THE PERMANENT MISSION
OF THE
UNITED STATES OF AMERICA
TO THE
UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS
IN GENEVA

April 26, 2018

Office of the High Commissioner for Human Rights
United Nations Office at Geneva

Dear OHCHR:

Thank you for your letter dated March 8, 2018, requesting input on human rights challenges relating to the right to privacy in the digital age, including on principles, standards and best practices with regard to the promotion and protection of the right to privacy.

In response to your request, the United States provides the attached information.

Sincerely,

Jason R. Mack
U.S. Deputy Permanent
Representative to the UN Human
Rights Council

SUBJECT: U.S. Submission to Report on Privacy in the Digital Age

1. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.

The freedom from arbitrary or unlawful interference with privacy is protected under the Fourth Amendment to the U.S. Constitution, which protects persons from unlawful searches and seizures by the government.[1] The Supreme Court has also stated that a right to privacy vis-à-vis the government emanates from the First Amendment (freedom of speech), Third Amendment (freedom from quartering soldiers), Fifth Amendment (freedom from self-incrimination), Ninth Amendment (protection of other rights), and Fourteenth Amendment (right to due process). A few state constitutions enshrine a right to privacy that mirrors language in the U.S. Constitution. However, with the exception of the State of California, none of these protections extends horizontally, and therefore they do not govern interactions in the private sphere.

Within the private sphere, it is primarily state and federal legislation that dictate the rules for collection and processing of personal information. At the federal level, Section 5 of the Federal Trade Commission Act, which authorizes the Federal Trade Commission (FTC) to take enforcement action against unfair and deceptive acts and practices in commerce, is a core privacy enforcement tool. In addition, there are several sector-specific laws governing how certain classes of information must be protected. At the state level, some level of privacy law has been enacted in 48 states. The scope of legislation in each state varies.

There have been several digital privacy developments in the U.S. over the last year. In December 2017, the Federal Communications Commission (FCC) adopted the "Restoring Internet Freedom" Order which restores the classification of broadband Internet service providers (ISPs) as information services under the Communications Act, thereby relieving ISPs of the need to comply with common carrier rules for the protection of Customer Proprietary Network Information (CPNI). CPNI is information about consumer usage of common carrier services, including usage amounts and patterns. The effect of this classification is to place the FTC in charge of enforcing ISP privacy commitments. The Ninth Circuit

[1] For an overview of the U.S. legal framework on privacy, see the United States' periodic reports to the Human Rights Committee regarding its obligations under the International Covenant on Civil and Political Rights, *available at* https://www.state.gov/j/drl/reports/treaties/.

Court of Appeals recently affirmed the FTC's authority to take enforcement actions against ISPs in *FTC v. AT&T Mobility, LLC*, No. 15-16585 (9th Cir. 2017).

In 2017, the FTC brought several privacy and data security enforcement actions and was able to obtain consent decrees from several large companies for general privacy violations, and obtained settlements and judgments for several companies' violations of standing consent decrees. The FTC has also brought several enforcement actions against Privacy Shield-certified companies to ensure compliance with the EU-U.S. Privacy Shield agreement.

Also of note is the first annual review of the EU-U.S. Privacy Shield. The review was held in September 2017 in Washington, D.C. with senior U.S. government officials and representatives from the European Commission and European Data Protection Authorities (DPAs). The European Commission published a report in October 2017 concluding that the Privacy Shield continues to ensure an adequate level of data protection for European individuals. The U.S. and Swiss Government also established the Swiss-U.S. Privacy Shield agreement in 2017.

In U.S. federal courts, the Supreme Court heard arguments in *Carpenter v. United States*. In *Carpenter*, the Supreme Court is reviewing the Fourth Amendment's protections against warrantless searches and seizures as they extend to cell-site-location information. The Court's holding has the potential to alter the current standard that information stored and collected by third-party service providers is not protected by the Fourth Amendment.

In January 2018, the U.S. Congress passed the FISA Amendments Reauthorization Act of 2017 ("FISA" refers to the Foreign Intelligence Surveillance Act). This Act reauthorized Section 702 of FISA for a period of six years. Section 702 authorizes the acquisition of electronic communications of non-U.S. persons located outside the United States for the express purpose of collecting foreign intelligence information. This acquisition must be conducted in accordance with strict procedures approved in advance by the Foreign Intelligence Surveillance Court, and is subject to the Court's ongoing oversight. The Act also added new privacy safeguards which supplement the existing protections.

In March 2018, the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The Act clarifies that warrants issued by U.S. courts to providers in the U.S. compel providers to disclose data in their possession or control, regardless of whether that data is stored inside the U.S. or on servers in

foreign countries. The law also allows the U.S. government to reach agreements with foreign governments to allow foreign court orders to be served directly on U.S. providers for data stored inside the United States. Such agreements are permitted only with countries with strong rule of law and civil liberties protections. Any entity served with foreign legal process subject to one of these agreements could challenge it under the domestic laws of the court that issued it, but could not argue that U.S. law blocks disclosure of the data.

2. Surveillance and communications interception:

a. Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

An essential function of government is to protect the security of the nation and its citizens. In order to carry out this function, the United States and its partners recognize that the collection of foreign intelligence, including through authorized interception of electronic communications, is essential. Governments must have insights into the world around them, and to draw those insights, they need intelligence services to seek out and analyze information that is not publicly available. Intelligence services must operate with some degree of secrecy. Otherwise, their efforts to obtain non-public information will be thwarted, and they will be rendered ineffective. Democratic governments must thus strike a balance between the transparency needed for their legitimacy and the need to protect the secrecy of their intelligence gathering activities.

The United States has actively sought to strike the appropriate balance between transparency of intelligence activities and the need to keep those activities secret. In 2013, then-President Obama directed the Intelligence Community (IC) to make public as much information as possible about its surveillance programs with the goal of earning and retaining public trust. To accomplish this goal, the Office of the Director of National Intelligence (ODNI) directed an interagency effort focusing on ways in which the IC could enhance transparency. This effort resulted in the Director of National Intelligence (DNI) publicly releasing statistics, beginning in 2014, relating to the use of critical national security authorities, including the Foreign Intelligence Surveillance Act (FISA), in an annual report called the Statistical Transparency Report Regarding the Use of National Security Authorities (commonly referred to as the Annual Transparency Report). Significantly, in 2015, the DNI signed the Principles of Intelligence Transparency

for the IC, appointed a Chief Transparency Officer for the IC, and authorized the creation of the Intelligence Transparency Council. The United States Congress has also affirmed the importance of transparency by incorporating public transparency reporting requirements into law, specifically: (i) the 2015 USA FREEDOM Act that codified a requirement for reporting on many of the statistics that the DNI was already providing in the Annual Transparency Report and that required the release of certain Foreign Intelligence Surveillance Court (FISC) opinions and (ii) the reauthorization of the FISA Amendments Act of 2017 that required additional statistics to be included in the Annual Transparency Report. Furthermore, the IC's coordinated and proactive approach has resulted in many transparency successes including the re-launch of the INTELLIGENCE.GOV website to improve public access to information about the IC; the creation of a historical declassification program; and the unprecedented amount of details released regarding the use and oversight of FISA, including Section 702. As recently as February 2018, the DNI signed a newly revised version of the Intelligence Community Directive (ICD) 107 on Civil Liberties, Privacy, and Transparency, to firmly establish transparency as a foundational element of securing public trust in the IC activities.

However, even where intelligence activities cannot be disclosed to the public, democratic nations must devise a system of oversight and accountability, with clear rules establishing safeguards to protect individuals' privacy, oversight mechanisms to verify the government is complying with those safeguards, and remedies to address situations where the safeguards have not been complied with. To be effective, intelligence oversight must be tailored to fit within each country's legal system and governing structures, and must take into account the country's unique history, culture, laws, traditions, and interests. Oversight and accountability mechanisms must also keep pace with new and changing security threats.

The United States has a multi-layered set of rules to ensure that the intelligence activities comport with the United States Constitution and applicable statutes, executive orders, and presidential directives. Oversight by all three branches of government – executive, judicial, and legislative – is designed to ensure that intelligence activities are consistent with our rules. For example, there exists a detailed legal regime – the FISA – for authorizing the collection of certain foreign intelligence information through electronic communications and for overseeing the handling of any communications that are collected under FISA. Specifically, FISA requires that the independent FISC approve Government demands for electronic communications from service providers located inside the United States; as part of its approval, the FISC reviews and approves each intelligence agency's procedures

concerning the acquisition, retention, and dissemination of personal information obtained under FISA. Globally, all U.S. signals intelligence is subject to a Presidential Policy Directive 28 (PPD-28) that imposes a number of constraints on collection and use of the data. PPD-28 requires that signal intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality and that signals intelligence activities must be as tailored as feasible. PPD-28 further requires that the collection of U.S. signals intelligence be for foreign intelligence and counterintelligence purposes and that such collection is not for the purpose of suppressing or burdening criticism or dissent, or the disadvantaging of persons based on their ethnicity, race, gender, sexual orientation, or religion. PPD-28 requires that privacy and civil liberties are integral considerations in the planning of signals intelligence activities and it requires each intelligence agency to adopt procedures to safeguard the personal information collected from signal intelligence activities of all persons, regardless of nationality, including procedures restricting the retention and dissemination of their personal data.

3. Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

The U.S. Government recognizes the importance of strong encryption. Encryption and anonymity tools facilitate digital safety for at-risk internet users, including journalists, members of civil society, and citizens from malevolent state and non-state actors, and are a key tool to secure commerce and trade. It is also critical for strong cybersecurity. At the same time, encryption poses a grave challenge for our national security and law enforcement professionals, who work to ensure that malicious actors are held to account and cannot exploit technology as a means to evade the law. We recognize that there is always a risk that encryption may be used for terrorist or other malevolent purposes, and we must do our utmost to combat this. With this in mind, we continue to engage with the private sector to find ways to address the national security and public safety challenges we face with the use of encryption.

Advances in technology that protects individual privacy, such as encryption and an increasing number of options to anonymously engage in online activity (including the proliferation of the Dark Net), has unfortunately also had a dramatic impact on child sexual exploitation. With little fear of being identified or located, offenders congregate online and encourage each other to commit the most egregious offenses

against children. For example, hidden services on the Dark Net that cater to individuals interested in engaging in sexual abuse of children as young as infants can have hundreds of thousands of participants. Most smart phones today are fully encrypted by default. These phones can be used to produce child pornography, share it, access it online, and to identify and groom victims through the use of social media apps.

The combination of online anonymity with encryption is a "one-two punch" that poses serious obstacles to law enforcement's ability to identify and apprehend child sexual predators. Typically, individuals who commit crimes online may be identified and located through their internet protocol address—a process which is not foolproof under normal conditions and which is effectively impossible with normal law enforcement techniques if the offender is on the Dark Net, or is using a virtual private network or proxies. Assuming law enforcement can overcome that hurdle to identify and locate an offender, their investigations may be stymied because the offender's media devices may be protected by encryption, thereby preventing access to critical evidence to prove the offender committed sex offenses against children.

Nonetheless, the United States is committed to protecting children from online sexual exploitation, using laws that prohibit the production, distribution, receipt, and possession of child pornography and online grooming. One such example is "Operation Pacifier," which targeted the administrators and users of "Playpen" – a highly-sophisticated, global enterprise dedicated to the sexual exploitation of children, organized via a members-only website that operated on the Tor anonymity network (a key network within the Dark Web). Playpen's administrators and more than 150,000 other members authored and viewed tens of thousands of postings relating to sexual abuse of children, infants, and toddlers. The results of the operation have been staggering in the United States and abroad—at least 348 arrests in the United States, the prosecution of at least 51 alleged hands-on child sex abusers, and the identification or rescue of at least 55 American children who were subjected to sexual abuse or exploitation; internationally, there have been at least 548 arrests and 296 children identified or rescued from sexual abuse or exploitation.

4. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.

The U.S. FTC has a robust privacy and data security program for U.S. commercial practices that protects consumers worldwide. The landscape of consumer privacy and security protection in the United States has evolved substantially in the last few decades. Many federal and state privacy and security laws have been enacted, and public and private litigation to enforce privacy rights has increased significantly.

The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. As part of this authority, the FTC can enforce the privacy promises that companies make, including when they participate in self-regulatory programs. The FTC also has authority to enforce more targeted privacy laws that protect certain financial and health information, information about children, and information used to make eligibility decisions about consumers. A report of the FTC's privacy enforcement is available at https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives.

Many federal statutes regulate the commercial collection and use of personal information, beyond Section 5 of the FTC Act, including: the Cable Communications Policy Act, the Child Online Privacy Protection Act (COPPA), the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Electronic Funds Transfer Act, the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act (VPPA). Many states have analogous laws in these areas as well.

Regarding personal data in the context of the communications sector, private rights of action are afforded by several federal laws. For example, the Electronic Communications Privacy Act (ECPA) provides a private right of action for the unauthorized interception of electronic communications. The VPPA provides private remedies for unauthorized disclosures of personal information by video tape service providers.

States have also been active in passing laws related to privacy and security. Since 2000, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring businesses to notify individuals of security breaches of personal information. At least thirty-two states and Puerto Rico have data disposal laws, establishing requirements for the destruction or disposal of personal information. Using these laws and other authorities, federal

and state governments have levied significant fines against companies that have failed to protect the privacy and security of consumers' personal information.

Private lawsuits have also led to successful judgments and settlements that provide additional privacy and data security protection for consumers. For example, in 2015 Target agreed to pay $10 million as part of a settlement with customers who claimed their personal financial information was compromised by a widespread data breach. Additionally, in 2013, AOL agreed to pay a $5 million settlement to resolve a class action involving alleged inadequate de-identification related to the release of search queries of hundreds of thousands of AOL members.

5. Growing reliance on data-driven technology and biometric data:

We think it will be important to foster greater discussion and sharing of views on topics related to new technologies, and where expertise and approaches are still developing within governments. Discussions on policy approaches to emerging technologies should include broad participation from a variety of stakeholders including the private sector, academia, and civil society. There are several AI and big data-focused initiatives already underway in this space, and we would be well served to work with them as we foster discussion on this issue.

6. Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, and approaches to protect those individuals.

The United States is well aware that undue interference with privacy can be committed by individual actors. These actors often target and disproportionately affect women, children and other vulnerable populations, including the elderly. The United States, through the Department of Justice, is committed to the vigorous enforcement of criminal statutes that protect individuals' rights to privacy (digital and otherwise), including protecting individuals from theft and/or exploitation of their personally identifiable information, their online identities, their intimate photographs, and other private information. The Department's primary tool has been, and continues to be, the investigation and criminal prosecution of individuals who commit such crimes. Depending on the specific evidence in a particular case, and the specific penalties available, prosecutors might charge such conduct under a variety of statutes, including: cyberstalking (18 U.S.C. § 2261A); interstate threats

(18 U.S.C. § 875(c),(d)); computer fraud and abuse (18 U.S.C. §1030(a)(2), (7); and aggravated identity theft (18 U.S.C. 1028A)).

The United States' commitment to protecting vulnerable individuals from interference with their privacy includes seeking substantial prison sentences for offenders. For example, several months ago, U.S. prosecutors obtained a 60-month prison sentence for Juan M. Thompson, a cyberstalker who stalked his former girlfriend, including distributing intimate images of her and sending hoax bomb threats in her name to various Jewish Community Centers and other organizations. *United States v. Juan Thompson*, 21 17 Cr. 167 (S.D. N.Y. 2017). In 2017, Ryan Vallee, a sextortionist who victimized dozens of teenaged females was sentenced to 96 months in prison. *United States v. Ryan Vallee*, 1:15-cr-00115-01-PB (D. NH 2015). In 2015, U.S. prosecutors obtained a 57-month prison sentence for Michael C. Ford, a prolific sextortionist who victimized over 75 young women in the United States, using his work computer at the U.S. Embassy in London. *United States v. Michael C. Ford*, 1:15-CR-00319-ELR-RGV (N.D. Ga. 2015).

In addition, U.S. courts are encouraged to enhance a sentence when the court deems that a particular victim is a "vulnerable victim." U.S. law defines a "vulnerable victim" as someone who is "unusually vulnerable due to age, physical or mental condition, or who is otherwise particularly susceptible to the criminal conduct." At the sentencing phase, prosecutors regularly seek greater sentences when vulnerable victims are targeted.

In addition to its core law enforcement work, the Department of Justice regularly provides training that is specifically geared toward investigating and prosecuting cyberstalking, sextortion, and related crimes. Through its Office of Violence Against Women and other outlets, the Department of Justice provides victim and witness outreach that is specifically geared toward assisting sextortion victims. The Department of Justice regularly offers its technical expertise to members of Congress who are proposing federal legislation that would specifically criminalize "sextortion" and non-consensual pornography involving adults, "doxing" and other attacks on digital privacy.

7. Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital communications or other forms of processing of personal data by governments, business enterprises or private organizations.

The United States has a multi-layered framework of rules and oversight designed to ensure that the intelligence community exercises its authorities and uses its capabilities properly. First and foremost, the rules must be consistent with the United States Constitution. The rules require a focus on national intelligence, pursuant to priorities established by the nation's leaders. Additionally, specific rules exist regarding the collection, retention, and dissemination of foreign intelligence information.

Specific rules such as statutes (e.g., laws enacted by the United States Congress and signed by the President) that are particularly relevant to the intelligence community include the FISA, the Privacy Act of 1974, and the Freedom of Information Act. These statutes, in turn, may call for implementing regulations, policies and procedures. For example, FISA requires that the government has court-approved procedures governing how it will conduct surveillance subject to FISA and how it will retain and disseminate information collected pursuant to that Act. Any collection under FISA may only be for foreign intelligence information regardless of the target's location or nationality. Additionally, rules such as Executive Orders (E.O.) are executed by the President and have the force of law. Particularly relevant to the IC is E.O. 12333, which directs the duties of the intelligence agencies and imposes key restrictions on how the IC can conduct its intelligence activities, including how information concerning U.S. persons can be collected, retained and disseminated (in other words, only in accordance with procedures approved by the Attorney General, commonly referred to as Attorney General Guidelines). Furthermore, Presidential Policy Directives are another way in which the President establishes rules. For example, PPD-28 establishes rules pertaining to signal intelligence and requires that intelligence agencies develop policies to extend certain protections to all people, regardless of nationality, and that signals intelligence activities shall be as tailored as feasible.

To ensure that the Government complies with the many rules, rigorous multi-layered oversight by all three branches of the Government exists. Within the executive branch, oversight includes internal oversight within each IC agency. IC agencies have offices of general counsel (OGC) to ensure that intelligence activities are conducted lawfully and offices of the inspector general (OIG) to independently carry out audit, investigation, and related functions to protect against fraud, waste, and abuse. Agencies may also have internal compliance offices to protect against non-compliance with the laws. Chief Privacy and Civil Liberties Officers are required at all intelligence agencies to ensure that privacy and civil liberties are considered and protected, including that agencies comply

with existing privacy statutes, regulations and guidelines. Many of these privacy officers also serve as their agencies chief transparency officers. Outside the IC, the Department of Justice plays a central role in reviewing and approving agency procedures under E.O. 12333 and conducting oversight of agencies that implement FISA authorities. Additionally, the Privacy and Civil Liberties Oversight Board (PCLOB) – an independent agency within the executive branch – also plays a key role in overseeing and advising on intelligence activities related to counterterrorism. Within the legislative branch, all U.S. intelligence activities are closely overseen by Congress. One way in which Congress conducts oversight is by authorizing (through the creation of new laws) and funding intelligence activities – or declining to authorize or fund them. Congressional oversight committees have secure facilities and professional staff. They receive frequent briefings and reports, and otherwise exercise oversight over our activities. Finally, the judicial branch, through the FISC, participates in oversight by authorizing intelligence activities as allowed by FISA and closely supervises the Government's implementation of those activities to ensure compliance with FISA. The independent FISC is composed of eleven federal district court judges who are designated by the Chief Justice of the United States and who are authorized to access classified information. The FISC is located in Washington D.C., in a secure facility and is supported by expert staff; since 2015, it also has individuals with security clearances who may be designated to serve as amici curiae. Many of its opinions are now public.