UNITED STATES OF AMERICA

Joint Submission to the United Nations
Twenty-Second Session of the Universal Periodic Review Working Group
Human Rights Council
May 2015

Secret Surveillance:
Five Large-Scale Global Programs

Submitted by:

American Civil Liberties Union

Center for Democracy & Technology

The American Civil Liberties Union is the United States' guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in the country.

The Center for Democracy & Technology is a champion of global online civil liberties and human rights, driving policy outcomes that keep the Internet open, innovative and free.

Contact: Sarah St.Vincent
sstvincent@cdt.org
+1 202 407 8835

Joseph L. Hall
jhall@cdt.org
+1 202 407 8825

Steven Watt
swatt@aclu.org
+1 212 519 7870

I. Introduction and Executive Summary

1. The Center for Democracy & Technology and the American Civil Liberties Union are pleased to make this submission to the Human Rights Council in preparation for the 2015 Universal Periodic Review ("UPR") of the United States of America. With an awareness that the UPR will encompass the US' compliance with all of its human rights obligations, we write to draw attention to several specific US secret surveillance programs that have been disclosed since the most recent UPR of the United States in 2010. These programs are conducted by US intelligence agencies, primarily the National Security Agency ("NSA").

2. Our submission explains the legal basis, methods of operation, and human rights consequences of five programs (which are commonly known by their code names):
    - **DISHFIRE**, an initiative through which the US collects hundreds of millions of private text messages worldwide every day;
    - **CO-TRAVELER**, through which the US captures billions of location updates daily from mobile phones around the world;
    - **MUSCULAR**, which entails the US' interception of *all* data transmitted between certain data centers operated by Yahoo! and Google outside of US territory;
    - **MYSTIC**, a US program that collects *all* telephone call details in five sovereign countries other than the US, as well as the full content of *all* phone calls in two of those countries; and
    - **QUANTUM**, a US program that listens in real-time to traffic on the Internet's most fundamental infrastructure and can respond based on certain triggering information with active attacks, including the delivery of malicious software to the end-user's device.

3. Our human rights concerns in the context of the US' surveillance extend beyond these five programs; however, we believe these programs merit special attention from the Human Rights Council, as their implications for human rights are particularly grave. We have sought to use our technological expertise to help ensure that the Council and all stakeholders enjoy a complete understanding of these highly complex programs and their enormous detrimental impact on privacy and related rights.

4. At the outset, we wish to make the practical consequences of these five programs clear: **on a daily basis, US authorities are intercepting the private communications and other personal electronic data of hundreds of millions of people across the globe, the vast majority of whom are not suspected of any wrongdoing. The intercepted data includes information about where those hundreds of millions of people are, with whom they correspond, and what they say in their correspondence.** In the aggregate, the data allow the agencies to create a detailed picture of an individual's personal life, even where that individual has no connection with any criminal investigation.

5. It is our view that the five programs are grossly inconsistent with the obligation to refrain from interfering arbitrarily with individuals' **privacy and correspondence**, as provided in Article 12 of the Universal Declaration of Human Rights ("UDHR") and Article 17 of the International Covenant on Civil and Political Rights ("ICCPR").

6. We are also gravely concerned about the negative implications of these programs for the **right to freedom of expression**, as guaranteed in Article 19 of the UDHR and Article 19 of the ICCPR, as well as the **right of peaceful assembly**, established at Article 20 of the UDHR and Article 21 of the ICCPR.

7. Further, as noted below, the sheer scale of these programs, combined with the general lack of redress for violations of the human rights they implicate, seriously undermines the **right to an effective remedy** provided in Article 8 of the UDHR and Article 2(3) of the ICCPR.

8. It is our position that the US is obligated to protect each of these rights not only within its own territory, but also extraterritorially to the extent set out in the Office of the High Commissioner for Human Rights' June 2014 report on the right to privacy in the digital age and the April 2014 concluding observations of the UN Human Rights Committee on the United States' compliance with its obligations under the ICCPR.[1]

9. Finally, insofar as they involve activities that take place in or directly touch upon other states' territories without the consent of those states, and impede the ability of those other states to ensure respect for human rights within their own jurisdictions, we believe these programs may also be inconsistent with Articles 2(1) and 2(4) of the Charter of the United Nations, and may defeat the object and purpose of the UDHR as well as other human rights instruments.

10. We observe that during the previous UPR of the United States in 2010, several states urged the US to make its anti-terrorism legislation fully consistent with human rights and, in particular, to protect the privacy of electronic communications.[2] Mexico, for example, encouraged the United States to "[r]espond [to] and follow up appropriately [on]" the recommendations made by the UN Special Rapporteur for the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism.[3] In a 2007 report on a mission to the United States, the Special Rapporteur had raised concerns about the inadequate (or unknown) human rights protections provided by the legal regimes that then governed US secret surveillance programs, and maintained that "the use of surveillance techniques without a warrant" violated the privacy rights guaranteed in Article 17 of the ICCPR.[4]

11. At the conclusion of the 2010 UPR process, the United States declared that Mexico's recommendation enjoyed the US' support.[5] In response to a recommendation by the Russian Federation in a related context, the US reassured the Human Rights Council that the country's domestic law "prohibit[s] the use of modern technology for excessive and unjustified interference in individuals' private lives."[6]

12. Regrettably, the disclosures concerning US secret surveillance activities that have appeared in the media since June 2013 indicate that the US has continued to violate privacy and related rights of individuals in the United States and around the world with impunity.

---

[1] Office of the U.N. High Comm'r for Hum. Rts., *The right to privacy in the digital age*, ¶¶ 31-34, U.N. Doc. A/HRC/27/37 (June 30, 2014) (hereinafter "OHCHR Report"); U.N. Hum. Rts. Comm., *Concluding observations on the fourth periodic report of the United States of America*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014).
[2] U.N. Hum. Rts. Council, *Report of the Working Group on the Universal Periodic Review: United States of America*, ¶¶ 92.58, 92.59, 92.90, 92.187, 92.188, A/HRC/16/11 (Jan. 4, 2011).
[3] *Ibid.* at ¶ 92.90.
[4] U.N. Hum. Rts. Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Mission to the United States of America*, ¶ 50, A/HRC/6/17/Add.3 (Nov. 22, 2007) (*prepared by* Martin Scheinin).
[5] U.N. Hum. Rts. Council, *Report of the Working Group on the Universal Periodic Review: United States of America*: Views on conclusions and/or recommendations, voluntary commitments and replies presented by the State under review, ¶ 13, A/HRC/16/11/Add.1 (Mar. 8, 2011).
[6] *Ibid.*

13. In April 2014, while reviewing the US' compliance with its obligations under the ICCPR, the UN Human Rights Committee made recommendations concerning the country's secret surveillance programs. In particular, the Committee urged the US to ensure that any interference with the right to privacy occurring as a result of these programs is authorized by laws that are publicly accessible and protect against abuse; the Committee also affirmed that the US should "ensure that its surveillance activities, *both within and outside the United States*, conform to its obligations under the [ICCPR], including article 17" (emphasis added).[7]

14. Unfortunately, as of the date of this submission, efforts by the US government to implement the Committee's recommendations have been inadequate, including where the five global surveillance programs discussed below are concerned.

II. Domestic Legal Framework

a. Powers of the executive and legislative branches concerning the authorization and regulation of intelligence-gathering

15. In the United States, the government's treatment of individuals within the country's borders (and some individuals outside of US territory) is governed at the broadest level by the Constitution, which includes a number of amendments guaranteeing fundamental rights. In the surveillance context, the most relevant of these amendments is the Fourth, which establishes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[8]

16. Where the treatment of foreigners abroad is concerned, the Constitution allocates certain powers between the legislative and executive branches. Although the precise division is a matter of controversy, as a general matter, the executive branch asserts significant authority over foreign affairs and policies directed at non-US persons abroad.[9]

17. Notwithstanding these claims, Congress has regulated the executive's conduct of foreign affairs in some circumstances. For example, Congress has regulated the executive's collection of foreign intelligence in some circumstances, even when that collection has taken place on foreign soil.[10] Congress may be similarly empowered to regulate surveillance that contravenes the ICCPR.

b. Non-statutory basis of the five surveillance programs

18. Prior to their disclosure in the media in 2013 and 2014, the five surveillance programs discussed in this submission were completely clandestine. This means that the precise legal basis the US intelligence community views as authorizing these programs (or their successors) remains unknown; to date, no relevant legal opinions by the intelligence agencies have been disclosed to the public. However, many advocates believe that the intelligence authorities conduct (or

[7] U.N. Hum. Rts. Comm., *Concluding observations on the fourth periodic report of the United States of America*, *supra* n. 1.
[8] U.S. CONST. amend. IV.
[9] In the context of this submission, the term "US person" means a US national or permanent resident; see 50 U.S.C. § 1801(i).
[10] *See, e.g.*, 50 U.S.C. § 1881c ("Other acquisitions targeting United States persons outside the United States").

conducted) the programs pursuant to a document known as **Executive Order 12333** ("EO 12333").[11]

19. EO 12333 is a presidential order issued in 1981.[12] It was not subject to legislative approval, and although it reaffirms the applicability of domestic laws concerning congressional oversight of the intelligence agencies, the extent to which the order's actual implementation is subject to meaningful legislative oversight remains unclear.[13] The chair of the US Senate Select Committee on Intelligence has indicated that Congress is not in fact currently overseeing programs conducted under EO 12333.[14]

20. EO 12333 authorizes the US intelligence agencies to collect, retain, and disseminate any "[i]nformation constituting foreign intelligence or counterintelligence." The order defines the term "foreign intelligence" very broadly: such intelligence includes any "information relating to the capabilities, intentions and activities of foreign powers, organizations *or persons*" (emphasis added).

21. The order directs that the authorities "shall use the least intrusive collection techniques feasible within the United States or directed against" US persons abroad.[15] However, the order does not afford the same level of protection to non-US persons, and the key regulations that implement the order where surveillance abroad is concerned, US Signal Intelligence Directive SP0018 and Defense Department regulation 5240.1-R, do not afford such protections either.[16] Additionally, EO 12333 permits the intelligence authorities to collect, retain, and disseminate the communications and other information of US persons as long as this information was "obtained in the course of" a lawful investigation. The intelligence community refers to this practice as "incidental" collection; despite the use of this term, however, the collection of US persons' communications as part of the programs discussed in this submission is reportedly very widespread.[17]

---

[11] *See, e.g.*, American Civil Liberties Union, *The Most Important Surveillance Order We Know Almost Nothing About*, Dec. 30, 2013, https://www.aclu.org/blog/national-security/most-important-surveillance-order-we-know-almost-nothing-about (last accessed Sept. 13, 2014).

[12] Exec. Order No. 12,333, 3 C.F.R. 200 (1981) (as amended).

[13] *See* John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans*, WASH. POST, July 18, 2014, *available at* http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html (last accessed Sept. 9, 2014).

[14] Ali Watkins, *Most of NSA's data collection authorized by order Ronald Reagan issued*, MCCLATCHY DC, http://www.mcclatchydc.com/2013/11/21/209167_most-of-nsas-data-collection-authorized.html?rh=1 (last accessed Sept. 13, 2014).

[15] *See supra* n. 9 for the definition of "US person."

[16] DEPARTMENT OF DEFENSE, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (DOD 5240.1-R) (1982), *available at* http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf (last accessed Sept. 13, 2014); National Security Agency/Central Security Service, United States Signals Intelligence Directive SP0018: Legal Compliance and U.S. Persons Minimization Procedures (2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf (last accessed Sept. 13, 2014).

[17] *See, e.g., ibid.*

c. Scope of fundamental-rights protections for non-US persons (and US persons abroad) under domestic law and policy

22. Pursuant to US domestic law, US persons abroad enjoy the Constitution's fundamental protections from US government abuses, and can enforce these protections in US federal courts.[18] However, the government has interpreted Supreme Court precedent as precluding non-US nationals outside of the United States from asserting constitutional rights, except in limited circumstances.[19] This asserted lack of constitutional protections, among other domestic legal factors, renders it extremely difficult for any non-US person outside of the US to bring a claim in a US court against the government (or its officials) for a violation that occurred outside of the United States, or for fundamental-rights violations arising from secret surveillance programs.

23. Operating in this apparent legal void, the executive branch has issued a policy document that provides guidance to the intelligence authorities but does not have any binding effect and is not enforceable in US courts. The document is known as **Presidential Policy Directive 28** ("PPD-28").[20] It includes a supplementary annex that remains classified.

24. Without assuming any binding legal obligations, PPD-28 expresses a view that "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside," and that "all persons have legitimate privacy interests in the handling of their personal information."

25. As a basis for the US' bulk (i.e., indiscriminate) collection of private communications, PPD-28 asserts the protection of US national security interests. In respect of this bulk collection, PPD-28 states that the US authorities shall use the intercepted data "only for the purposes of detecting and countering (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats…"

26. Notwithstanding these restrictions on the *use* of intercepted data, the declassified portion of PPD-28 does not impose any restrictions on the *collection* of that data.

27. Pursuant to PPD-28, the US may retain an item of intercepted data for up to five years, or for a longer period if the Director of National Intelligence determines that continued retention is "in the national security interests of the United States."

28. As a policy, PPD-28 applies to each of the programs described below. However, to the extent that the directive contains limitations on the conduct of the programs, these limitations do not impose any enforceable legal obligations upon any US entity.

[18] Reid v. Covert, 354 U.S. 1 (1955).
[19] *See, e.g.*, Brief for the Respondents, Boumediene v. Bush and Al-Odah v. U.S., 553 U.S. 723 (2008) (Nos. 06-1195 and 06-1196).
[20] Presidential Policy Directive/PPD-28 (2014), *available at* http://fas.org/irp/offdocs/ppd/ppd-28.pdf (last accessed Sept. 9, 2014).

III. Programs that Include Indiscriminate Collection of, or Other Interference with, Private Electronic Data

A. DISHFIRE

29. Revealed in January 2013 by two British media outlets, DISHFIRE is a massive US-controlled database of text messages.[21] While it remains unclear exactly how the US collects this information, the relevant disclosures suggest that the intelligence authorities are able to capture hundreds of millions of text messages *per day*. The US subsequently mines these messages for personal data including location information, contacts, travel activity, and financial transactions (including credit card numbers); it also engages in what is known as "contact chaining," i.e., the creation of a map of an individual's social network through the examination of his or her patterns of communication. In other words, the United States secretly collects private text messages and uses certain basic data contained in them to build a picture of individuals' private and professional lives without their knowledge or consent.

30. The US' collection of this private personal data is not based on any individualized suspicion or targeting, nor is the collection itself subject to any judicial oversight.

31. *The Guardian* has reported that documents it has reviewed show that the US selectively purges communications related to US telephone numbers from the database. However, there are no indications that the US plans to stop collecting any of these data, or purge any communications related to non-US telephone numbers.

B. CO-TRAVELER

32. The CO-TRAVELER program is similar to DISHFIRE in that it entails the US' indiscriminate interception of personal data. CO-TRAVELER, however, focuses on mobile phone location information with the goal of being able to discover previously unknown associates of persons of interest. In collaboration with an unknown industry partner, the US intelligence authorities collect billions of location updates from hundreds of millions of devices *each day*.[22]

33. Mobile phones regularly send "registration" messages to nearby cellular towers so that the carrier can route phone calls efficiently to the phone. In addition, when a mobile-phone user crosses national boundaries, a roaming message is often sent that informs the user of the current rates for using data and voice in the new country.

34. By collecting and combining registration updates and roaming messages, the US intelligence authorities can map, with reasonable precision, the whereabouts of any mobile-phone user in the world. To discover a target's associates, the authorities can analyze over time how many other mobile phones remain physically close to that targeted device.

---

[21] James Ball, *NSA collects millions of text messages daily in 'untargeted' global sweep*, GUARDIAN, Jan. 16, 2014, *available at* http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (last accessed Sept. 9, 2014).

[22] Barton Gellman and Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, WASH. POST, Dec. 4, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (last accessed Sept. 9, 2014).

35. As under DISHFIRE, the US "incidentally" intercepts and retains US persons' location data as part of CO-TRAVELER, although it does not deliberately target US persons. Meanwhile, the lack of limits on the interception, retention, use, or dissemination of location data concerning non-US persons mirrors the lack of limits under DISHFIRE.

C. MUSCULAR

36. In October 2013, *The Washington Post* reported that through a program code-named MUSCULAR, the US intelligence authorities have been collecting all of the data traffic that flows between certain data centers operated by Yahoo! and Google outside of US territory.[23] Both Yahoo! and Google maintain such data centers in order to keep data closer to the end-user, a practice that improves the speed and responsiveness of the companies' communications services. The various data centers owned by the companies regularly exchange data in order to distribute those data more efficiently, create back-up records, and deliver the companies' services.

37. The networks that connect these data centers employ fiber-optic data cables that the companies own or lease, and that are not directly connected to the public Internet. The US intelligence authorities have reportedly tapped into these private networks in order to get access to the raw, unencrypted bulk transfers of data between the data centers. The amount of private data collected in this fashion can be extremely large: for example, if a Yahoo! e-mail user relocates, and Yahoo! decides that it would be more efficient for that user's data to be stored and processed in a different data center, it is possible that the US intelligence authorities could intercept the entire contents of that user's email history.

38. Since the existence of the MUSCULAR program was revealed, both Yahoo! and Google have begun to encrypt the traffic between their data centers. However, the amount of private communications data that the US intelligence authorities may have intercepted pursuant to the program remains both unknown and potentially vast, possibly affecting hundreds of millions of users worldwide.

D. MYSTIC

39. In March 2014, *The Washington Post* described a secret surveillance program called MYSTIC, through which the US collects telephone calling details from five countries—later revealed by *The Intercept* to be the Bahamas, Mexico, Kenya, the Philippines, and one undisclosed country.[24] Through MYSTIC, the US indiscriminately collects comprehensive calling details for all calls in these five countries. This information includes, at minimum, the date and time when a call was placed, the telephone numbers of the caller and recipient.

---

[23]Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASH. POST, Oct. 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (last accessed Sept. 9, 2014).

[24] Barton Gellman and Ashkan Soltani, *NSA surveillance program reaches 'into the past' to retrieve, replay phone calls*, WASH. POST, Mar. 18, 2014, *available at* http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (last accessed Sept. 12, 2014); Ryan Devereaux et al., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, INTERCEPT, May 19, 2014, *available at* https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (last accessed Sept. 12, 2014).

40. For the Bahamas and the undisclosed country, the US is recording (or has recorded) **the full audio content of every single mobile telephone call placed to, from, or within these countries**.[25]

41. *The Intercept* estimates that this program collects call details and full conversation content from 250 million people across these five countries, encompassing nearly 100 million calls every day.

E. QUANTUM

42. In October 2013, *The Guardian* reported that the US intelligence authorities, under a program code-named QUANTUM, have the ability to "shoot" any Internet user in real-time, essentially targeting the delivery of malicious software to the individual as his or her traffic passes by on the Internet.[26]

43. To conduct this program, the US intelligence authorities install equipment on the Internet backbones, i.e., the infrastructure that makes Internet activity possible. This equipment can monitor Internet traffic and make exceedingly quick, automated decisions about possible "triggers" seen in the data passing by. If the system sees a target (or "selector") of interest, it can respond quickly and mount malicious attacks against the user. These attacks range from active "man-in-the-middle" attacks—where the system does just enough to eavesdrop on encrypted traffic—to the delivery of malware, which can compromise the user's computing device and establish a presence on that device. Once it has established such a presence inside the device, the US can deliver additional malicious software, such as key-logger tools (which record every key typed on a device, including sensitive information such as passwords).[27]

44. QUANTUM is often used to defeat certain anonymity tools such as Tor, which facilitates Internet activity that cannot be traced to a particular user. Anonymity tools are used by a wide variety of human rights activists for whom privacy, freedom of expression, and freedom of assembly are critical. This means that the invasiveness of QUANTUM has especially grave implications for the human rights addressed in this submission.

45. QUANTUM, like each of the other programs described above, does not appear to be subject to any form of judicial oversight.

IV. Failure of These Programs to Comply with Human Rights Obligations

46. Regardless of the extent to which the US may be legally bound under the relevant human rights treaties to respect the fundamental rights of individuals within or outside of its territory and jurisdiction, we believe that the five surveillance programs described above are grossly inconsistent with the **right to freedom from arbitrary or unlawful interference in privacy and**

---

[25] Devereaux et al., *supra* n. 24.

[26] James Ball et al., *NSA and GCHQ target Tor network that protects anonymity of web users*, GUARDIAN, Oct. 4, 2013, *available at* http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (last accessed Sept. 9, 2014); Nicholas Weaver, *Our Government Has Weaponized the Internet. Here's How They Did It*, WIRED, Nov. 13, 2013, *available at* http://www.wired.com/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon/ (last accessed Sept. 9, 2014).

[27] Bruce Schneier, *Attacking Tor: how the NSA targets users' online anonymity*, GUARDIAN, Oct. 4, 2013, *available at* http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (last accessed Sept. 11, 2014).

correspondence, as established in Article of the 12 UDHR and Article of the 17 ICCPR. This serious inconsistency arises from a combination of the following factors:

- The programs are not authorized by clear, specific, and publicly-accessible statutory laws or case-law, and instead are authorized by an imprecisely-worded executive order that confers virtually unfettered discretion on intelligence decision-makers and was not subject to legislative approval (as human rights law requires);[28]
- Members of the public, both within and outside the US, are not realistically able to foresee the circumstances under which the US may intercept their communications;[29]
- Individuals' private communications are intercepted on a large scale without suspicion or grounds for believing that the communications will be relevant to a legitimate investigation (criminal or otherwise);[30]
- There is a lack of judicial or other independent authorization of the monitoring of individuals' communications;[31]
- There is an additional lack of judicial oversight (or other supervision that is independent of the entities executing the surveillance) over the implementation of these five surveillance programs as a whole;[32]
- The duration of the surveillance itself lacks firm and effective limits;[33]
- The US' retention of the intercepted data similarly lacks firm and effective limits;[34]
- The programs treat metadata (i.e., data about the sender, recipient, time, duration, etc. of the communications) as subject to few or no legal protections;[35] and
- There is a substantial likelihood that the US' interception of the overwhelming majority of the communications data collected through these five programs is not necessary to address compelling interests such as an imminent threat to national security or public order.[36]

47. In this respect, we recall in particular the determination of the European Court of Human Rights, as well as the finding of the UN High Commissioner for Human Rights, that even the mere interception of communications data constitutes an interference with the right to privacy that must

[28] *Cf.* U.N. Hum. Rts. Comm., *CCPR General Comment No. 16: Article 17 (Right to Privacy)*, ¶¶ 2-3, U.N. Doc. HRI/GEN/1/Rev.1 (Sept. 20, 1988) (hereinafter "General Comment 16"); OHCHR Report, *supra* n. 1, ¶¶ 23, 29; Malone v. United Kingdom, App. No. 8691/79, Judgment, 82 Eur. Ct. H.R. 10 (1984), ¶¶ 67, 87; Ass'n for Eur. Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, Judgment, 2007 Eur. Ct. H.R. 533 (2007), ¶ 76; Donoso v. Panama, Judgment, Inter-Am. Ct. H. R. (ser. C), No. 193 (2009), ¶ 56; Escher v. Colombia, Judgment, Inter-Am. Ct. H. R. (ser. C), No. 200 (2009), ¶¶ 130-131.

[29] *Cf.* OHCHR Report, *supra* n. 1, ¶¶ 23, 28; Liberty v. United Kingdom, App. No. 58243/00, Judgment, 2008 Eur. Ct. H.R. 568 (2008), ¶ 59; Malone v. United Kingdom, *supra* n. 28, ¶ 67; Leander v. Sweden, App. No. 9248/81, Judgment, 116 Eur. Ct. H.R. 4 (1987), ¶ 51.

[30] *Cf.* General Comment 16, *supra* n. 28, ¶ 8; Klass v. Germany, App. No. 5029/71, Judgment, 28 Eur. Ct. H.R. 4 (1978), ¶ 51.

[31] *Cf.* OHCHR Report, *supra* n. 1, ¶¶ 37-38; Klass v. Germany, *supra* n. 30, ¶ 56; Rotaru v. Romania, App. No. 28341/95, Judgment, 2000-V Eur. Ct. H.R. 192 (2000), ¶ 59.

[32] *Cf.* OHCHR Report, *supra* n. 1, ¶¶ 37-38; Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* n. 28, ¶¶ 85-87 (2007); Iordachi v. Moldova, App. No. 25198/02, 2009 Eur. Ct. H. R. 256 (2009), ¶ 49.

[33] *Cf.* Klass v. Germany, *supra* n. 30, ¶ 52; Weber and Saravia v. Germany, App. No. 54934/00, Decision (Admissibility), 2006-XI Eur. Ct. H.R. 1173 (2006), ¶ 98; Iordachi v. Moldova, *supra* n. 32, ¶ 45.

[34] *Cf.* Klass v. Germany, *supra* n. 30, ¶ 52; Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* n. 28, ¶ 86.

[35] *Cf.* OHCHR Report, *supra* n. 1, ¶ 19; Escher v. Colombia, *supra* note 28, ¶ 114; Digital Rights Ireland (Judgment), 2014 EUECJ C-293/12 (2014), ¶¶ 26-28.

[36] *Cf.* OHCHR Report, *supra* n. 1, ¶¶ 23-25; Rotaru v. Romania, *supra* n. 31, ¶ 47.

be justified in order to be lawful.[37] These findings suggest that the US is violating the privacy rights of hundreds of millions of individuals—both within and outside the US—by collecting their communications data without justification or consent.

48. We also believe these five programs have serious negative implications for the **right to freedom of expression**, as guaranteed in Article 19 of the UDHR and Article 19 of the ICCPR. We recall that secret surveillance programs may have a particular chilling effect upon journalists, lawyers, political dissidents, and non-governmental organizations whose work is essential to ensuring the transparency and proper functioning of democratic institutions.[38] The chilling effect of such pervasive surveillance upon the freedom of expression of other individuals is of equally grave concern. The QUANTUM program is especially troubling in this respect.

49. We are further concerned about the chilling effect that these programs may have upon the **right of peaceful assembly** provided in Article 20 of the UDHR and Article 21 of the ICCPR. Again, we are particularly troubled by the implications of the QUANTUM program for the exercise of this right, as attacks on individuals' communications devices may impair the ability of political dissidents and others to exercise their right to conduct peaceful meetings or demonstrations.

50. Due to the lack of meaningful protections for both US persons and non-US persons in the secret surveillance context under the domestic legal regime described above, we have additional and extremely serious concerns about the lack of an accessible and enforceable **right to a remedy** (as established in Article 8 of the UDHR and Article 2(3) of the ICCPR) in respect of these five programs. While some limitations on the right to a remedy may be required where violations arise from secret surveillance programs, the US should nevertheless ensure that an effective remedy is available.[39]

51. Finally, we believe that to the extent that these five programs impede the ability of other states to ensure respect for human rights within their own jurisdictions, they are inconsistent with the objects and purposes of the UDHR and may also be inconsistent with Articles 2(1) and 2(4) of the Charter of the United Nations. These articles of the Charter enshrine the principles of the sovereign equality and territorial sovereignty of all states.

V. Recommendations

- **The United States should immediately discontinue all indiscriminate interception, retention, use, and dissemination of individuals' private communications content and metadata both within and outside US territory and jurisdiction.**

- **The United States should also immediately discontinue any attacks of the kind that are, or have been, carried out under the QUANTUM program, except where such attacks are necessary and non-arbitrary in relation to a specific known threat, or where otherwise permitted by international human rights law.**

---

[37] OHCHR Report, *supra* n. 1, ¶ 20; *e.g.*, Weber and Saravia v. Germany, *supra* n. 33, ¶ 79.
[38] *See, e.g.*, Weber and Saravia v. Germany, *supra* n. 33, ¶¶ 143-146; Youth Initiative for Human Rights v. Serbia, App. No. 48135/06, Judgment, 2013 Eur. Ct. H. R. 584 (2013), ¶¶ 6, 22-26; HUMAN RIGHTS WATCH AND AMERICAN CIVIL LIBERTIES UNION, WITH LIBERTY TO MONITOR ALL (2014), *available at* http://www.hrw.org/reports/2014/07/28/liberty-monitor-all (last accessed Sept. 13, 2014).
[39] *Cf.* Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* n. 28, ¶ 100.

- **The United States executive branch should immediately make a complete disclosure of all large-scale or indiscriminate surveillance activities conducted pursuant to Executive Order 12333 to the Permanent Select Committee on Intelligence of the US House of Representatives, the US Senate Select Committee on Intelligence, and the House and Senate Judiciary Committees.**

- **The United States executive branch should also make such disclosures about its large-scale surveillance activities as are necessary to satisfy the requirement in international human rights law that members of the public be able to foresee the circumstances in which the US may intercept their communications.**

- **The United States executive branch should review all large-scale or indiscriminate surveillance activities conducted pursuant to Executive Order 12333, including those described in this submission, and conduct a comprehensive revision of the executive order and the regulations that implement it. These revisions should afford individuals within and outside the United States the fundamental rights to privacy, freedom of expression, and freedom of assembly protected under international human rights law. At minimum, the revision should include:**

    - **Restrictions on the type and duration of surveillance measures;**
    - **An unambiguous list of grounds on which the authorizing body may order that surveillance measures be imposed;**
    - **An explanation of which bodies may request, authorize, conduct, supervise, and terminate surveillance measures;**
    - **Specific and clear procedures for storing, sharing, and destroying the intercepted data; and**
    - **Effective remedies for violations of fundamental rights that occur in this context.**[40]

- **The United States executive branch should inform the public about how it has implemented the provisions of PPD-28 imposing policy restrictions on the dissemination and retention of information about non-US persons and on the use of information acquired through bulk collection.**

- **The United States should create effective judicial and other remedies for US and non-US persons who have a reasonable basis for believing that US surveillance activities have violated their fundamental rights.**

- **The United States executive branch should actively promote the legislative codification of limitations on the retention, use, and dissemination of information concerning US persons collected incidentally or inadvertently under foreign intelligence surveillance authorities, including Executive Order 12333.**

[40] *Cf.* Escher v. Colombia, *supra* n. 28, ¶ 131; Weber and Saravia v. Germany, *supra* n. 33, ¶ 95; Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* n. 28, ¶ 76.