Problems and progress on the Global Privacy Trail

千里之行"A journey of a thousand miles begins with a single step" 始於足下

It is perhaps appropriate that for a meeting in Hong Kong, China, one seeks inspiration from a famous Chinese philosopher. Some time between the 6th and 4th centuries B.C., Lao Tzu or Laozi as he is often known, is believed to have been one of the authors, if not the primary author, of the *Tao Te Ching* or *Daodejing*, one of the most significant works in Chinese cosmogony. In Chapter 64 one reads "*A journey of a thousand li starts beneath one's feet*" which today is commonly rendered as "A journey of a thousand miles begins with a single step". This was the spirit which encouraged me to welcome the creation of the post of and accept the role of UN Special Rapporteur on Privacy and indeed it is a source of encouragement in taking the next important steps. This report to the 39th International Conference of Data Protection and Privacy Commissioners ("ICDPPC") is intended to up-date the participants about the most important steps taken since the 38th Conference in Morocco and also outline the steps that one can possibly look forward to before the 40th conference due in 2018.

The ICDPPC conference is one of the friendliest places and core stakeholder constituencies for the UN Special Rapporteur on Privacy (SRP). So it should not come as a surprise that it was at the Amsterdam ICDPPC conference in 2015 that the mandate's tentative ten-point plan[1] was first openly

[1] a) *Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect:* There is a need to work on developing a better, more detailed and more universal understanding of what is meant by "the right to privacy". What does it mean and what should it mean in the 21st century? How can it be better protected in the digital age? Activities will be organised and research will be supported to examine possible answers to these key questions which will help provide essential foundations for other parts of the SRP's action plan.

(b) *Increasing awareness*: Another important issue is the development of greater awareness amongst citizens in order to help them understand what privacy is. It is important to have a general discourse on what their privacy rights are, how their privacy may be infringed upon especially by new technologies and by their behaviour in cyberspace. They need to learn on how their personal data has been monetised and what are the existing safeguards and remedies. What can they do to minimize privacy risk and how can they interact with their law-makers and the corporate sector to improve privacy protection? This creation of awareness is a massive task in its own right, and the Special Rapporteur will contribute to this awareness-raising throughout on-going engagement with all stakeholders and especially civil society for the entire duration of his mandate.

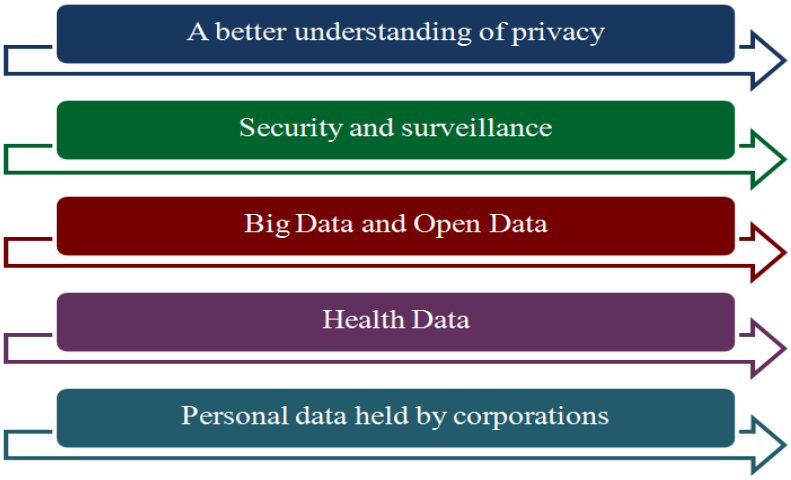
(c) *The creation of a structured, on-going dialogue about privacy*. The establishment of a more structured, more open, more comprehensive, more effective and most importantly permanent dialogue between the different stakeholders is crucial. In order to achieve the protection of privacy bridges are required and need to be built. The Special Rapporteur would like to put great emphasis on this activity and will use existing fora as well as creating new fora. To be included are particularly the facilitating of a structured dialogue between Non-Governmental Organizations, Data Protection and Privacy Commissioners, Law Enforcement Agencies (LEAs) and Security and Intelligence Services (SIS). It is essential to work with all classes of stakeholders in order to improve internal procedures, increase the level of privacy by design in the technologies they deploy and the procedures they follow. It is important to maximise transparency and accountability and reinforce impartial and effective oversight to the point where it becomes significantly more effective and credible. Without genuinely engaging with key stakeholders including those whose role may be completely necessary and legitimate in a modern society, progress cannot be achieved.

(d) *A comprehensive approach to legal, procedural and operational safeguards and remedies:* Appropriate safeguards and effective remedies have been part of the "raison d'etre" of data protection law since its inception aimed at providing guidance and protection at the correct level of detail required in a world rendered more complex by constant technological change. Clearer and more effective protection for citizens should be provided in order to prevent the infringement of privacy. Real remedies need to be available to all concerned in those cases where an infringement actually occurs. The search for safeguards and remedies is transversal and underlies all of the SRP's thematic studies identified in 4.2 above.

(e) *A renewed emphasis on technical safeguards:* The safeguards and remedies available to citizens cannot ever be purely legal or operational. Law alone is not enough. The SRP will continue to engage with the technical community in an effort to promote the development of effective technical safeguards including encryption, overlay software and various other technical solutions where privacy-by-design is genuinely put into practice.

(f) *A specially-focused dialogue with the corporate world*. An increasing number of corporations today already gather much more personal data than most governments ever can or will. What are the acceptable alternatives to or the key modifications that society should expect from current business models where personal data has been heavily monetised? Which are the safeguards applicable in cases where data held by private corporations are requested by state authorities? This dimension of the mandate requires much time and attention. The SRP has already commenced direct contacts with industry and will maintain a privacy-focused dialogue relevant to these

discussed. Nearly two years down the line, it is good to be able to report some progress as well as confirm some of the serious problems that were evident from the outset. In Morocco, in October 2016, the SRP reported on how the ten-point plan had been further refined during 2015-2016 to include the first set of five priorities (which may possibly eventually be extended to six to include "Children's rights and privacy")



This present Sep 2017 report will chart some of the progress registered on this set of priorities.

Since Morocco – 26 events, 26 SRP-related trips, 15 countries, 4 continents

2016-2017 has been a particularly hectic year for the SRP mandate and it may be useful to try to get a flavour of what has been done on the ground even through a cursory look at the list of engagements completed by the SRP. Since we last met, the SRP mandate has engaged with civil society, governments, law enforcement, intelligence services, data protection authorities, intelligence oversight authorities, academics, corporations and other stakeholders in Africa, America (North, Central and South), Asia, Australasia, and Europe. Twenty-six of these engagements took the

issues with a range of industry players with the intention of informing new developments in the corporate sector as well as other parts of the SRP's mandate.

(g) *Promoting national and regional developments in privacy-protection mechanisms* The value of national and regional developments in privacy-protection mechanisms should be appreciated more at the global level. The SRP has an important complementary role to play when working in close co-operation with Data Protection and Privacy Commissioners world-wide. Through mutual cooperation and dialogue the global standards of privacy protection could be raised significantly. The SRP has commenced a series of global activities planned and executed with Data Protection Authorities world-wide. These include events planned for Australia, Morocco, New Zealand, Northern Ireland and Tunisia for 2016 with many others in the pipeline for future years.

(h) *Harnessing the energy and influence of civil society*. Having already met with representatives of over forty (40) NGOs during his first six months in office, the SRP intends to continue dedicating considerable time to listening to and working with those representatives of civil society who are putting in so much effort to better protect privacy world-wide.

(i) *Cyberspace, Cyber-privacy, Cyber-espionage, Cyberwar and Cyberpeace* The global community needs to be inquisitive, frank and open about what is really going on in cyberspace, including the realities of mass surveillance, cyber-espionage and cyberwar. Tackling these realities will build upon the results of other action points outlined above as well as the results of the thematic studies indicate in 4.2 above. The Special Rapporteur expects these issues to be a constant feature of a number of his reports as well as in many of the country visits and, by transparently engaging with stakeholders about these issues, hopes to play a constructive role in improving the protection of privacy in the digital age.

(j) *Investing further in International Law.* While law alone is not enough it is very important. The potential for development of international law relevant to privacy should be explored in all forms and the SRP is open to examining the value of any legal instrument irrespective of whether this is classed as soft law or hard law. A priority issue such as up-dating legal instruments through an expanded understanding of what is meant by the right to privacy would seem to be an essential starting point. There appears to be a consensus amongst several stakeholders that one of these legal instruments could take the form of an additional protocol to Art. 17 of the ICCPR[1] wherein the SRP is being urged "to promote the opening of negotiations on this additional protocol during his first mandate"[1]. The precise timing of this however should probably be contingent on the duration and outcome of in-depth and wide-ranging discussions invoked through action point a) above – i.e. achieving a better universal understanding of what the core values in privacy are or may be

SRP personally to over thirty different cities, some of which in Asia, North Afsfrica and Central America, with a fourth of these engagements in the USA and over a half in Europe.

1. USA - UN General Assembly - October 2016 – New York
2. Czech Republic – MAPPING AGA – Prague November 2016
3. Mexico – IAPPA – November 2016
4. Czech Republic - Cyberspace 2016 - Brno - November 2016
5. Ireland 07 December – Dublin – Irish Civil Liberties Council - 2016
6. UK Northern Ireland –Belfast – Human Rights Commission – 08 December 2016
7. Belgium- CPDP – Brussels 25 January 2017
8. Spain – February 2017 - Madrid
9. USA – ISA 2017 Baltimore 20-22 Feb 2017
10. Denmark – ICANN – 13-14 March 2017
11. Switzerland – European Broadcasting Union – 20 March Geneva
12. Malta – MITLA conference – St Julians 28 March 2017
13. Belgium - RightsCon 2017 – Brussels 29 March 2017 (Privacy rights of Children with UNICEF)
14. France - 2017 – GIGARTS – Paris 30-31 March 2017
15. Spain – Barcelona 03 April 2017
16. Ireland – Dublin – 04 April 2017
17. UK – Northern Ireland – 05 April 2017
18. Portugal – BILETA conference – Porto – 20-21 April 2017
19. Indonesia – 23 April-04 May 2017
20. Tunisia – 23-25 UN SRP Privacy, Personality & Flows of Information Tunis 23-25 May 2017
21. Ireland – Dublin – International Data Summit - June 2017
22. USA – Official UN SRP visit (Washington, New York, Chicago, Sacramento, San Francisco, Washington 17-28 June 2017
23. Switzerland – UN SRs meeting – Geneva 28-30 June 2017
24. UK – England - Privacy Laws & Business Conference – Cambridge 03-05 July 2017
25. France – SRP & MAPPING Workshop on Surveillance Legal Instrument 13-14 Sep 2017
26. France – SRP & MAPPING Law Enforcement Workshop on Surveillance Legal Instrument – INTERPOL - Lyon 15 Sep 2017

The above outline list does not include remote participation in events in Ghana (April 20th), Japan (multiple, May-June 2017). For the record and a better understanding of how impact is achieved, It should be pointed out that, save for the official country visit to the USA in June 2017, none of the above engagements were financed by the SRP mandate's UN OHCHR budget but were instead completed thanks to extra-mural funding, largely from the hosts of the relative events.

"Privacy and Surveillance - A journey of a thousand miles begins with a single step" 始於足下

Draft international legal instrument on surveillance and privacy

It is particularly appropriate that this Chinese saying is applied to one of the SRP mandate's most important initiatives in the field of security and surveillance. This key priority is one which was amongst the most important core issues which led to the creation of the mandate of the SRP by the UN Human Rights Council in 2015. It is also one of the most difficult areas to tackle and it sets the SRP mandate apart from many of the other mandates of other Special Rapporteurs.

One of the major differences is that in the case of the majority of other mandates, there are already a number of countries firmly committed to the cause. Without in any way diminishing the difficulties or importance of other SR mandates, it is a matter of historical development that in the case of many mandates there exist years and often decades of consensus and momentum at the national and international level with a growing group of countries which are sincerely and unambiguously supportive of the work of the mandate. This is clearly not the case for a young mandate like that for privacy, which is barely two years old and which was born straight into a hellfire of controversy stirred by the Snowden revelations and since complicated much further by a number of terrorist attacks on countries which could otherwise have normally been relied upon to be at the forefront of protecting privacy. The increased tempo of terrorist attacks in Belgium, France, Germany and the United Kingdom have created national and sometimes international moods which give priority to security and which put privacy somewhere on the back burner if not off the hob or cooking range and out of the kitchen altogether. Such terrorist attacks are always highly regrettable and deplorable but the timing has additionally not been helpful to the SRP mandate. When it comes to surveillance it is always difficult if not impossible to avoid the impression that some countries are very cynical or downright hypocritical in their approach to privacy but in an atmosphere of heightened tension due to terrorism, legitimate concerns about security sometimes tend to be increased unduly by an emotive and/or calculatingly political approach which prevents governments from dealing with threats and risks in a proportionate manner as befits any measures interfering with privacy in a democratic society. Moreover, in their wish to be seen to be doing something about terrorism or other threats, some governments, happily not all, have displayed a tendency to introduce privacy-intrusive measures in their laws and operational procedures which do not appear to be effective nor proportionate nor necessary. During 2016-2017 the Governments of Belgium, Germany, the Netherlands and the UK, to mention but a handful of examples, have introduced legislation the effectiveness, proportionality and scope of which varies considerably.

The situation is complicated further by the elephants (plural) in the room. Privacy and surveillance continue to be particularly hot potatoes which few countries appear to be keen to discuss since well over a hundred individual UN member states appear to be receiving and exchanging intelligence on a bilateral basis with at least one and sometimes more than one of the five permanent members of the Security Council of the UN. While few are prepared to admit this openly, doing anything which would appear to openly support international initiatives aimed at reducing the extent to which privacy is interfered with by surveillance, is not a particularly attractive prospect for those countries big or small which wish to continue to receive intelligence on a bilateral basis. None of these countries wish to upset the power(s) which is/are feeding them with intelligence and sometimes even with material assistance including hardware and software which can be used for surveillance. This then is the context in which the SRP is expected to work and achieve progress in protecting privacy from undue interference from surveillance.

The attitude of some major powers known to be carrying out bulk interception, bulk hacking and other aggressive forms of surveillance in cyberspace has been particularly disappointing though perhaps not at all surprising. Their reaction to any approaches regarding the extent to which state behaviour in cyberspace can be considered to be appropriate and respectful of privacy ranges from polite discussion to lack of engagement to near-hysterical accusations which one could hopefully be forgiven for translating as “This has nothing to do with your mandate and mind your own business”. In the face of such hostility or indifference when it comes to the priority of surveillance and privacy, it is difficult to detect formal sources of encouragement to do much about the subject in the behaviour of a number of important and powerful UN member states. For the reasons given previously, the number of other less powerful states willing to openly hold the larger states to

account in matters of surveillance and privacy is *prima facie* at first very small. Not wishing to upset one or more of the 5Ps means that the stage set for the SRP to take action in this priority area is fraught with unseen obstacles and difficulties such that one risks running against an unholy alliance intent on blocking any initiatives which may reduce the ability of the state to carry out surveillance.

On the other hand, civil society, academia and a whole range of other stakeholders – including a growing number of governments – have expressed genuine interest in the efforts of the SRP to get a proper, constructive, international discussion going about privacy and surveillance. The number of countries not engaging in mass surveillance or bulk interception on the internet far outweighs the number of countries that do possess and deploy such capabilities. There is also a number of emerging economies keen to put their fledgling democracies on the right path when it comes to human rights. Many of these regularly ask the SRP to provide them with a model law which they can use when it comes to surveillance and privacy. The SRP is unable to, hand on heart, refer such questions to any state which has set a gold standard through its own legislation on surveillance, since in his opinion there is no shining example of national surveillance legislation which is perfectly in compliance with and respectful of the universal right to privacy. Instead, it is clearly time to define and refine such a standard in such a way that it would be useful at both national and international law.

The mention of international law here is deliberate. Another obstacle to the protection of the right to privacy that I have identified is the vacuum that there exists in international law when it comes to surveillance and privacy in cyberspace. To be fair, there are many areas of cyberlaw which are currently unregulated in a satisfactory manner, bedevilled as the subject is by problems of definition, jurisdiction and attempts to impose notions of national sovereignty ill-suited to an internet without borders. At this stage however the primary concern of the SRP is not to cure all the problems readily apparent in the regulation of a cyberspace where currently the only piece of international law applicable is the Cybercrime Convention. The primary focus is surveillance in cyberspace, the very set of issues brought to public attention by the Snowden revelations and which fuelled much of the discussion which led to the creation of the SRP's mandate. Moreover it is not only **the lack of substantive rules** which have been identified as an obstacle to privacy promotion and protection but also of **adequate mechanisms.** For example, the March 2017 report of the SRP to the UN Human Rights Council points out that

> [The Cybercrime Convention] has not yet managed to make the transfer of personal data across borders and access to data required for investigations as fast and as problem-free as some would have hoped for. One of the main reasons for this relative failure is that it has continued to rely too much on the 19th century mind-set of the sovereign nation state rather than cater for the reality of the borderless internet of the 21st century. … the Cybercrime Convention has not delivered on timely transborder flows of personal data which are suitable for detection, investigation and prevention of crime in the Internet age. One of the main reasons for not doing so is possibly that it did not go that extra step of creating a mechanism such as an international body tasked with – and granted the authority to authorise - international access to data, internationally.

Almost needless to point out is that what applies above to transborder flows in the area of crime, largely also applies to privacy and personal data in the field of national security where most countries remain reliant on bilateral arrangements based on mutual trust or a lack of trust. The lack of transparency or at least adequate oversight in such flows of personal data does nothing to generate trust or confidence in the individual citizen, the general public or amongst nations.

When briefly examining the issue of mechanisms, in my report to the UN Human Rights Council on 7th March 2017, I indicated that

> *"the Cybercrime Convention, in tandem with other multilateral treaties, including new ones created for the purpose, has the potential to be expanded in such a way so as to create an international authority which would be able to grant the equivalent of an international surveillance warrant or international data access warrant (IDAW) that would be enforceable in cyberspace. Countries signing up to such a new treaty or additional protocol could be contributing their own specialised independent judges to a pool who would, sitting as a panel, conceivably act as a one-stop shop for relevant judicial warrants enforceable world-wide – naturally in those countries which would become party to the treaty. In this way, to return to our previous example of the July 2015 decision, companies like Microsoft, Google, Facebook, Amazon, Apple and other tech giants operating data centres internationally would not need to worry about any state overstepping its boundaries but rather would be faced with an international data access warrant issued on grounds of reasonable suspicion under clear international law. Likewise, citizens world-wide would be assured that their right to privacy, not to mention other rights such as freedom of expression and freedom of association, is being protected with appropriate safeguards, even-handedly and universally."*

The mandate given to the SRP in 2015 states very clearly that I have the duty

"(c) To identify possible obstacles to the promotion and protection of the right to privacy, to identify, exchange and promote principles and best practices at the national, regional and international levels, and to submit proposals and recommendations to the Human Rights Council in that regard, including with a view to particular challenges arising in the digital age"[2]

In keeping with this mandate I have identified obstacles, some of which I have outlined above in this report, but likewise in keeping with the mandate, one may ask what are my proposals and recommendations to the Human Rights Council about this subject going to be? At this stage, it is growingly apparent that one of the things that would be most meaningful for my mandate would be to recommend to the Human Rights Council that it move to support the discussion and adoption of a legal instrument within the UN that could simultaneously achieve two main purposes:

i. provide the governments of states with a set of principles and model provisions that could be integrated into their national legislation embodying and enforcing the highest principles of human rights law and especially privacy when it comes to surveillance;
ii. provide the governments of states with a number of options to be considered to help plug the gaps and fill the vacuum in international law and particularly those relating to privacy and surveillance in cyberspace.

While the need for such a legal instrument is clear, its precise scope and form are as yet unclear. Whereas the substance of its contents is emerging clearly from ongoing research and stakeholder consultations, the best vehicle to achieve these purposes is yet to be determined especially given the mood in some countries and the preoccupation with other priorities at the international level. The project of embarking on a new piece of international law is not something to be undertaken lightly and it is very important to get the timing right. While many stakeholders in civil society and

[2] See section on mandate at http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

corporations make no secret of having a preference to develop safeguards and remedies through a piece of hard law such as a multilateral treaty, others advocate a more gradual approach through a piece of soft law such as a set of Guidelines or Recommendations.

There are many more paragraphs with more detailed reasoning which one may wish to read in the SRP report to the Human Rights Council of the 7th March 2017 but my interim conclusions were and remain:

> *"In summary therefore, a legal instrument regulating surveillance in cyberspace would be another step, complementary to other pieces of existing cyberlaw such as the Cybercrime Convention, one which could do much to provide concrete safeguards to privacy on the Internet. Happily for the SRP's mandate, a pre-existing initiative, the EU-supported MAPPING project is actually exploring options for a legal instrument regulating surveillance in cyberspace. A draft text exists, is being debated by experts from civil society and some of the larger international corporations and it is expected that this text will get a public airing some time in 2017 and certainly before the spring of 2018. It would be premature for anybody including the SRP to take a position on such a text or a similar one at this early stage of exploring options but it is possible that this could eventually prove to be a useful spring-board for discussion by governments within inter-governmental organisations including and perhaps especially the UN".*

Given the mood, cynicism, hypocrisy and occasionally even the downright open hostility of some governments, one could be forgiven for being at least slightly discouraged from going ahead with an initiative such as a draft legal instrument on surveillance and privacy. Yet the very many advantages of having such a legal instrument so outweigh the disadvantages of the risks implied in the journey, that many stakeholders have encouraged the SRP not to lose any more time or opportunity in taking such an initiative forward. From beginning the discussion to hopefully achieving fruition in having international law enhanced through a new legal instrument where states can agree about privacy and surveillance, especially in cyberspace, is a process which will take many, many years. It is a process which cannot be achieved by one person or indeed one state alone but is one around which one seeks to have coalesce many individuals and eventually associations and governments. It will be above all a gradual process which will last a number of years which overall will far outlast the three-year or maximum six-year term served by any Special Rapporteur for Privacy. Is that however a reason for the SRP not to embark on the process? Mindful of the many difficulties and the long-term time-frame, but equally mindful that "A journey of a thousand miles begins with a single step", to date the SRP is currently minded to embark on the journey and take the first single step: recommend to the Human Rights Council that it agrees on the process required to study, draft and negotiate an international legal instrument aimed at promoting and protecting privacy in the case of surveillance activities with a special emphasis on on-line surveillance.

As stated explicitly in the last report presented to the Human Rights Council in Geneva in March 2017, in taking this single first step, the SRP will be benefitting greatly from synergy created with the EU-supported MAPPING project. This project had held stakeholder consultation meetings in Washington D.C. during 2015 and 2016 as well as other workshops in Malta and New York in 2016 which produced the first very rough draft text of the legal instrument. Following endorsement by the MAPPING project Steering Committee, more workshops were jointly organised by the UN SRP and the MAPPING project in order to further examine and develop the text for a draft legal instrument. These workshops gradually brought together experts from Civil Society, law enforcement,

intelligence services and large international corporations. Following the joint meeting with the MAPPING WP4 Working Group on Internet Governance and Surveillance held in Miami, Florida, USA, in February 2017, on 16 March 2017 a revised version was produced. This attempted to reflect the consensus reached in Miami on all comments received and discussions held.

The mention made of the related developments in the MAPPING project and the eventual possible use at UN level of the MAPPING draft legal instrument on surveillance as mentioned in the annual report to the UN Human Rights Council in Geneva on 07 March 2017 has received considerable international attention especially in print and on-line media. In response to the overwhelmingly positive reception to the idea of such a legal instrument, the SRP has, throughout March and April 2017, carried out further extensive, confidential informal consultations world-wide about the thrust of the text and especially his mention of an International panel of judges and an International Data Access Warrant as discussed in Miami.

The dozens of stakeholders involved in the drafting process were given another four months to reflect on the text and offer comments in writing prior to the next Workshop on the draft legal instrument and surveillance which was jointly organised by the UN SRP and the MAPPING Project in Paris, France on 13-14 September 2017. By this stage, workshops which previously had registered an average of 25-30 participants, had grown to some fifty experts being registered to participate in and otherwise contribute to this latest consultation event, this time organised in Europe. The Paris event was followed by yet another consultation meeting, this time with law enforcement practitioners, which was held at INTERPOL headquarters in Lyon France on 15th September 2017. It is the SRP's and the MAPPING Project's intention to next take the outcome of the Paris and Lyon meetings in September and, by around 15th October 2017, circulate the duly revised draft to invitees to IIOF2017. The International Intelligence Oversight Forum (IIOF) is scheduled to be held in Brussels Belgium 20-21 November 2017 and will afford both intelligence oversight authorities and intelligence practitioners with an opportunity to examine the then-current draft of the legal instrument and offer their own comments and/or suggestions. The output of this particular stakeholder consultation event is expected to result in a draft version which would then be published on-line in December 2017.

The published version of the draft legal instrument will enable participants to prepare themselves for the first public discussion of this initiative in Rome during a special joint UN SRP- MAPPING Surveillance Stakeholder Consultation Conference scheduled for 18-19 January 2018. Any outcomes from the Rome conference will be taken into account during the **MAPPING Final General Assembly to be held in Malta on 12-14 February 2018**. Privacy and Data Protection Commissioners who may be interested in following this process more closely are very welcome to contact the SRP in order to receive invitations to either one or both of the Rome and Malta events.

If so authorised by the MAPPING Steering Committee – and to date there is explicit authorisation to do so - and if the reactions received continue to be overall positive, it is my intention to present the Draft Legal Instrument on Surveillance to the UN Human Rights Council in March 2018, endorsing it in my capacity as UN Special Rapporteur for Privacy with my specific recommendation that this be taken forward for consideration for study and eventual adoption in one form or another by the United Nations.

An essential part of the solution in avoiding a surveillance society – Creation or reinforcement of authorisation & oversight mechanisms – From IIOF2016 to IIOF 2017

It has long been recognised that one of the few areas in which the right to privacy cannot be absolute is that of the detection, prevention, investigation and prosecution of crime as well as in matters of national security. In all of these cases however it is likewise well established that any measures that interfere with privacy must be explicitly provided for by law and must pass the tests of being necessary and proportionate in a democratic society. These measure must therefore help preserve democracy and all the fundamental human rights a democracy embraces. Such measures should put in place a number of checks and balances which aim to ensure that any surveillance carried out is there to protect a free society and not one which would be largely intended to preserve control over citizens by a small elite. The prior (*ex-ante)* authorisation of surveillance and the subsequent (*ex-post*) oversight of surveillance activities, whether carried out by law enforcement agencies (LEAs) or services entrusted with protecting national security (SIS) is therefore a key part of the tapestry of rules, safeguards and remedies which a democratic society needs to put in place in order to preserve the freedoms which are part of its defining characteristics.

Devising and deploying such measures as part of a system which cherishes the rule of law is one of the priorities addressed in draft legal instrument outlined in the previous section. Setting the international gold standard for legislative safeguards and remedies for privacy in a surveillance context is one of the main functions for such a legal instrument but this is a constantly evolving field especially because of the deployment and use of various new technologies and methodologies. This is why a second major thrust in the surveillance sector by the mandate of the UN Special Rapporteur on Privacy (SRP) is that of identifying and promoting good practices which help preserve and protect privacy. As reported during the meeting in Morocco, a first edition of a new forum initiated by the SRP, the International Intelligence Oversight Forum –IIOF2016, was co-organised in Bucharest Romania in October 2016 with the support of the four Intelligence Oversight Committees of the Romanian Parliament and the EU's Fundamental Rights Agency. This enables Oversight agencies and entities to share good practices and also contribute directly to the work of the mandate of the SRP.

It is particularly a pleasure to report that IIOF2017 will be co-hosted together with three national Data Protection Authorities, those from the BENELUX countries, in line with the SRP mandate's policy of creating synergies between DPAs and Intelligence Oversight entities. It is expected to be held in Brussels on 20-21 November with a packed agenda including follow-up from IIOF2016, a presentation of the new Dutch law on surveillance and a session dedicated to an in-depth discussion of the draft international legal instrument on surveillance.

Letters of Allegation – currently not in public domain

Some of the Letters of Allegation sent by the SRP mandate to Governments also related directly or indirectly to surveillance. These will be published in due course, once a year, normally in March, in line with current UN OHCHR practice. The precise details cannot be released at this stage, especially since the 60-day period allowed to Governments for each response may not have elapsed in some cases, but they also include cases where malware was planted, possibly abusively, on the mobile devices, including smartphones of journalists and human rights activists. On the 19th July 2017, together with other Special Rapporteurs, the SRP took the initiative to issue a letter calling on the Government of Mexico to carry out a transparent, independent and impartial investigation into allegations of monitoring and illegal surveillance against human rights defenders, social activists, and journalists.
http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=E

Letters of Allegation or concern – Public domain - Japan

On the 18th May 2017, I took the unusual step of publishing an open Letter of Allegation to the Government of Japan on the SRP mandate's OHCHR website, two hours after the Geneva office having faxed the letter to Permanent Mission of Japan in Geneva. This letter, available at http://www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf , was addressed directly to the Prime Minister of Japan in response to the latter's insistence on trying to push through a law commonly dubbed as "The Anti-conspiracy bill" which possibly permits surveillance on the flimsiest of grounds and ostensibly to permit Japan to ratify the UN 2000 Convention on Transnational Organised Crime.

A. It is important to emphasise that I was compelled to write an open letter to the Japanese Government because of the extremely short timeframe which the very same Government had set itself for pushing through the law. Under normal circumstances, in a time-frame which is often longer than a year, sometimes two, where a Government often first publishes a Green Paper with the intent for consultation, and then a White Paper with specific proposals arising out of the consultations and finally a Bill with more definitive advanced proposals, I would have proceeded with a whole series of actions out of the public eye in direct dialogue with the Government. This was not possible in a situation where the Government set itself a deadline of less than 90 days for getting the bill through both chambers of the Japanese Diet especially in circumstances where over a period of ten years two previous attempts to pass such a bill had failed.
B. The method chosen and specifically the ultra-short time-frame pursued by the Japanese Government to ram through the legislation in question justifiably raises suspicions. These suspicions are further reinforced by the argumentation publicly presented by the Japanese Government i.e. that this legislation is needed to enable Japan to accede to the UN Convention on Transnational Organised Crime of 2000 in order to be better able to prevent terrorism ahead of the 2020 Tokyo Olympic Games. This is an extremely weak argument since that particular treaty was never designed to counter terrorism but rather it was aimed at organised crime, money laundering and drug trafficking. As a number of other experts have testified, including some in the Japanese Diet, there was absolutely no need to enact a law containing most of the provisions of the anti-conspiracy act in order for Japan to be able to accede to that convention. All that was needed was a law to introduce criminalisation of the forming of a conspiracy. Moreover, even had there been a need, there is no argument for the bill not to contain the privacy safeguards I indicated in my letter of the 18th May. In this context the Japanese Government's argumentation is one which is part of that body of political rhetoric which I have categorically criticised and rejected in my report to the Human Rights Council of the 7th March 2017 where I am taking political leaders word-wide to task for using the psychology of fear to push through ill-advised legislation. This is not something which has happened only in Japan but two wrongs do not make a right. If other Governments have behaved badly by using the psychology of fear of terrorism to push through defective legislation, I have criticised them in no uncertain terms. When the Abe Government in Japan attempts to use public fear of terrorism during the Tokyo 2020 Games to justify its actions and this, a few days after my report to the UN HRC in March, I am duty-bound to call it out. The argumentation used by the Japanese Government about the necessity to accede to the UN Convention on Transnational Organised Crime does not appear to have persuaded many people and smacks of being a pretext, not a genuine motivation. I am not the first person to say this and I suspect that I won't be the last. The Government of Japan did deposit its instrument to ratification for the said Convention on 11th July 2017 directly after the law was enacted however the extent of the powers created by the law is not yet be proven to be necessary and proportionate in a democratic society.

C. The Japanese Government at first made no response about the substantive points made in my letter of the 18th May but instead embarked on a campaign aimed at undermining the credibility of UN Special Rapporteurs in general. It also called my letter one-sided. Almost needless to say, calling my letter one-sided does not make it one-sided. At no point has the Japanese Government or the Japanese Prime Minister explained where or why it is one-sided.
D. The Government of Japan did finally publish a formal response to my letter of allegation in August 2017 http://www.mofa.go.jp/mofaj/files/000282252.pdf . This letter merely reproduces arguments already presented within the Japanese Parliament but is not satisfactory on a number of important counts not least the safeguards and remedies set out for *ex-ante* surveillance and *ex-post* oversight. I would normally have sought further clarifications and the opportunity to create dialogue directly with the Government of Japan as my next step. However the timing of this next step is uncertain since the Prime Minister of Japan is reported to be set to dissolve the lower house of the Japanese Parliament on Monday 25th September with snap elections set for 22nd October 2017. I shall therefore await the outcome of the elections and take up the subject directly with the newly constituted Japanese Government whoever the new Prime Minister may be.
E. Many citizens of Japan have written to me to explain their idea that, to date, the public utterances by PM Abe Shinzo and other Government officials give the impression that they seek all the excuses NOT to engage with the substance of what I have said or indeed all the procedural excuses not to engage with the SRP mandate in a constructive and fruitful manner. I have had no problem with making my arguments public and would have no problems with carrying out dialogue both in public and in private but many citizens of Japan have written to me to say that the words and actions of their Government suggest that there seems to be no will on the part of the Japanese Government to engage in fruitful dialogue about this and other matters.
F. The Japanese Government has yet to indicate as to where, in Japanese law, one may find the privacy safeguards indicated in my letter. As a matter of fact it only mentions requirements for judicial warrants required in the case of criminal investigations but makes absolutely no reference to cases of surveillance which are carried out by the intelligence services and not by the police. Instead it has sought to reassure that additional safeguards are not required by sidestepping a number of issues, including the real way that surveillance is carried out and the interaction between Japan's intelligence services and its police. Many citizens of Japan have written to me, apologising for their Government's behaviour and complaining that the behaviour of the Government of Japan is not honourable. I am patiently and sincerely continuing to offer the opportunity for fruitful and constructive dialogue.
G. The exchange of correspondence with the Japanese Government has generated considerable public debate and media attention which remains ongoing since May.
H. I am going ahead with plans to travel to Japan on an unofficial visit on the 1-3 October 2017 to speak at a long-planned symposium hosted by the Japan Civil Liberties Union as well as other events where privacy in Japan will be discussed. It is my plan that those events will continue to increase the awareness of the importance of protecting privacy in Japan
I. My UN OHCHR office in Geneva has written to the Government of Japan indicating that I am awaiting its responses as well as an invitation to travel to Japan on an official UN Special Rapporteur visit to explore all ways to strengthen the right to privacy in Japan. If and when this invitation were to materialise, the Japanese Government would very quickly find that it would be welcoming a sincere friend of the Japanese people and its Government, whoever it may be. A sincere friend may also be a critical friend for that is the role of UN Special Rapporteur, but constructive criticism should be welcomed and appreciated. The area of surveillance is one which is work-in-progress world-wide. There is no shame in not having got things right the first time round but there should be shame if one persists in error.

J. Whatever the outcome of all the issues indicated above, the situation of privacy in Japan will also be referred to in my report to the UN Human Rights Council in March 2018.

Other ongoing initiatives related to surveillance

There are other initiatives which the UN SRP mandate is exploring in the sector of surveillance, security and privacy but these are currently part of discreet negotiations at the diplomatic level and currently would not benefit from too much exposure. If judged appropriate more details will be made public at a later stage.

A better understanding of Privacy

On 9 March 2016, in my report to the UN's Human Rights Council I included a section on *Privacy and Personality across cultures* which responded to the crying need I had identified of achieving a better understanding of what privacy is or should be across cultures in 2016 in a way which makes the understanding of the right more relevant to a digital age where the internet operates without borders. In asking the question "Why privacy?" and positing privacy as an enabling right as opposed to being an end in itself, the SRP is pursuing an analysis of privacy as an essential right which enables the achievement of an over-arching fundamental right to the free, unhindered development of one's personality.

In order to help focus a fresh, structured debate on fundamentals I then stated my intention

> "to provocatively posit privacy as being an enabling right as opposed to being an end in itself. Several countries around the world have identified an over-arching fundamental right to dignity and the free, unhindered development of one's personality. Countries as geographically far apart as Brazil and Germany have this right written into their constitution and it is the SRP's contention that a) such a right to dignity and the free, unhindered development of one's personality should be considered to be universally applicable and b) that already-recognised rights such as privacy, freedom of expression and freedom of access to information constitute a tripod of enabling rights which are best considered in the context of their usefulness in enabling a human being to develop his or her personality in the freest of manners".

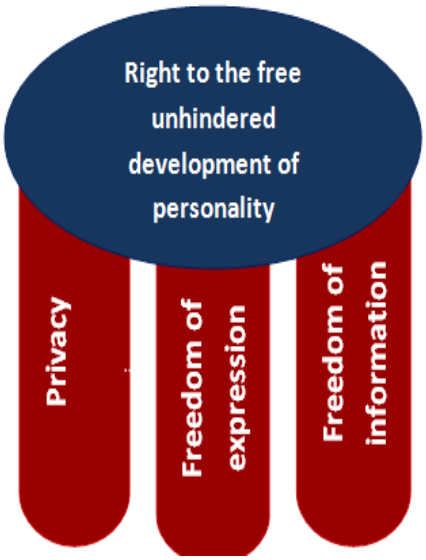
This initiative kicked off with a capacity-filling event (90 participants registered) entitled "Privacy, Personality and Flows of Information" (PPFI) held in New York in July 2016. The participation in this event by experts and stakeholders, especially civil society from around five continents was very encouraging and confirmed the need to hold a series of PPFI events around the world.

UN Human Rights Council resolution recognising right to development of personality

One of the objectives of such events is to, amongst other things, further explore a dimension of privacy which has, in March 2017, a year since the SRP's appeal about the subject in March 2016, historically been articulated and recognised in a resolution (*(UN A/HRC/L.17/Rev – March 2017))* of the Human Rights Council in March 2017:

> *"Recognizing the right to privacy also as an enabling right to the free development of personality and, in this regard, noting with concern that any violation to the right to privacy might affect other human rights, including the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association"*

This way of conceiving the relationship between Privacy and other rights followed the schematic presentation made at the PPFI in New York in July 2017



As is the case for IIOF2017 reported above, the second edition of PPFI, the one for MENA – the Middle East and North African region - was also born out of the successful relationship with and the support of the SRP's mandate by national Data Protection Authorities. The SRP takes this opportunity to publicly thank the Tunisian DPA and especially Chawki Gaddes for the wholehearted financial, logistical and moral support extended to his mandate for the organisation of PPFI MENA 2017 in Tunis 25-26 May 2017. Thanks are also due to NGOs such as Access Now, ATI and CAWTAR – The Centre of Arab Women for training and research, who collaborated continuously to help put the event together. The event was a resounding success with some 65-70 participants from Algeria, Egypt, Lebanon, Morocco, Syria, Tunisia and Qatar actively contributing to the discussion.

The Task Force on Privacy and Personality is personally chaired by the SRP with Dr. Elizabeth Coombs, until very recently Privacy Commissioner for New South Wales, Australia serving as Vice-Chair. The third edition of Privacy, Personality and Flows of Information (PPFI) will be held in Hong Kong, China on September 29-30 2017 back-to back with ICDPPC2017. This workshop conference is setup under the auspices of the mandate of the United Nations Special Rapporteur on Privacy (SRP) and is organized in cooperation with the Security, Technology & e-Privacy Research Group (STeP) at the University of Groningen in the Netherlands, the Department of Information Policy and Governance of the University of Malta and the MAPPING Project (Managing Alternatives for Privacy, Property and Internet Governance). We are happy to have Digital Asia Hub and the University of Hong Kong as local partners and hosts, with the Data Protection Commissioner for Hong Kong, Mr Stephen Wong also lending his support at what is a very busy time for him and his office. Once again the SRP extends sincere thanks to all those who have worked so hard to make this event happen. It so far has in excess of seventy (70) participants registered so growing rapidly from workshop status.

This meeting will have a particular focus on developments and trends in Asia which will be studied and discussed from an interdisciplinary perspective. Some of the topics covered will include Asian traditions in privacy, surveillance and privacy in Asia, Privacy and its relationship to other human rights in Asia and Women and Privacy in Asia.

The fourth edition of PPFI is currently being planned and will most probably take place in South America in Spring 2018. More details and a “save the date” will be released after further consultations are held at ICDPPC2017… so a special appeal is here being made to Data Protection Authorities and activists in South America to contact me if they would be interested in co-hosting or otherwise lending support.

Big Data and Open Data

The work on this subject by the ad hoc Task Force led by David Watts, until very recently, Data Protection and Privacy Commissioner for the state of Victoria in Australia, has progressed well and the draft report to be presented to the UN General Assembly at the end of October is currently undergoing peer review. This is the first of a number of thematic reports planned to be researched and presented by the mandate of the UN Special Rapporteur on the right to privacy (SRP) with the assistance and often the primary effort of a Task Force formed by volunteers and sectoral experts from around the world. The report was originally intended to be in a more finalised state by July 2017. Circumstances arose however, more details about which cannot be published before March 2018, where at least one serious incident of re-identification of data occurred during 2016-2017. This incident is the subject of an investigation by the SRP, which cannot be concluded until the relevant Government has had the time allocated to Governments to respond to correspondence (normally at least 60 days for each response as well as subsequent follow-up exchanges) and a decision made on whether the case should be included in the report of this Taskforce to the Human Rights Council. Thus it has not been possible to undertake a broad public consultation prior to finalising this interim version of the report, and therefore, it was decided to modify the procedure for the report to be developed as follows:

i. The work of the Task Force to July 2017 as reviewed and edited by the SRP would be developed with two main objectives: firstly to be presented to the General Assembly of the United Nations In October 2017 as an introductory study identifying some key issues and making some

preliminary recommendations; secondly to be used as a discussion and consultation document about the next steps to be taken at the national and international levels;

ii. Once published in October 2017, this first report on the subject would be opened for public consultation wherein all stakeholders would be able to offer comments and suggestions over a six months period until March 2018;

iii. Once the report to the Human Rights Council containing the Letters of Allegation by the SRP and the responses from Governments is published in March 2018, it would be possible to hold one or more events around the theme including a two-day conference on Big Data and Open Data co-organised by the SRP. This would enable at least three things to be taken into consideration:

a. This original preliminary report to be published in October 2017

b. Comments and suggestions received from stakeholders around the world between October 2017 and March 2018

c. The allegations and Government responses published in March 2018

iv. It is now planned that the public consultation conference will be held in Australia some time in March-May 2018

Health Data

The SRP's Task Force on Health Data has commenced work under the leadership of Dr Steve Steffensen of the United States. It is expected that the first results of its work would be made public for consultation in spring-summer 2018

Use of Personal Data by Corporations

The SRP has personally continued to lead some work on business models and privacy within corporate use of personal data also within the MAPPING Project and this as a build-up to the launch of the SRP's Task Force on the subject. It is expected that the latter will work within the timeframes announced at http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx

Official Country visits

The influence of countries world-wide especially on the legislative process in other states, especially in ex-colonies, as well as reported surveillance-related activity is one of the principal considerations when requesting formal country visits. This may be seen especially in the choice of requested country visits: the United States of America (19-28 June 2017), France (requested for 13-17 November 2017), the United Kingdom (confirmed 11-17 December 2017), Germany (requested for 29 January-02 Feb 2018) and South Korea (03-15 July 2018). These are countries with strong democratic pedigrees and are states that the SRP expects to take a leadership role, in defining best practices and safeguards in the field of surveillance and fundamental human rights, especially privacy. Additionally, these countries have been particularly active in this area during the past several years, both in terms of applied surveillance technologies as well as new legislation. Each of these visits includes requests to meet intelligence services, oversight authorities, and ministers

responsible for both LEAs and SIS. The end-of-mission statement for the official country visit to the USA is available at http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx while the related press release may be found at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21806&LangID=E

The more detailed report on Privacy in the USA is expected to be published in or around March 2018.

Acknowledging assistance from a number of friends and colleagues

The SRP is pleased to report an improvement in the quality of support – though not yet in the quantity – from OHCHR in Geneva. Relationships have progressed to being professional, cordial and productive. As ever, tremendous support is extended to the SRP by colleagues from the Security, Technology & e-Privacy Research Group (STeP) at the University of Groningen in the Netherlands and the Department of Information Policy and Governance of the University of Malta. Without them, their understanding and assistance it would have been impossible to function.

While always working very closely at a local level with NGOs most of which are quite small, the work of the SRP could not be undertaken successfully had it not been for the assistance of larger NGOs from around the world. Without in any way detracting from the value of the work of other Civil Society Organisations, the SRP would like to single out for attention the usefulness of the efforts of the following CSOs with whom the mandate collaborates in a variety of ways: ACLU[3], Access Now[4], Amnesty International[5], APC[6], Article19[7], Human Rights Watch[8], INCLO[9] and Privacy International[10].

Many of the NGOs the SRP mandate works with are indeed excellent. Some, however, remain fractious and a tiny minority of their officials are – in the words of a senior Data Protection Authority official – "very aggressive" in their attitude towards each other, the SRP and often life in general and occasionally everybody and nobody in particular. Additionally, and just as regrettably, in some cases, the behaviour and mind-set of some NGOs and/or their officials has come to resemble more that of the politicians and diplomats that they have to deal with, often losing sight of the very reason for their existence in the first place. Power struggles, personal ambition, weird and wonderful personalities, a lack of a thorough knowledge of the subject or of the workings of national and international diplomacy, all of these factors and more lead to a minority of NGOs or their leaders to behave in a way which is both unwelcome and unproductive. In their written and published statements, not to mention their behind-the-scenes machinations, it is often clearly the case of some being a hammer which thinks that everything is a nail. Hopefully some day these people will realise that an SRP must be a Swiss Army knife not a hammer cast in their own image…and treat him or her as such. Until that day, if ever, we will not be holding our breath but extending a friendly hand to one and all men and women of goodwill. Finally, a special "Thank you" to the organisers of ICDPPC for this opportunity to bring you up to date with the activities and progress of the last year.

[3] https://www.aclu.org/issues/national-security/privacy-and-surveillance
[4] https://www.accessnow.org/issue/privacy/
[5] http://www.amnestyusa.org/our-work/issues/security-and-human-rights/mass-surveillance and https://www.amnesty.org.uk/issues/Mass-surveillance
[6] https://www.apc.org/en/pubs/research
[7] https://www.article19.org/cgi-bin/search.cgi?q=privacy
[8] https://www.hrw.org/sitesearch/surveillance
[9] http://www.inclo.net/
[10] https://www.privacyinternational.org/reports