband across the nation. The rollout of rural broadband should include clear benchmarks and timeframes. Municipal infrastructure projects and upgrades must take into account the importance of accessibility in the areas of education, high-speed broadband inclusion and digital literacy.

The federal government must balance spectrum allocations and sharing in such a way that this important resource serves the public while promoting private sector innovation. Spectrum (the radio frequency by which wireless communication travels) is a scant and precious resource. The Federal Communications Commission manages spectrum through licensing systems granted to non-federal users. There is concern over spectrum shortages, interference, and mergers that would lock in control of large blocks of spectrum with one or two corporations. Any policy proposal by which spectrum is "shared" between government and commercial use, licensed and unlicensed use, or innovative solutions must be guided by the goal of achieving maximum access for all citizens without limiting the type of content delivered to consumers.

For example, "zero-rating" models do not charge consumers for data usage for certain content when the creators or suppliers of that content have paid the channels/carriers. Therefore, in these models the content appears "free" to the consumer, but the content creator is actually paying for consumers to view that content with or without the consumers' knowledge. Proposals to free up previously-owned government spectrum for the wireless industry should only be considered if the plans promote access to each and every consumer regardless of income while also supporting the newest innovation in the marketplace. Innovation is critical to a strong economy and improved life conditions. However, public spectrum must not be used solely for private gain, and control over this public resource must not be granted to a small handful of companies.

The increasing number of users of the Internet, both across the United States and around the world, and the ubiquity of technology in all aspects of modern life should translate to a model of government support that promotes connectivity and does not leave a single user behind, regardless of geographical or financial limitations. To remain competitive globally, consumers require access to multiple sources of diverse and high-quality information. This is an area in which both the public interest and private sector agree. A strong Internet is supported by diverse content and expanded connectivity.

ii. Economic Motivation

The future of the U.S. economy will depend on a robust and flexible approach to regulating "accessibility" by promoting open Internet policies.

The sharing economy, for example, is in its nascent stages but already has generated considerable revenue. In order to continue to expand this sector of the economy, we urge the federal government to regulate cautiously and prudently, and in a manner that supports innovation and promotes entrepreneurship.

Moreover, to keep abreast of and ahead in the global marketplace, the U.S. should focus on developing and providing educational programs, including adult educational programs, centered on digital literacy in order to equip the workforce with the necessary skills to keep pace with technological advancements.

Furthermore, to maximize our strength, skills and knowledge base in the digital age, we must promote a diverse workforce, and attract and retain high-skilled workers from all backgrounds.

Recommendations:

1. Investment in the "raw materials" of technology infrastructure will be the key to America's continued leadership in the digital global economy. These raw materials include: ubiquitous broadband availability; well-planned cyberarchitecture, *viz.* traditional infrastructure that uses technology to protect and maintain its integrity and continued functioning in the face of cyberthreats; and training and retraining citizens in the use of varied and sophisticated forms of technology.

2. Update laws and regulations to encourage technological growth, investment in various aspects of technology, and ease of use and access by all citizens. Revisions of U.S. laws that concern infrastructure, both traditional and technological, must also consider the use and control of data, e-commerce and the global economy.

III. PRIVACY LAWS

Privacy laws in the U.S. are disparate, sector-based and not easily reconciled with the laws of other jurisdictions, including the European Union, Argentina and Israel among others. This makes it difficult for businesses to comply with the laws of various jurisdictions and can stymie efficient world trade, particularly as the world grows increasingly dependent on technology, data and cross border commerce.

U.S. businesses and other entities will benefit from a review of what the multitudes of privacy related laws are meant to protect and how data can be efficiently managed.

a. The Privacy Act

Forty-two years ago, the United States enacted the Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, 5 U.S.C. §552a) (the "Privacy Act"). The law governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals ("PII") by the federal government.

The initial draft of the Privacy Act was based on a report of an advisory committee of the Department for Health, Education and Welfare ("HEW"). The report stated that individuals have a right to participate in how their personal information is used and to whom it is disclosed. According to the HEW report, that right is provided through fair information practices. Those initial five principles inspired the Organization for Economic Cooperation and Development ("OECD").

In 1980, the OECD built upon those principles and created a set of eight principles commonly referred to as the Fair Information Practices (FIPs).[2] The OECD issued guidelines on the protection of privacy which have been adopted by all OECD members and forms the basis of many privacy protection laws across the globe. However, in jurisdictions such as the E.U., FIPs and personal data protection laws are not limited to governmental agencies or to specific sectors. Instead, E.U. data protection laws apply to all entities in the private and government sectors which handle personal information or personal data. The E.U. and several other jurisdictions accord broad protections to individuals' personal information with comprehensive laws which are updated in an effort to keep pace with technology.

Recommendation

1. Update the Privacy Act by extending its application, consistent with First Amendment requirements, beyond government to the public and private sectors and with an eye towards compatibility with data privacy and protection laws around the world.

[2] Pam Dixon, "A Brief Introduction to Fair Information Practices", World Privacy Forum, Updated Dec. 19, 2007, *available at* https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (last visited February 13, 2017).

b. National Data Breach Notification Law

An entity that uses, transmits or stores certain personal information must do a variety of things when that entity has a breach: assess the situation, contain the harm/breach, notify authorities and, depending on the type and extent of information concerned, notify the affected individuals. A breach or incident is generally defined as unauthorized access to an individual's personal information or the possibility of such access.

The precise definition of the personal information, who needs to be notified, within what time-frame and other measures are all determined by individual state laws—forty-seven of them. In addition, there are four other jurisdictions with their own breach notification laws: Guam, Puerto Rico, the U.S. Virgin Islands and Washington, D.C.

This state by state assessment and determination is costly and burdensome to the affected entity and can have a detrimental impact on the affected individuals.

Recommendation

1. It is not possible to completely secure data or prevent data breaches. However, a uniform breach notification law which clearly defines personal information, sets forth whether or not that information needs to be protected and, if so, how, and sets forth which definitive authority(ies) to notify, will go a long way towards setting clear standards and better protecting personal information.

c. Globally Compatible Privacy Laws

It is natural that sovereign nations will enact laws appropriate to their country without regard to other nations' laws. However, in world where technology touches every aspect of life and technology by its very nature is borderless, the lack of regard to coexistence with extraterritorial laws related to technology is short-sighted and may have a detrimental impact on business and economic growth. The regulation and protection of personally identifying information ("PII") is one of these areas well worth examining.

The difference between the European approach to personal data and the U.S. approach to PII is stark. The E.U. considers an individual's right in and to their own personal data a fundamental right, while the U.S. treats much of the same personal data as a commodity. These differences have impacted commerce as demonstrated by the invalidation of the Safe Harbor mechanism[3] and the scramble to enact its replacement, the Privacy Shield.[4] The impact on trans-Atlantic commerce is likely to increase after May 2018 when the E.U.'s General Data Protection Regulation ("GDPR") goes into effect. This rigorous data protection law will have far-reaching

[3] "Safe Harbor" was a mechanism devised by the U.S. Department of Commerce and E. U. regulators in 2000 to enable the transfer of personal data from the E.U. to the U.S. which is deemed an adequate jurisdiction for purposes of data protection. Safe Harbor was invalidated by the E.U. Court of Justice in October 2015.

[4] "Privacy Shield" is a preliminarily acceptable way to legally transfer personal data from the E.U. to the U.S.; however, it is currently under legal challenge in the E.U.

economic consequences for any U.S. company which markets to the E.U. or conducts business there.

Technology companies are some of the largest entities collecting, using, handling and storing personal data. Many of the world's largest technology companies are U.S. businesses (e.g. Apple, Microsoft, Facebook, Amazon, Google, IBM, etc.). For its own business interests and in the interest of its citizens, the U.S. will be well-served to take the lead on data protection/data privacy laws to ensure that they are compatible with data protection/privacy laws around the world.

Within the United States itself, there is mounting concern over the lack of a cohesive legal framework governing data collection and protection practices of various entities, including telecommunications and internet services companies, retail merchants, marketing firms, data collectors and, U.S. and State government agencies. Ever-increasing incidents of data breaches aggravate the concern.

Recommendation

1. Enact personal data usage laws which respect, consistent with First Amendment requirements, individuals' rights to their personal data and which apply to all States and across all sectors—public, private and government. This will facilitate compliance and U.S. participation in world trade while upholding the American traditions of freedom and respect for individual privacy.

IV. ELECTRONIC COMMUNICATIONS PRIVACY ACT

a. ECPA Update

The Electronic Communications Privacy Act of 1986 (ECPA) is entering its third decade. The law was originally enacted to support restrictions on government "wire-taps" and it was extended to require warrants in order for government and law enforcement to access this type of communication. However, as technology has advanced, the ECPA, particularly Title II, the Stored Communications Act, has been minimally updated. Whether the protections for stored communication and the content of electronic messages should receive the same stringent warrant requirements as those for wire-tapping remains an open question.

Email became a dominant communication mode over the last two decades, but ECPA does not "neatly" apply to email and other types of instant communication, particularly since much email and text communication is currently stored on cloud servers around the world. ECPA needs an overhaul on several levels and for a variety of reasons.

A recent case illustrates one aspect of the needed reform. In *Microsoft v. United States*,[5] the Second Circuit Court of Appeals held that ECPA in general (and section 2703, the Stored

[5] *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, No. 14-cv-2985 (2nd Cir. July 14, 2016) (*pet. for rehearing en banc filed* Oct. 14, 2016).

Communications Act, in particular) does not apply to data held by an email service provider outside the United States at the time of service, even where the data remains effectively under the control of an American company. In this instance, the U.S. government did not obtain the content of the emails it sought under the ECPA.

According to briefs filed in the case, large email service providers like Google receive over 600 ECPA/SCA subpoenas every month from federal law enforcement authorities seeking information from approximately 1,500 accounts. Many, if not most, of these subpoenas are accompanied by gag orders under ECPA § 2705(b). Thus, for electronic communications service providers, a growing tension exists between the demands of their customers (who want maximum privacy) and the demands of law enforcement authorities (who want maximum disclosure with minimal delay). In addition, such companies must dedicate resources, financial and human, to respond to the ever-increasing requests.

One alternative when the sought-after data is stored outside of the U.S. is the cumbersome process of Mutual Legal Assistance Treaties ("MLAT").[6] This would only apply if the data is stored in a country with whom the U.S. has a MLAT.

Recommendations

ECPA reforms should provide greater search and seizure protections to private electronic communications while ensuring the government retains the ability to obtain such communications with proper judicial review. A key issue in this sensitive area is reciprocity: whatever the U.S. asks of service providers, it can expect other nations to ask as well. Any changes to the ECPA will also have an effect on global commerce. The U.S. must be current in its legal treatment and policy understanding of privacy and communications.

1. Amend Title II of ECPA (the Stored Communications Act) to expressly apply regardless of the location of the data and keeping the reciprocity point in mind. At this time, there are at least three pending bills that would change the current situation.[7] Without expressing a preference for any of the bills, we recommend legislative measures that provide for a district court to modify ECPA subpoenas or warrants if compliance would be unreasonable or oppressive (*see, e.g.,* Fed. R. Crim. P. 17) if such legislation includes: (a) senior-level approval within the Department of Justice, (b) Congressional reauthorization after a limited number of ECPA subpoenas, warrants, and gag-orders, (c) a pre-application attempt to determine the nationality or location of account holders, (d) a presumptive warrant requirement for private email accounts, and (e) an appropriation to facilitate international cooperation with respect

[6] MLATs allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See* U.S. Dep't of State, 7 Foreign Affairs Manual § 962.1 (2013) *at* https://fam.state.gov/FAM/07FAM/07FAM0960.html (last visited Feb. 13, 2017). The United States is a party to a MLAT with each member of the European Union.

[7] *See, e.g.,* the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act"); the Email Privacy Act; and the International Communications Privacy Act.

to compelling the prompt disclosure of electronic communications for law enforcement purposes.

2. Reform the ECPA to include stricter protection to e-mail, text and other messaging content and protect the privacy of U.S. personal communication.

3. Uphold the ECPA warrant requirement with an overarching stringent warrant requirement to access the content of 21st century forms of communication; emails, text, instant messaging and those yet to be implemented.

4. Renegotiate MLATs to establish clear and efficient procedures and definitions (regarding e.g., data location) for bilateral cooperation in this field, consistent with the updated statutory framework.

V. COMPELLING ASSISTANCE TO LAW ENFORCEMENT

In the wake of the San Bernardino shooting on December 2, 2015, the government demanded that Apple provide "reasonable technical assistance" to the FBI by writing software to unlock a shooter's iPhone. This brought the question of whether the government could force companies to create backdoors into their technology to the forefront of public debate.

On February 16, 2016, a federal magistrate judge ordered Apple to help unlock the iPhone.[8] After a failed month-long, behind-the-scenes negotiation between Apple and the government seeking a deal to unlock the phone, Apple opposed the order. Ultimately, the FBI paid a contractor some $1.3 million to bypass the security feature at issue and access the device, obviating the need for a hearing on the matter.

Although that particular situation was resolved, government demands for private technical assistance constitute a recurring constitutional issue ripe for legislation. Forcing companies to write code or create a backdoor that allows the government to access individual's personal devices raises Fourth amendment privacy concerns as well as questions about the scope of government authority under the All Writs Act of 1789, which the government has relied on in seeking similar orders against Apple and other companies. In February 2016, a federal magistrate judge in the Eastern District of New York refused to grant such an order, stating that Congress has created no statutory authority that specifically speaks to the question of whether the government could compel a company such as Apple to bypass the security on one of its devices, and that in the context of this lack of express statutory authority, it is unclear whether the All Writs Act applies.[9] As such, until there is a clear course of action, we recommend that the administration direct federal authorities to restrict use of the All Writs Act for these purposes.

---

[8] *See Order of Magistrate Judge Sheri Pym of the U.S. District Court for the Central District of California*, *available at* https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf (last visited Feb. 13, 2017).

[9] *In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court*. 15-MC-1902 (E.D.N.Y. Feb. 29, 2016).

We urge the administration to work with Congress on this issue to develop a workable legal framework that balances the free speech and privacy rights of Americans protected by the First and Fourth amendment with interests of law enforcement to access devices which contain much more than law enforcement may otherwise be entitled to review. New legislation should weigh the priorities, values, sensibilities, and rights of all concerned: law enforcement, private enterprise and private citizens.

John S. Kiernan
President, New York City Bar Association

Maia T. Spilman
Co-Chair, Information Technology and Cyber Law Committee

Reissued April 2017