**Preliminary observations by the United Nations Special Rapporteur on the right to privacy, Mr. Joe Cannataci at the end of his visit to the United States of America**

1. **Scope**
   1. This document presents the preliminary observations on the official country visit undertaken by the United Nations (UN) Special Rapporteur on the right to Privacy (SRP) during the period 17-28 June 2017. The full report on this visit will be presented to the Human Rights Council in March 2018;
   2. The team from the SRP mandate (the Mandate) will remain in touch with all the officials and stakeholders it met, will continue exchanges with them via e-mail and video-conferencing as and when necessary and appropriate. Supplementing its findings on the ground with further literature review, it welcomes the willingness of all stakeholders it met to help review and fact-check results and conclusions prior to completion of more final versions of this report;
   3. If further evidence or argumentation presented after 17h00 Eastern Time on the 26th June 2017 is persuasive, the SRP Mandate reserves its right to later amend or review some of its findings, conclusions and/or recommendations;
   4. The issues studied in this visit are relevant both within the US as well as around the world. Privacy is a universal right and the USA is a global player. US policies and practices not only have an impact on the privacy of US citizens but, perhaps uniquely, also on the privacy of hundreds of millions, some would say billions, of people world-wide.
2. **Appreciation and thanks**
   1. The Special Rapporteur on the right to Privacy thanks the US Government for the open way in which it greeted the SRP and facilitated his visits. Discussions with Government officials were held in a cordial, candid and productive atmosphere;
   2. The SRP likewise thanks Civil Society, urban police persons, governmental officials and other stakeholders who presented him with detailed documentation and organised several meetings with him in order to provide detailed briefings;
   3. The SRP thanks those Congress people and their staffers who met with him and answered several questions, providing insights into issues of primary concern regarding privacy.
   4. The SRP also thanks the State of California’s Department of Justice, Office of the Attorney General as well as its Assembly Committee on Privacy and Consumer Protection for its collaboration and support;
3. **Surveillance for purposes of national security**

Positive points:

* + 1. The pervasive presence of Privacy and Civil Rights Officers at all levels of US Government Service, is a good thing, an overwhelmingly positive influence on the development of internal practices that may often be quite stringent, or at least perceived by many to be such. This appears to have had the effect of “baking in” a healthy approach to privacy within Government in many ways;
    2. There exists a general consensus that the establishment of the Privacy and Civil Liberties Oversight Board (PCLOB) was a very positive development. Of note is the impact of its reports and the willingness of many parts of the executive branch to implement its recommendations.
    3. The US has already moved to a position where case law has outlawed the carrying out of surveillance by any agency which is not specifically tasked and empowered by law to carry out surveillance.
    4. *Improvements since 2013:*
       1. The USA Freedom Act of 2015 imposed some new limits on bulk collection by American intelligence agencies, including the National Security Agency. It also restored authorization for roving wiretaps and tracking lone wolf terrorism;
       2. During the previous (Obama) administration the FCC had introduced rules that would require ISPs to obtain subscribers’ consent before using or selling data about their Internet habits. These FCC rules have regrettably been scrapped by Congress[[1]](#footnote-1), a move endorsed by President Trump in April 2017.
       3. President Obama had in January 2014 issued Presidential Policy Directive 28 which laid out that Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. While clearly a move in the right direction, the precise impact of this directive has yet to be determined.

1. **Smart surveillance in US urban areas and surveillance for purposes of law enforcement**
   1. The SRP has commenced but not completed an on-site inspection of urban police technology installations in two large US urban areas. Chicago and New York were selected because of their open public embracing of surveillance technologies for at least a decade.
   2. The SRP Mandate team is seeking to continue on-site visits to urban US Police forces during October 2017 since, for reasons outside the control of the US State Department or the SRP Mandate team, these could not be accommodated during the June 2017 visit.
   3. The on-site visits to Police installations during June 2017 focused on:
      1. The level of use of Closed Circuit Tele Vision (CCTV);
      2. The integration, if any, of CCTV with other sensors such as gunshot detectors, explosives detectors, radiation detectors, LPNR (licence plate number reader technology);
      3. The creation of police databases and the interconnectivity of local city databases with regional or national databases;
      4. The adoption of body-camera technology and its integration into existing systems;
      5. The existence of policies which enforce strict privacy standards while at the same time encouraging transparency of technology use by police forces;
      6. Mission creep by technology usage which can lead to risks to privacy;
      7. The ability of national intelligence agencies to access local urban systems with the explicit consent and knowledge of local police officials or unbeknownst to local authorities.
2. **Consumer data: privacy in the sector dominated by corporate activity**
   1. The USA’s approach to the use of personal data by non-governmental entities differs markedly from the European “omnibus” approach. Whereas the Europeans have spent the last forty years developing a system of principles which are applied equally to the public and private sectors, the USA has preferred a route where legislation is much more fragmented:
      1. The public sector is largely regulated by the Federal Privacy Act of 1974
      2. The private sector is regulated by a number of laws which were introduced in a gradual manner depending on the primary concerns of the day. Many of these which deal with personal data collected and processed in the private sector are regulated by the Federal Trade Commission (FTC). These include:
         1. The Children’s Online Privacy Protection Act (COPPA)
         2. The Fair Credit Reporting Act
         3. The Gramm-Leach-Bliley Act
         4. The Privacy Shield Framework
   2. During the meetings with corporations in the course of his June 2017 USA country visit, the focus was largely on the way corporations react to requests from Governments regarding personal data held by corporations. This has been the subject of several previous meetings by the SRP in his current and previous roles and will continue to be the subject of meetings related to the draft legal instrument on surveillance mentioned by the SRP in his report to the UN Human Rights Council on 7th March 2017. That work is expected to be subjected to public consultation in Rome 17-19 January 2018 prior to a formal view being taken by the SRP as to a further process of development and adoption, some time between March and July 2018.
   3. The SRP is also due, in a separate meeting with a number of US-led corporations scheduled for September 2017, to dedicate two days (jointly with the MAPPING Project) to discussing use of personal data by the business models of corporations.
   4. Furthermore, the SRP is awaiting the outcome of the Privacy Shield review of September 2017 to further inform his views on the use of personal data by Corporations in the USA.
   5. It is expected that the different aspects outlined above would eventually be taken into consideration by the TASk force on use of personal data by Corporations set up by the SRP and about the composition of which he also held meetings during his June 2017 visit.
3. **Health Data**
   1. *State of current protection*: The 1996 Health Insurance Portability and Accountability Act (HIPAA)[[2]](#footnote-2) provides protection to confidential health information and regulates the way in which “covered entities” (healthcare providers and organizations) can handle such information. It establishes a common standard which allows the flow of health information across the public and private health systems in the US and requires covered entities to ensure the confidentiality and security of protected health information when it is transferred, received, handled, or shared. Regarding the security of the data, HIPAA requires all covered entities to report any data breach they have suffered, even if there is no evidence that patient data was compromised. Covered entities also have the obligation to maintain backups of their patients’ information, so that they can continue to operate in case of emergency, including ransomware and other types of cyberattacks. Under the HIPAA system, patients have the right to get a copy of their medical records and ask for wrong information in their files to be corrected. If patient and health provider disagree in a diagnoses, the patient has the right to have his or her position included in the file. Also, the patient’s written consent is required to share health information with their employer, or to sell it for marketing and advertising purposes.
   2. *Glaring loopholes in current protection*: the Special Rapporteur is concerned that the current legislation, HIPAA, is not extensive enough in its coverage. Today, twenty years after the introduction of this US law, there are whole areas of data relating to an individual’s health which are not covered by HIPAA. Whether it is the data generated by fitbits and other trackers or the genetic data collected by certain companies offering genealogy services, there needs to be a thorough reconsideration of the protection afforded to all data linked to a person’s health
4. **The Privacy of Sex workers**
   1. *Autonomy of personal choice and prostitution:*
      1. The possibility of independent free choice to become a sex worker and the inalienable right to do so was emphasised by a representative of the erotic services industry who stated that “I’ve been a prostitute for 25 years and I hope to be a prostitute for the next 25 years.”
      2. While recognising that some sex workers are forced into that role, sometimes by human trafficking, it should not be assumed that there are not many sex workers, whether a large minority or indeed possibly a majority who are not part of the industry out of free choice.
      3. The erotic services industry representative who requested to meet with the SRP on learning on his visit to the USA, is currently litigating a case arguing that the criminalisation of prostitution inter alia infringes on the sex worker’s right to privacy, though in this case the SRP pointed out that what is meant here is not informational privacy but the autonomy of choice and action which is often related to privacy but is more part of self-determination.[[3]](#footnote-3)
   2. *Complications caused by criminalisation of prostitution*
      1. In 49 out of 50 US states prostitution is still illegal and the criminalisation of sex workers as well as their clients has a direct and negative impact on the private and family lives of sex workers.
      2. In a number of cases, and most recently in the case of Celeste Guap in California, it is clear that the rules of engagement for surveillance by law enforcement in cases of sex workers may need to be seriously revised. [[4]](#footnote-4) As in the UK, where recently revised codes of conduct for undercover surveillance by police have explicitly prohibited sexual liaisons of any sort as part of official work, it is time to revisit US law enforcement agency codes of conduct in this respect.
   3. *Identity management by sex workers and their private and family lives*
      1. *The right to private and family life of a sex worker*
         1. All persons, sex workers have the right to their own private and family lives. They are often mothers who wish to attend Parents Teacher Association meetings like other mothers, who wish to bring up their children without stigma, who wish to support their children to college and lead a life with the greatest normality possible. In order to do so, sex workers very often adopt at least one other identity which is completely separate to their real legal identity and live in a world, often but not always compartmentalised from their private and family life.
         2. The criminalisation of prostitution in the USA often ends up with sex workers having their real identities being divulged or publicised. One example of this practise is when a prostitute is put on a public register of sex offenders especially in those instances where they may have been arrested and accused of being traffickers or self-traffickers.
5. **The California effect: Privacy initiatives at state level**
   1. The complexities of the US situation are further increased by the fact that it is a federal state. This presented the SRP with an additional opportunity since there are a number of other federal states within the UN system for which models of good practice may always be useful.
6. **Conclusions**
   1. The USA has some of the strongest oversight mechanisms when it comes to surveillance but that is also partially because the rest of the world generally has much weaker mechanisms or non-existent ones.
   2. The USA continues with strengthening of its oversight mechanisms very much as an organic form of Work-in-Progress. In some agencies like the FBI and the CIA the process of reinforcing privacy protection and establishing a Privacy and Civil Liberties Office has been going on for years, sometimes decades. In other agencies like the NSA the effort is markedly more recent and less mature but nonetheless enthusiastic. The NSA PCLO asserted that strict safeguards are in place and existing policies are being further reviewed.
   3. Civil Society is understandably displeased that it would appear that the Director of National Intelligence appears to have reneged on what would appear to be a prior commitment to provide figures of the impact of US Government surveillance activities on US persons and specifically a quantification of the number of Americans impacted by such surveillance.
   4. The US has significantly weakened its own mechanisms which once could be considered to be the world gold standard and, post-9/11, has produced a situation where the surveillance permissible under US law would *prima facie* appear to be disproportionate to legitimate national security considerations.
   5. The USA should take the opportunity provided by the re-authorisation of FISA 702 to revert as close as possible to the pre-existing US standards some of which would then be adopted by the UN SRP as the gold standard and used in model laws and international legal instruments related to surveillance.
   6. The SRP has not, as yet, been offered evidence of the utility, efficacy, necessity and proportionality of bulk acquisition of data – some aspects of which are known as mass surveillance – but shall request that such evidence be presented to the greatest extent possible, even in a way which would be protected from undue disclosure.
   7. There would, as yet, not appear to be any cause for alarm in the uptake of smart surveillance technologies in large US urban centres, but this finding is subject to further investigation.
   8. Privacy protection in the corporate activity sector is fragmented, is possibly prone to loopholes in some areas and may be difficult to comprehend for most US citizens. The recent disapproval of FCC broadband rules intended to protect the privacy of internet users is a retrograde step.
   9. The coverage of existing laws in the health sector is inadequate and needs to be extended.
   10. The private and family lives of sex workers in many US states may be at risk because of complications arising out of the criminalisation of prostitution and may require the introduction of additional safeguards, particularly in the area of identity management.
   11. The innovative privacy-friendly actions taken at state level have a beneficial effect on privacy and may be used as a model to help speed up the protection of privacy and generally raising the level of such protection in federal states.
7. **Recommendations**
   1. Surveillance for the purposes of national security;
      1. *Nomination and Appointment of PCLOB Members*
         1. The vacant posts in PCLOB membership be filled without further delay by nomination and subsequent confirmation.
      2. *FISA Section 702*
         1. I would recommend that the US Government responds to my concerns that Congress should not re-authorise FISA Section 702 or, at the very least, if FISA Section 702 were to be re-authorised then FISA needs to be reformed by a return to a regime where an individualised warrant for non-US persons located outside the USA be issued by an independent judicial authority outside the intelligence service such as FISC against criteria of “probable cause” BEFORE any surveillance is carried out as opposed to the current approval by the FISC of targeting procedures which are administered on an individualised basis by the intelligence agencies before any surveillance is carried;
            1. I recommend that the US Government respond to the following concerns that have been represented to me by the ACLU, specifically, to re-establish FISA’s previous strengths “the US Congress should seek to:

Close the “backdoor search loophole” by prohibiting the government from searching through information obtained under FISA Section 702 for information about Americans without a warrant, and prohibiting the use of this information for domestic criminal investigations and other non-national security related activities;

Narrow the scope of FISA Section 702 to prevent the targeting of individuals who are not agents of a foreign power and who have no connection to terrorism, espionage, or nuclear proliferation;

End the mass searching of Americans’ emails and other online communications by ending the Upstream program, where the government scans and copies the contents of millions of

Americans’ communications for information related to over 90,000 foreign targets;

Improve oversight and transparency by enhancing review by the Foreign Intelligence Surveillance Court (FISC) and requiring the government to report statistics on its surveillance activities;

Limit the retention and dissemination of information collected under FISA Section 702; and

Ensure that individuals are able to challenge Section 702 surveillance in court by requiring the government to comply with its notice obligations, providing statutory standing to affected individuals, and reforming the state secrets doctrine.”

* + 1. *Executive Order 12333*
       1. The SRP mandate is investigating further the nature of oversight mechanisms applied in EO 12333 situations and expects to report about this matter at a later stage.
  1. *Smart surveillance in an urban environment and surveillance carried out for Law Enforcement purposes*:
     1. Codes of conduct and policies should be made both mandatory and transparent prior to the deployment of any technology.
     2. The extent to which intelligence agencies have access to local, city-level surveillance systems should be set out at law with all safeguards and remedies explicitly provided for by law.
  2. *Overall recommendations regarding surveillance*:
     1. The current tendency of US lawmakers to discriminate between US persons and non-US persons when it comes to privacy safeguards and remedies should be formally discontinued. In order to adopt and implement best practice, for the US to set an example internationally, the US should ensure, in recognition of the universal nature of the right to privacy that all safeguards and remedies for privacy be extended to all persons not engaged in military or espionage activities regardless of their citizenship status. This would also appear to be in line with the spirit of PPD28. Congress should extend such safeguards and remedies in all new laws and revisit existing legislation in order to bring existing statutes in line with the universal nature of the right to privacy.
     2. Congress should, consistently with its own recent record on legislating regarding surveillance[[5]](#footnote-5), and as formally already recognised in other fora[[6]](#footnote-6), introduce new legislation which would treat mass surveillance as being a disproportionate and unnecessary measure in a democratic society. Such legislation should, irrespective of whether the target is a US person or non-US person, effectively outlaw mass surveillance and restrict surveillance to targeted surveillance where pre-authorisation is obtained only upon demonstration of probable cause.
  3. *Recommendations regarding personal data held by corporations*
     1. Citizens and users need to be better educated when it comes to the impact innovative technology and business models have on their right to privacy.
     2. The USA should increase international co-operation to solve the problem of the use of corporate-held data for law enforcement and intelligence purposes.
     3. The use of corporate-held data by governmental authorities should be more transparent.
     4. the US government should commit to secure and safe systems and therefore support the use and implementation by corporations of privacy enhancing technologies such as encryption.
  4. *Recommendations regarding health data*
     1. The right to privacy should be at the core of any regulation on the collection, use and distribution of health data.
     2. No unauthorized use of personal health data should be conducted, whether identified or de-identified.
     3. HIPAA coverage should be extended to all forms of health data.
  5. *Recommendations regarding privacy of sex workers*
     1. The private and family lives of sex workers in many US states may require the introduction of additional safeguards, particularly in the area of identity management.
     2. Codes of conduct should prohibit sexual liaisons between law enforcement officers with sex workers as part of surveillance carried out for detecting or investigating trafficking of human beings as well as other illegal activities.
  6. *Recommendations regarding the simplification of privacy:*
     1. Efforts should be made at both the federal and state levels in order to provide simplified information about threats to privacy and the existence of privacy rights and how to exercise them.
     2. The information may be provided by both federal and state government or else by civil society supported by state and federal governments. So long as the myriad rules and procedures are explained systematically, comprehensively yet comprehensibly, then US citizens would be better served than they are at present.
  7. *Recommendations regarding initiatives at state level*
     1. States should be encouraged to continue to take an innovative and proactive approach to privacy, including an ongoing dialogue with the SRP in order to identify areas of good practice which could further serve as models for other federated states.
     2. States should support a variety of events co-organised with the SRP mandate in order to further promote privacy protection at state level, including especially the launching of privacy-by-design teaching in ICT courses at all levels.

1. A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services". Last accessed on 27th June 2017 at <https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34> [↑](#footnote-ref-1)
2. Complemented by the 2001 Privacy Rule, the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act and the 2008 Genetic Information Non-Discrimination Act. [↑](#footnote-ref-2)
3. For more information on the case Erotic Service Provider Legal, et al. v. George Gascon, et al., On Appeal from the United States District Court, Northern District of California see http://esplerp.org/wp-content/uploads/2016/10/22-Brief-of-American-Civil-Liberties-Union-Foundation1.pdf 27.06.2017. [↑](#footnote-ref-3)
4. Anthony, “Celeste Guap” testifies for 1st time in Bay Area police sexual misconduct scandal, ABC News San Francisco, http://abc7news.com/news/celeste-guap-testifies-for-1st-time-/2010511/ , 27.06.2017. [↑](#footnote-ref-4)
5. USA Freedom Act 2015. [↑](#footnote-ref-5)
6. Court of Justice of the European Union, Joined Cases C–203/15 and C–698/15 Tele2 Sverige EU:C:2016:970. [↑](#footnote-ref-6)