UNITED STATES RESPONSE TO OHCHR QUESTIONNAIRE ON "THE RIGHT TO PRIVACY IN THE DIGITAL AGE"

While recent unauthorized disclosures and other allegations of the United States' intelligence activities have garnered attention and influenced the debate on privacy in the digital age, the United States has long recognized that unchecked surveillance programs can be abused, and that privacy and civil liberties need to be integral considerations for all law enforcement and intelligence practices. It is also essential to acknowledge the necessary role that intelligence and law enforcement activities play in protecting our national security and the security of our partners and allies and furthering the investigation and prosecution of criminal activity. As technology has advanced, lawful and appropriate government access to certain electronic communications has become more – not less – important to furthering those objectives. We recognize that a rule of law framework with transparent laws and effective and meaningful oversight (which can take different forms) is essential to ensure that electronic surveillance authorities are not abused, such as by being undertaken for the purpose of suppressing criticism or dissent or disadvantaging people based on their ethnicity, race, gender, or religion. Efforts to increase transparency about electronic surveillance activities – without unduly constraining important law enforcement and intelligence activities – will help ensure respect for privacy and civil liberties.

The right to protection of the law from arbitrary or unlawful interference with privacy is enshrined in the International Covenant on Civil and Political Rights (ICCPR) and protected under the U.S. Constitution and U.S. laws. The OHCHR's survey and UN General Assembly Resolution 68/167 use the shorthand "right to privacy." Article 17 of the ICCPR states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy…" and that "[e]veryone has the right to the protection of the law against such interference…" We read the use of "right to privacy," or "privacy rights," to be describing what is laid out in Article 17 of the ICCPR, which is not an absolute right to privacy but rather is a right to protection against *unlawful* or *arbitrary* interferences with privacy. The United States understands this requirement to mean that, to be consistent with Article 17, an interference with privacy must be in accordance with transparent laws and must not be arbitrary. Some commentators have indicated that an interference under Article 17 has to be essential or necessary and be the least intrusive means to achieve a legitimate objective. Such a test goes beyond the text of Article 17, which only prohibits unlawful or arbitrary interferences, and is not supported by the travaux of the treaty. Because the ICCPR applies to governmental action, Article 17 applies to state actors, not to non-state actors. However, recognizing the impact that companies and other non-state actors can have on one's privacy, particularly in the digital age, we have included information about protections against non-state interferences with privacy in this response. The United States also notes its longstanding position that the

ICCPR only applies to individuals who are both within the territory of the State Party and within that State Party's jurisdiction in line with Article 2(1) of the ICCPR.

With this understanding of the parameters of Article 17, we will first discuss our framework regarding electronic methods of criminal investigation, then discuss protections in place with regards to electronic surveillance for intelligence purposes, and finally note policies and statutes that protect against non-state actor interference with privacy.

The United States notes that protection from unlawful or arbitrary interference with privacy is grounded in the Fourth Amendment of the U.S. Constitution and is also implemented by federal statutes. In addition, state and local laws and regulations provide myriad protections in this regard and states have rigorous processes in place to ensure that investigative activities are undertaken consistent with the Constitution.

The Fourth Amendment protects persons from unreasonable searches and seizures by the Government at both state and federal levels and protects the privacy of correspondence. The U.S. Supreme Court has defined search under the Fourth Amendment to be a government infringement of a person's reasonable expectation of privacy. Rakas v. Illinois, 439 U.S. 128, 240-49 (1978). A person's reasonable expectation of privacy is the linchpin of the Fourth Amendment. Where there exists a reasonable expectation of privacy, the Constitution generally does not permit government violation of that reasonable expectation without probable cause to believe that a crime is occurring or that evidence of crime will be found. Furthermore, except in limited, well-defined circumstances, officers must obtain a search warrant, which must be authorized by a neutral and detached magistrate, before they can conduct a search or seizure that impinges upon a reasonable expectation of privacy. When officers seek a warrant, the Fourth Amendment requires that they must make a showing of probable cause before a neutral and detached magistrate, not an agent or arm of the investigating authority.

With regard to governmental use of electronic methods of criminal investigation, there are a number of specific statutory protections in place to avoid arbitrary interference with privacy. At the federal level, the U.S. Congress as early as 1934 recognized that there could be substantial privacy infringement through use of electronic devices to track the movements of persons or things and to intercept private communications. Such devices now include wiretaps and datataps (accessing the content of voice or data communications in real time), pen registers, and trap and trace devices (which can, among other things, record telephone numbers called from a particular phone and the numbers of telephones from which calls are made to a particular phone, respectively), and surreptitiously installed microphones. Note that there is a difference in constitutional and statutory protections afforded to "content" that is collected using devices, such as wiretaps, as opposed to non-content that is collected using devices, such as pen registers.

In 1968 Congress enacted the Wiretap Act, which has been subsequently modified to accommodate technological advances, to regulate the use of electronic audio listening. 18 U.S.C. sections 2510-21 (Title III of the Omnibus Crime Control and Safe Streets Act of 1968-Wiretapping and Electronic Surveillance, Pub. L. No. 90-351, 82 Stat. 212). The Wiretap Act bans the use of certain electronic techniques by private citizens and requires government officials to obtain a court order before utilizing electronic techniques, such as wiretaps. Under the Wiretap Act, intercepting the content of communications is generally a two-step process. First, federal law enforcement must obtain internal approval to seek a court order authorizing interception from specified senior officials within the DOJ;[i] state and local law enforcement must obtain similar approval from senior state or local prosecuting officials.

Once they have obtained internal approval, federal agents must then apply for and obtain an order from a federal court to intercept wire, oral, or electronic communications unless there is an emergency involving immediate danger of death or serious bodily injury to any person or when conspiratorial activities threaten national security interests or are characteristic of organized crime. In such emergency situations, law enforcement must obtain the approval of high-level officials within the DOJ, or, for state and local governments, a high-level prosecutor, before beginning emergency interception. Furthermore, the government must obtain a court order authorizing and approving the emergency interception within 48 hours after interception occurs or begins to occur.

Generally an application for court approval of the interception of content using electronic means by law enforcement must set forth sufficient facts to satisfy the court that probable cause exists to believe that (i) certain identified persons have committed, are committing or will commit one of the specific serious felony offences covered by the statute; (ii) all or some of the persons have used, are using, or will use a targeted communication facility or premises in connection with the commission of the listed offence; and (iii) the targeted communication facility or premises has been used, is being used, or will be used in connection with the crime. The government's application must also satisfy the judge that other less intrusive investigative procedures have been tried without success, would not be likely to succeed, or would be too dangerous to use. The application must also include a complete statement of all other applications that have been made for wire and datataps involving the persons, facilities, or premises. The order is valid for no longer than 30 days but can be extended repeatedly. The court may require progress reports on the wire or data taps and the need to continue them. In addition, the judge issuing the order and the DOJ are required to make reports to the Administrative Office of U.S. Courts on each such wire or data trap and the number of arrests, suppression orders, and convictions that resulted. During the period of the order, the agents are under a continuing duty to minimize – that is, to not record or overhear conversations that are not related to the crimes or persons for which the order was obtained. The

recordings must also be sealed in a manner that will protect them from tampering. The government is expressly limited in the purposes for which, and to whom, it may disclose those communications.[ii]

Congress enacted the Electronic Communications Privacy Act (ECPA) in 1986 to address, among other matters, (i) access to stored wire and electronic communications and transactional records (the Wiretap Act applied to telephone calls) and (ii) the use of pen registers and trap and trace devices (See Titles II and III of ECPA, Pub. L. No. 99-508, 100 Stat. 1848). Title II of ECPA generally prohibits unauthorized access to or disclosure of stored wire and electronic communications, absent certain statutory exceptions. Title II of ECPA also provides for legal process that law enforcement must use to compel the production of such stored communications and transactional records. The pen register and trap and trace provisions of ECPA prohibit the installation or use of a pen register or trap or trace device, except as provided in the statute. Except in narrow, specified emergencies, law enforcement may not install a pen register or a trap and trace device without a prior court order.

After the September 2001 terrorist attacks, Congress passed the USA PATRIOT Act, which did several things that affected electronic methods. It updated federal anti-terrorism and criminal laws to bring them up to date with the modern technologies actually used by terrorists. It also provided terrorism investigators with important tools that were previously available in organized crime and drug trafficking investigations. For example, law enforcement had long used multi-point, or "roving," wiretaps to investigate non-terrorism crimes, such as drug offenses. Now, federal agents are allowed to use multi-point wiretaps, with court approval, to investigate sophisticated international terrorists who are trained to evade detection. This authority is directed to the problem of terrorists who seek to avoid investigation by frequently changing telephones, and allows investigators in certain specified circumstances to obtain from a federal court a wiretap order that relates to a specified person rather than a specific phone. This authority has been available in criminal investigations for years, but only became available in foreign intelligence investigations upon enactment of the USA PATRIOT Act. It allows the implementation to continue uninterrupted even though the terrorist changes phones. However, it is important to note that use of "roving" wiretaps are still subject to the approval requirements and demonstrating to the court the various factual prerequisites for obtaining a court order discussed above.

With regards to electronic surveillance for intelligence purposes, in furtherance of our core values, U.S. intelligence collection programs and activities are subject to stringent and multilayered oversight mechanisms. We note at the outset that we understand that, in the wake of the unauthorized disclosures and other allegations of U.S. intelligence surveillance activities, some have raised human rights concerns, including privacy concerns, in the United States and in other countries. It is a bedrock concept that U.S. intelligence collection activities are authorized pursuant to a rule of law framework. Such activities occur pursuant to the U.S. Constitution and, within that democratic

constitutional structure, a variety of statutes and other authorities, such as Executive Orders. It is essential to reiterate that all of the collection activities of U.S. intelligence agencies are carried out pursuant to a valid foreign intelligence or counterintelligence purpose; as a democratic nation, this is a requirement we take very seriously. Our intelligence priorities are set annually through an interagency process through which the leaders of our nation tell the intelligence community what information they need in the service of the nation, its citizens, and its interests. Further, the United States does not collect intelligence to suppress dissent, to provide a competitive advantage to U.S. companies or commercial sectors commercially, or to disadvantage any person on the basis of categories like ethnicity, race, gender, sexual orientation, or religious belief.

First, it is important to note that certain intelligence collection activities have long been overseen by the Foreign Intelligence Surveillance Court (FISC), as well as by Congress and oversight entities in the Executive Branch in order to ensure such activities meet applicable constitutional requirements and, accordingly, that privacy and civil liberties concerns are addressed. Intelligence collection overseas is also regulated and is carried out to meet foreign intelligence and counterintelligence objectives and not indiscriminately invade the privacy of foreign nationals. The 1978 Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801 et seq., regulates, among other things, electronic surveillance and physical searches as defined by the statute. Titles I and III FISA allow DOJ to obtain orders from the FISC if, *inter alia*, there is probable cause to believe that the target of the electronic surveillance or the physical search is a foreign power or an agent of a foreign power. 50 U.S.C. 1805 (a)(2)(A) and 1823(a)(3)(A). FISA also permits other types of surveillance activities, such as the installation and use of pen register and trap and trace devices. 50 U.S.C. 1842. FISA also permits the Attorney General to authorize the emergency employment of electronic surveillance and/or physical search if the Attorney General reasonably determines that an emergency situation exists, and he/she subsequently makes an application to the FISC within seven (7) days of the emergency authorization. 50 U.S.C. 1805(e) and 1824(e)(1). By law, FISA and chapters 119, 121, and 206 of title 18 (Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and titles II and III of ECPA) are the exclusive means by which electronic surveillance, as defined in that act, and the interception of domestic wire, and oral or electronic communications, may be conducted, 50 U.S.C. 1809.[iii]

As noted, the FISC plays an important role in overseeing certain government collection activities conducted pursuant to FISA. It not only authorizes these activities, but it also plays a continuing and active role in ensuring that they are carried out appropriately. Moreover, if at any time the government discovers that an authority or approval granted by the FISC has been implemented in a manner that did not comply with the Court's authorization or approval, or with applicable law, the government must immediately notify the FISC and appropriate corrective measures must be taken.[iv] The FISC consists of

11 independent federal judges who must ensure that these critical foreign intelligence surveillance activities are authorized consistent with the rule of law. This court uses an ex parte process similar to the one that the government has long followed in seeking permission from other federal courts in ordinary criminal investigations to engage in wiretapping, pen register, and trap and trace surveillance, or to conduct searches. This longstanding process has been codified for decades in statutes and has been upheld repeatedly by U.S. courts.

It is important to note that electronic surveillance initially authorized by the FISC may later be subject to an adversarial process. For example, should the government use information obtained from electronic surveillance authorized under FISA against a defendant in a criminal prosecution, and if the defendant was either the target of the electronic surveillance or a person whose communications or activities were subject to electronic surveillance, then the government generally must notify both the defendant and the court of that fact. The defendant can then challenge the legality of the surveillance. See 50 U.S.C. § 1806(c)-(h). In this context, numerous judicial decisions have upheld the legality of surveillances authorized by the FISC.

In addition to this legal framework under FISA and the FISC, the Office of the Director of National Intelligence (DNI) has a dedicated Civil Liberties Protection Officer who actively oversees intelligence programs. Independent agency Inspectors General also review intelligence operations. The National Security Agency (NSA), moreover, has an internal compliance officer, whose job includes developing processes that all NSA personnel must follow to ensure that NSA is complying with the law, and its own Civil Liberties Protection Officer. The U.S. intelligence community is required to report to Congress on its programs and activities, where there are vigorous debates on these issues.

As is now well known, the signals intelligence programs disclosed and declassified last year are conducted with the approval – and under the supervision – of the independent FISC. This fact notwithstanding, the Obama Administration undertook a broad-ranging and unprecedented review of U.S. signals intelligence programs in the latter half of 2013 and early 2014. The review process drew on input from key stakeholders, including the President's Review Group on Intelligence and Communications Technologies (established by the President in August 2013), Congress, the tech community, civil society, foreign partners, the Privacy and Civil Liberties Oversight Board, and others. The review examined how, in light of new and changing technologies, we can use our intelligence capabilities in a way that optimally protects our national security, while respecting privacy and civil liberties, maintaining the public trust, supporting our foreign policy, and reducing the risk of unauthorized disclosures. In January 2014, President Obama announced several reforms and issued a Presidential Policy Directive on signals intelligence activities.

To that end, the United States is undertaking a series of concrete and substantial reforms to increase transparency of our signals intelligence collection programs, and to implement additional protections for individuals' privacy regardless of nationality. As stated in Presidential Policy Directive 28, appropriate safeguards shall apply to personal information of all individuals, regardless of nationality, collected from signals intelligence activities. To that end, the President directed that the personal information of non-U.S. persons collected through signals intelligence shall be retained or disseminated only if the retention or dissemination of comparable information of U.S. persons would be permissible. Signals intelligence collected in bulk may only be used for a specified set of purposes, which the DNI has made public.

In January, 2014, the President announced that he was "ordering a transition" that will end the "bulk metadata program as it currently exists, and establish a new mechanism that preserves the capabilities we need without the government holding this bulk metadata."[v] The President announced two immediate changes to that program. First, under the program, the government "will only pursue phone calls that are two steps," rather than the previous three steps, removed from a selector (query term) associated with a terrorist organization. Second, during this transition period, queries can be made "only after a judicial finding or in case of a true emergency." The President also announced that he had instructed the Intelligence Community and the Attorney General to "develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this metadata itself" and to report to the President by March 28, 2014. On March 27, 2014, the President further announced that, having considered the options presented to him by the Intelligence Community and the Attorney General, he will seek legislation to replace the Section 215 bulk telephony-metadata program. Under that replacement approach announced by the President, telephone companies would retain the bulk telephony metadata for the length of time they independently do today, and the government would obtain query results from that data pursuant to individual orders from the FISC. The President also reiterated "the importance of maintaining the capabilities" of the Section 215 program, and announced that the government would seek reauthorization of the program (with the President's two changes in January) by the FISC because the necessary legislation for the change announced in March is not yet in place.

The United States has in place a number of other statutes that protect privacy interests regarding collection of information in other contexts. The Privacy Act incorporates all of the Fair Information Practice Principles (FIPPs) that have long been a cornerstone of international instruments relating to informational privacy, including but not limited to the Organization for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The Privacy Act requires federal agencies to provide public notice of its information

collections, including the purpose and intended uses of those collections, and prevents them from using or disclosing information collected for one purpose for an incompatible purpose, unless excepted by the Act. It also requires government agencies, subject to certain exemptions, to "maintain in [their] records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President." 5 U.S.C. 552a (e) (1). The Computer Matching and Privacy Protection Act of 1988 specifically addresses the use by federal agencies of computer data. The Act regulates the computer matching of federal data for federal benefits eligibility or recouping delinquent debts. The government may not take adverse action based on such computer checks without giving individuals an opportunity to respond.[vi]

In addition, there are other U.S. laws that govern aspects of privacy. The E-Government Act of 2002 requires federal government agencies to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available. The Homeland Security Act of 2002 requires the appointment of a Chief Privacy Officer at the Department of Homeland Security. The Implementing Recommendations of the 9/11 Commission Act of 2007 requires similar appointments at other federal agencies. Additional guidance to federal agencies concerning implementation of privacy regulation comes from the Office of Management and Budget (OMB).

The United States also has a variety of statutes and policies in place that protect individuals' privacy with respect to non-state actors.[vii] In 2012, the White House issued a blueprint for privacy in the information age to give consumers clear guidance on what they should expect from those who handle their personal information, and set expectations for companies that use personal data.[viii] The Privacy Blueprint contains four key elements: 1) a Consumer Privacy Bill of Rights based on the FIPPs; 2) a call for government-convened multistakeholder processes to apply the FIPPs to particular business contexts; 3) support for effective enforcement by the Federal Trade Commission (FTC) and State Attorneys General; and 4) a commitment to the international interoperability of commercial privacy regimes.

The Blueprint recognizes that the existing consumer data privacy framework in the United States is flexible and effectively addresses many consumer data privacy challenges in the digital age. This framework consists of sectoral federal privacy laws, state laws that enhance the federal regime, industry best practices, vigorous enforcement by the FTC, executive agencies, and state prosecutors, and a network of chief privacy officers and other privacy professionals who develop privacy practices that adapt to changes in technology and business models and create a growing culture of privacy awareness within companies. However, federal data privacy statutes apply only to particular types of data (such as electronic communications) or specific sectors, such as healthcare, education, communications, and financial services or, in the case of online data collection, children. Because some personal data collected from individuals is not subject to comprehensive federal statutory protection, the Administration set forth

the Consumer Privacy Bill of Rights to promote more consistent responses to privacy concerns across the wide range of environments in which individuals have access to networked technologies and in which a broad array of companies collect and use personal data. The Consumer Privacy Bill of Rights states clear baseline protections for consumers, providing for: 1) individual control; 2) transparency; 3) respect for context; 4) security; 5) access and accuracy; 6) focused collection; and 7) accountability. The document is based on the time-honored FIPPs, but applies the principles to the interactive and highly networked world we live in today, adapting them to the dynamic environment of the commercial Internet. The White House called for stakeholders from industry, civil society, and the technical community to apply the Consumer Privacy Bill of Rights to specific business contexts through voluntary, enforceable codes of conduct.[ix] Such practices and frameworks have played a crucial role in advancing consumers' interests, particularly when they include robust accountability mechanisms and are subject to FTC enforcement.

---

[i] The Wiretap Act requires approval from senior DOJ officials with regard to oral communications (e.g. statements intercepted by a hidden microphone or recording device) and wire communications (e.g. telephone conversations captured via a wiretap). It imposes a slightly lower standard – requiring only prior approval from a prosecutor as opposed to a senior official – with regard to electronic communications, which by statutory definition do not include any transmission of the human voice and include, among other things, email communications. However, the federal government has adopted a higher bar to obtaining interceptions of electronic communications and requires federal law enforcement to obtain the same type of authorization to apply for a court order from senior DOJ officials regardless of the type of communications that law enforcement seeks to intercept.

[ii] Section 223 of the USA PATRIOT Act provided for civil liability for unauthorized disclosures and provided that a person aggrieved by certain willful violation may commence an action for money damages against the United States. It also provides for the initiation of administrative proceedings.

[iii] The Protect America Act (PAA) was signed into law August 5, 2007. It carved out of the FISA definition of electronic surveillance directed at a person reasonably believed to be located outside the United States. (Sec. 105A) The PAA authorized the Attorney General (AG) and the Director of National Intelligence (DNI) to jointly authorize, for periods of up to one year, the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the AG and DNI determined that (a) there were reasonable (targeting) procedures in place for determining that the acquisition of foreign intelligence information concerned persons reasonably believed to be located outside the United States; (b) the acquisition did not constitute electronic surveillance as defined by FISA; (c) the acquisition involved obtaining foreign intelligence information from or with the assistance of a Communications Service provider who had access to communications as they were transmitted or stored; (d) a significant purpose of acquisition was to obtain foreign intelligence information; and (e) minimization procedures to be used for the collection met FISA definitions of minimization procedures. (Sec. 105B(1) – (5)). Following a 15 day extension, the PAA expired on February 16, 2008. Subsequently, in July 2008, the FISA Amendments Act (FAA) was signed into law. FAA Section 702 generally provides that upon the issuance of an order by the FISC approving a certification and the use of targeting and minimization procedures for an acquisition, the Attorney General and the Director of National Intelligence may jointly authorize for up to one year from the date of the authorization, the targeting of non U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. That said, acquisitions under FAA Section 702 may not: (a) intentionally target a person known at time of acquisition to be located in the United States (FISA

must be used for such acquisitions based upon a showing of probable cause and specific authorization from the FISC); (b) intentionally target a person reasonably believed to be located outside the U.S. if the purpose of the acquisition is to target a particular known person reasonably believed to be in the U.S.; (c) intentionally target a United States person reasonably believed to be located outside the United States; (d) intentionally acquire communications in which the sender and all intended recipients are located within the United States; and (e) the acquisition must be conducted in conformity with Fourth Amendment to the U.S. Constitution.

[iv] The Executive has reported several significant compliance problems encountered by certain programs, such as those uncovered in 2009, to the Intelligence and the Judiciary Committees in both houses of Congress. In 2009, the committees received the FISA court documents and the government submissions to the court related to those compliance problems. Those documents have since been declassified and released by the DNI to give the public a better understanding of how the government and the FISC respond to compliance problems once they are identified. Of course, no compliance incident is a good thing. However, what the recently declassified documents reveal is an oversight process that works. The government brought compliance issues to the Court's attention; the Court ordered certain responses; and the government responded accordingly. This is precisely how oversight should operate.

[v] This program is known as the "Section 215 program" because the Foreign Intelligence Surveillance Court authorizes it under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted as section 215 of the USA PATRIOT Act.

[vi] Another statute that protects privacy and could impact personal data collected digitally is the Right to Financial Privacy Act, which sets procedures regarding when federal agencies may review customers' bank records. 12 U.S.C. 3401-22.

[vii] For example, Title II of ECPA generally prohibits unauthorized access by private parties to wire and electronic communications while in transit and when stored. The Fair Credit Reporting Act, 15 U.S.C. 1681-81 (v), regulates the distribution and use of credit information by credit agencies. The Video Privacy Protection Act, 18 U.S.C. 2710, protects the disclosure and sale of customer records regarding video rentals. Title V of the Gramm-Leach-Bliley Act, 113 Stat. 1338, addresses the protection and disclosure of nonpublic customer information by financial institutions. The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, protects the privacy of students' educational records. The Rehabilitation Act of 1973 and the Americans with Disabilities Act provide for confidentiality of medical information submitted to employers by employees relating to their disabilities, as well as restrictions on the types of medical information that can be requested by employers. The Equal Employment Opportunity Commission (EEOC) has issued extensive guidance on these provisions at 29 C.F.R. 1630 and in advisory opinions and guidance available at http://www.eeoc.gov. In addition, the Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d-1320d-8, provides for protections regarding the privacy of individually identifiable health information

[viii] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[ix] Stakeholder groups have made progress in this effort, with groups convened by the Department of Commerce drafting a code of conduct for privacy disclosures on mobile applications and working to improve privacy protections related to facial recognition technology. http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency and http://www.ntia.doc.gov/blog/2014/ntia-convene-first-facial-recognition-technology-multistakeholder-meeting.