PRIVACY AND PEACE

Joseph A. Cannataci[1]

Abstract – Privacy and Peace: The paper identifies the smartphone as one of the most important privacy-relevant changes since Erich Schweighofer entered the scene in the 1980s. The resultant explosion in user-generated content and transactional data as people access the web non-stop, everywhere, provides fertile ground for online surveillance by state-sponsored actors. As states fight an undeclared war in cyberspace, two new paradoxes emerge. Privacy has become a prime casualty of a cold war currently raging in cyberspace which may actually be preventing hot war with live bullets breaking out in the off-line world.

---

[1] JOE CANNATACI was appointed as the first ever UN Special Rapporteur on Privacy in 2015, following the Snowden revelations about mass surveillance. His UN mandate was renewed in 2018 until August 2021. He is head of the Department of Information Policy & Governance at the Faculty of Media & Knowledge Sciences of the University of Malta. He also co-founded and continues as Co-director (on a part-time basis) of STeP, the Security, Technology & e-Privacy Research Group at the University of Groningen in the Netherlands, where he is Full Professor, holding the Chair of European Information Policy & Technology Law. A Fellow of the British Computer Society (FBCS) and UK Chartered Information Technology Professional (CITP), his law background meets his techie side as a Full Professor (adjunct) at the Security Research Institute & School of Computer and Security Science, Edith Cowan University Australia, as well as a Senior Fellow and Associate Researcher at the CNAM Security-Defense-Intelligence Department in Paris, France. His past roles include Vice-Chairman/Chairman of Council of Europe's (CoE) Commmittee of Experts on Data Protection 1992–1998, Working Parties on: Data Protection and New technologies (1995–2000); Data Protection & Insurance (1994–1998); CoE Rapporteur on Data Protection and Police (1993; 2010; 2012); CoE Expert Consultant on Data Protection and Cybercrime (2012–2014); UNESCO Expert Consultant on Privacy & Transparency on the Internet (2015); Scientific Co-ordinator of multiple EU FP7 & H2020 research projects focussing on privacy. He was decorated by the Republic of France as Officier de l'Ordre de Palmes Academiques (2002). His latest books include *The Individual and Privacy* (Routledge March 2015), *Privacy, Free Expression & Transparency* (UNESCO co-editor 2016–2017) and *Handling and Exchanging Electronic Evidence across Europe* (co-ed. Springer 2018).

Table of contents

The first University departments or research teams in «Computers and Law» which were established in Europe in the 1970s and 1980s, dedicated their time to two main branches of activity: the legal applications of then-new computer technologies and the legal implications of these technologies. To explain their interests to other researchers, they often distinguished these two main branches of activity as «the computer as a tool for the lawyer» and «the computer as a subject of the law». In the latter category Privacy, was a major concern of that very first tiny community of researchers in the field. It is an even larger concern today, on the cusp of 2020. That concern was part of the movement that led to the first generation of data protection laws between 1970 and 1981 leading to the Council of Europe's 1981 Convention on Data Protection and the EU's Directive 46/95. It remained strong enough to generate the EU's GDPR which came into force in May 2018 as well as the updating of the Council of Europe's work in Convention 108+ which opened for signature in October 2018. As we look back on almost forty years of activity in the field of computers and law[2] we are also looking back at the history of the evolution of concerns about privacy and its relationships with other areas of what has now come to be called «Technology Law». I intend to here explore further some of the complex web of relationships between privacy and security, and ultimately, privacy and peace.

[2] This essay was written in honour of Erich Schweighofer for his 60th birthday. Erich became interested in «Computers and Law» since his student days in the early 1980s and has been active in the field ever since. His professional career over the past thirty-five years has progressed in parallel to the technological developments that are outlined in this essay, and the intention here is to invite reflection on those things that we foresaw, those things which we could have foreseen and those things which just grew organically without adequate policy discussions or even much academic consideration.

The Cuckoo's Egg[3] is a book published in 1989. In it, author Cliff Stoll gives a first-person account of how he tracked a hacker who was selling to Russia's KGB information stolen from computers mostly located in the USA. Thirty years later the stories about Russian-instigated or financed hacking have not gone away. They have been significant and they have multiplied. Some of them were so serious that they became the subject of major investigations and court cases. «Russia stories» have been joined by stories about hacking carried out by or on behalf of a variety of nation-state actors, including China, Israel, Iran, North Korea, the United Kingdom and the USA, to mention but a few. There are some significant differences however between 1989 and 2019. Let us briefly look at those differences produced by an evolution of the technologies used by citizens in their everyday lives and especially the internet. So what has the Internet and its most famous overlay, the World-Wide Web, achieved, intentionally or otherwise, since 1989?

1. It provided a paradigm shift for the level of interaction between consumer and media producer with the citizen no longer being a passive consumer;

2. It created new classes of service providers including Internet service providers (ISP), search engine providers and other entities which benefit from innovative ways of attracting, organising and presenting information;

3. The interaction between consumer and media content supplier created a new class of creator of content: the consumer himself or herself. No longer solely reliant on journalists, writers, radio or film producers, consumers began to publish themselves. Thus, user-generated content (UGC) was born wherein the user is often revealing information about himself or herself whether in text or through images, moving or still;

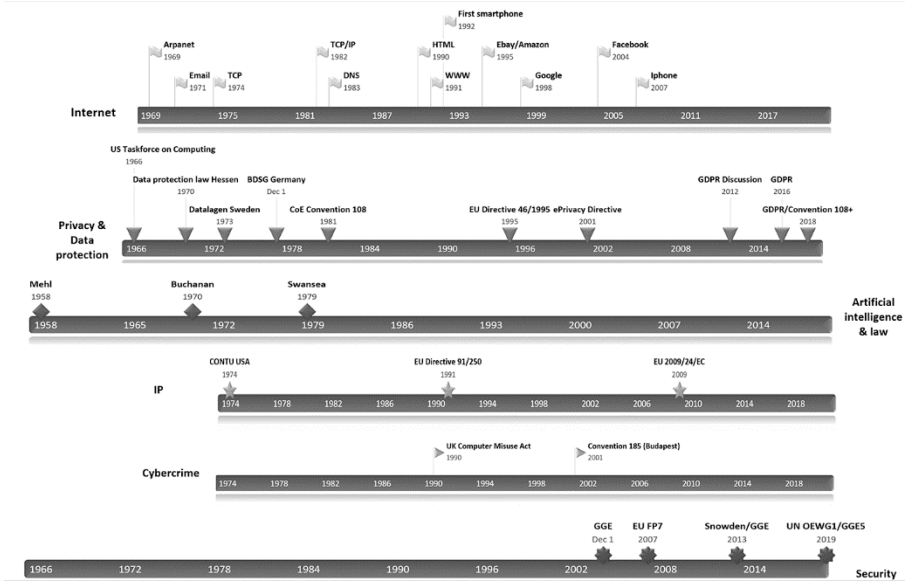
4. It is not only UGC that may contain personal information – the very inter-action by the user and an ISP or a website creates a mass of personal data because each transaction leaves an electronic track;

---

[3] CLIFFORD STOLL, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,* Doubleday, USA 1989.

5. The convergence of technologies especially in terms of mobile telephony, photography, computerisation and internet access in hand-held devices, especially smart phones, has dramatically increased the frequency and diversity of geographical locations where UGC is produced. It has also multiplied by quantum levels the «particulates» consumers produce – the telltale electronic fingerprints and footprints that litter the electronic universe.

These developments in society took place against a background where an old-established, traditional discipline like law was being challenged to create one or more new sub-disciplines. Over the years, the intersection of law with new technologies has been a sub-discipline or set of sub-disciplines known by many names such as «computer law» or «IT law» or «ICT law» or «Internet Law» or «Technology Law». The table below attempts to place the major developments in this emerging field against a time-line illustrating the development of a key technology: the Internet. This should better explain what any scholar interested in Technology Law would have had to cope with simultaneously over the past four decades. At least six new sub-disciplines were opening up in Technology Law: Legal Information Retrieval, Privacy & Data Protection law, Artificial Intelligence and Law, Intellectual Property Rights in hardware and software, Cybercrime, and Security. The time-lines in the diagram below should illustrate what kind of world any 18–20 year old aspiring law student would have found, arriving at University in 1979 and what he or she would have had to live through in their first six or so formative years of study. Back then, «computers and law» was a highly specialised field of study, a «special interest» topic which most Faculties of Law around Europe had largely never heard of. Even today, in 2020, it is only a small minority of Universities that have established centres of excellence in Technology Law.



Thus, any law student «mad enough[4]» to be interested in the subject of «computers and law» in the first half of the 1980s would have had a very interesting time, if fortunate or determined enough to get anywhere near those very rare books or journal articles touching upon the topic. He or she would not only have found a 10–15 year old ongoing debate on computers and privacy. There would also be seminal movements in the field of software and intellectual property rights, such as when the US Congress in 1980 added the definition of «computer program» to 17 U.S.C. Across the Atlantic, the Council of Europe went beyond the soft law established in the very first recommendation on the protection of medical data adopted in 1980, when in January 1981 it opened for signature the world's first – and still leading – binding international treaty focused on privacy and data protection, the so-called Convention 108. He or she would have found a revived debate about artificial intelligence and law which Lucien Mehl had launched in 1958. For much of the excitement about using the computer for legal information retrieval had, by 1979, already given way to interest in AI and Law, an interest that was to

4 The sanity of this author, like so many others, was questioned when he announced that he was interested in computers and law, publishing his first papers in the field in 1983–84.

prove cyclical at best over the next thirty years. Throughout all these developments however, it can be seen that, with some notable exceptions, most lawyers stuck to their traditional sub-disciplines: IP lawyers did IP in software and hardware, constitutional law and other public law lawyers did Privacy, academic lawyers and computer scientists did AI and Law. Indeed, when the emphasis turned to cybercrime in the decade 1990–2000, most of those working on the subject came from the field of criminal law. This concentration explain why minimal allowance was made for privacy and other fundamental rights in the Cybercrime convention.

This then was the world that provided the formative years for Erich Schweighofer who, by the end of the 1990s, had dedicated much effort to legal expert systems and automated representation of document structure and content, while trying to remain abreast of developments in other areas of ICT Law. The sub-disciplines of «computers and law» did meet occasionally in conferences like BILETA or IRIS, once or twice a year, but efforts at true interdisciplinarity were relatively few and far between. Yet, something which had been creeping quietly onto the scene, was the security dimension. A whiff of this had been obtained in 1987 when the Council of Europe devised and launched its Recommendation on Data Protection and the Police, easily one of the most successful examples of soft law ever[5], but European researchers had to wait another 20 years until 2007 when security was finally recognised as a stand-alone field of research in the European Commission's Framework Programmes. As of FP7, joining the dots in computer law became more inter-disciplinary by design, with the legal implications of surveillance, smart surveillance, privacy and internet governance, amongst other topics, interwoven with studies as to how technology could be used to achieve better security for European citizens. The many projects we worked on together with Erich in FP7 were to

[5] Recommendation (87)15 of the Council of Europe provided the data protection references for the Schengen treaty in 1989, became part of the EU's *acquis communautaire* by 1996 and was so well established as a European standard that, the ten countries which joined the EU in 2004 had to incorporate its provisions into their law as a pre-requisite to joining. The principles of Rec(87)15 live on in their entirety, in considerably more detail, in the EU's «Police Directive» (EU Directive 2016/680) which came into force on 06 May 2018.

prepare us mentally for the post-Snowden world, which as of June 2013, announced itself as one where security would henceforth remain inextricably linked with subjects like privacy.

Now, colleagues as far apart as Australia[6] and Europe sought to provide some level of conceptualisation of security and security science[7], but the link between Privacy and Peace may not have been immediately apparent to many, even those working for many years in the field of «computers and law».

PEACE

The Simple English Wiktionary provides the following definition for peace.

> *Peace is a time without any fights or wars. In a larger sense, peace (or peacefulness) can mean a state of harmony, quiet or calm that is not disturbed by anything at all, like a still pond with no ripples.*

While, interestingly enough, the Oxford English dictionary includes both Privacy and Security under synonyms in the following definition of Peace[8]

> *«can't a man get any peace around here?»*
>
> *SYNONYMS*
>
> ***tranquillity***, calm, calmness, restfulness, peace and quiet, peacefulness, quiet, quietness, quietude, silence, soundlessness, hush, noiselessness, stillness, still

---

6 CLIFTON SMITH and DAVID J. BROOKS, Security Science: The Theory and Practice of Security, Butterworth-Heinemann, Elsevier, 2013.

7 For example, the Department of Information Policy & Governance at the University of Malta formally conceptualises, understands and operates security science as an «*interdisciplinary science that draws on many fields [disciplines] (such as computer science, information and communications technology, information policy and governance, law, psychology, criminology, sociology, social anthropology and philosophy) in developing theories, constructing a structured body of knowledge and identifying concepts and principles about risks/threats to human beings, material or intangible assets in a variety of specified contexts or situations as well as the protection to be extended to such human beings and/or assets in such situations*» (CANNATACI 2015).

8 https://www.lexico.com/en/synonym/peace last accessed on 08 December 2019.

> ***privacy**, privateness, seclusion, solitude, isolation, retirement, lack of disturbance, lack of interruption, freedom from interference*
>
> *ANTONYMS noise, irritation*
>
> *2'those who have guilty secrets rarely enjoy true peace of mind'*
>
> *SYNONYMS*
>
> ***serenity**, peacefulness, tranquillity, equanimity, calm, calmness, composure, placidity, placidness, rest, repose, ease, comfort, contentment, content, contentedness, security*
>
> ***bliss**, joy, nirvana*

Perhaps it was almost inevitable that the Cold War never really ended but instead morphed into the intense economic, political, military, and ideological rivalry between nations, yet falling short of conventional military conflict, that we have today. Are we at war, even if only through proxy wars or in the intense hostilities that can be detected in cyberspace? As Conor Deane-McKenna has put it

> *«The world is fighting a hidden war thanks to a massive shift in the technologies countries can use to attack each other. Much like the Cold War, the conflict is being fought indirectly rather than through open declarations of hostility. It has so far been fought without casualties but has the potential to cause suffering similar to that of any bomb blast. It is the Cyber War. When we think of cyber attacks, we often think of terrorists or criminals hacking their way into our bank accounts or damaging government websites. But they have now been joined by agents of different governments that are launching cyber attacks against one another.»*[9]

So, already our definition of what actually constitutes peace may be a doubtful one. Are we any more at peace – or at war – than when the Cuckoo's Egg was published in 1989? In 2020, NATO on the one hand, and the Russian Federation, Iran, China and North Korea on the other hand, may not be formally at open war. Yet, their

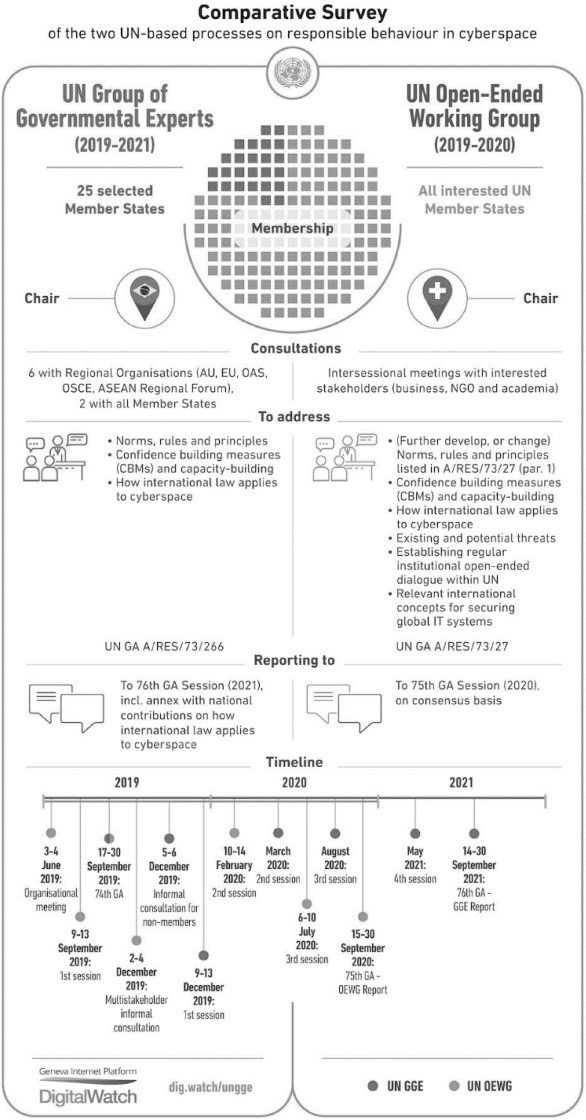
---

9 CONOR DEANE-MCKENNA, The next Cold War has already begun – in cyberspace, The Conversation, April 7, 2016, last accessed on 09 December 2019 at https://theconversation.com/the-next-cold-war-has-already-begun-in-cyberspace-57367

activities in cyberspace are unquestionably hostile towards each other. The United Nations has long tried to make the peace a more real and enduring one. The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) is a UN-mandated working group in the field of information security. Six working groups have been established since 2004, including the GGE 2019–2021 which was set up on the initiative of the USA. The fifth GGE ended up in failure and recrimination in 2017, while the current sixth GGE which opened in 2019 is being shadowed by a parallel process, that of the Open-Ended Working Group (OEWG) created in 2018 on an initiative of the Russian Federation.

The following diagram reproduced here with the kind permission of the Geneva Internet Platform summarises in a concise way the different yet overlapping roles of the UN's GGE and OEWG are both seeking to develop to arrive at responsible behaviour in cyberspace. [10]

[10] These are running in parallel with a third UN process approved in November 2019, that of a new UN cybercrime regulation initiative led by Russia and supported by China. There exists the risk that rather than tackling cybercrime, the UN-endorsed treaty would give governments the green light to block websites which are critical of the government in any given state. It would possibly also encourage governments to use technologies to monitor dissidents under the guise of tackling cybercrime.



Geneva Internet Platform (2019) Comparative survey of the two UN-based processes on responsible behaviour in cyberspace. Digital Watch observatory. Available at https://dig.watch/processes/un-gge

It is still too early to tell as to whether either or both of the two established UN processes on responsible behaviour in cyberspace, GGE and OEWG, will end in success or failure. The most important point to note at this stage is that, whatever is agreed at the UN, it is our personal data and privacy which are at stake. Indeed, it was the intrusions on privacy in the name of state security as evident in the Snowden revelations which, in the first place, led to the creation of the UN Special Rapporteur on Privacy in 2015. In my first report to the Human Rights Council on 9 March 2016, I referred to the importance of working together towards ensuring cyberpeace. That report also made positive reference to the efforts made by several influential States to start defusing the growing tensions in cyberspace, but it was written before the failure of the 2017 GGE.

The fact remains that cyberspace risks being ruined by cyberwar and cyber-surveillance. Therefore, it should stand to reason that Governments and other stakeholders should work towards cyberpeace. In this sense at least, Privacy protection is also part of the cyberpeace movement. The key link between Privacy and Peace is that you cannot really have one without the other and yet the quest for one may destroy the other. To be more precise, many state actors carry out surveillance in cyberspace in order to maintain and enhance their own security. This enhanced security may contribute to «keeping the peace» yet the price which comes with surveillance in cyberspace is often that of the infringement of the privacy of individual citizens spread across multiple nations. Let us take two examples.

PRIVACY OF 500 MILLION YAHOO! USERS INFRINGED – 2014–2016

Formal indictments were brought in the United States of America by the Department of Justice, which announced on Wednesday 15th March 2017 the «indictments of two Russian spies and two criminal hackers in connection with the heist of 500 million Yahoo user accounts in 2014, marking the first U.S. criminal cyber charges ever against Russian government officials. The indictments target two members of the Russian intelligence agency FSB, and two hackers hired by the Russians. The charges include hacking, wire fraud, trade secret theft and economic espionage, according to officials.»[11] The

[11] As reported via ELLEN NAKASHIMA, *Justice Department charges Russian spies and criminal hackers in Yahoo intrusion,* The Washington Post, March 15th 2017 last accessed on 03 October 2019 at

case was partially included in May 2018 with the conviction of a Canadian hacker-for-hire. The case presented convincing evidence.[12]

Although enormous, this was not the largest breach of email privacy in history. Evidence emerged in October 2017 that all 3 billion Yahoo Accounts were compromised in an even larger privacy breach that occurred a year earlier in a 2013 hack[13] with evidence whether it was a state-sponsored attack.

The point here is that the spread of the damage was global. The world has twice witnessed what where possibly the largest or some of the largest known privacy intrusions in history, compromising e-mail. We must therefore consider the problem of the nature and scale of the attack in addition to the instability induced by public accusations made against Russia. The guilt of the accused appears to have been proved beyond reasonable doubt, and thus the problem is compounded by the involvement of state officials who may or may not have been acting on behalf of the government. Given the sums involved in the payment of the hacker-for-hire, the likelihood of government involvement is almost certain. It is highly the instructions seem to have been there. State involvement is

https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?utm_term=.e200088586fb).

12 «Baratov, a Canadian national and resident, and three other defendants, including two officers of the Russian Federal Security Service (FSB), Russia's domestic law enforcement and intelligence service, were charged with a number of offenses relating to the hacking of webmail accounts at Yahoo and other service providers. In particular, the defendants were charged in a computer hacking conspiracy in which the two Russian FSB officers hired criminal hackers to collect information through computer intrusions in the United States and abroad, which resulted in the unauthorized access of Yahoo's network and the spear phishing of webmail accounts at other service providers between January 2014 and December 2016.» International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison Russian Officers Tasked Prolific Hacker-for-Hire to Target Webmail Accounts. US Department of Justice Media Release last accessed on 19 December 2019 at https://www.justice.gov/opa/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-60-months.

13 JONATHAN STEMPEL, JIM FINKLE, *Yahoo says all three billion accounts hacked in 2013 data theft*, Reuters, October 3, 2017 / 10:57 PM last accessed on 19 December 2019 at https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

almost certain since it is highly unlikely that the Russian agents concerned were spending their own money rather than that of their employer. Even if there had been no government involvement, the suspicion of agents acting for the Russian state is already a destabilising factor in international relations and threatening all forms of peace, above and beyond cyberpeace. The violation of the personal space of hundreds of millions of internet users has not, to date, attracted much attention but it remains a source of major concern to those involved, over and above the charges actually made in the US indictment.

PRIVACY OF 500 MILLION (?) YAHOO! USERS BREACHED BY US AGENCY (REPORTED 4th OCTOBER 2016)

If you're a Yahoo! e-mail user, if it's not one government hacking into your e-mail account or scanning your incoming messages, then it's another. Or, at least uncontradicted media reports so suggest. For some time during the period 2014–2016, hundreds of millions of Yahoo! e-mail users apparently not only suffered the most massive hack in history as already mentioned above (allegedly by a combination of Russian criminal and state-connected persons), but also had their incoming mail scan-read on the orders of a US Government agency.[14] There are multiple causes for concern here. Firstly, all those Yahoo! users within the United States may arguably claim that such searches violated their Fourth Amendment rights under the US constitution, although the scan-reading was carried out in terms of lower-level US law (FISA). Secondly, it should be clear to all concerned that well more than half of those five hundred million Yahoo users are not US citizens and would need to seek recourse elsewhere for protection of their fundamental and universal right to privacy. Where they could do so, however, is the obvious. Even if such a breach were ever to be considered a proportional measure to achieve US national security interests – and that is a contentious point in its own right – unless there were an international agreement that elucidated appropriate state behaviour in cyberspace, hundreds of millions of

[14] JOSEPH MENN, *Yahoo secretly scanned customer emails for U.S. intelligence*, 4th October 2016, Reuters, last accessed on 24th April 2017 at http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT.

international citizens to whom US constitutional protections don't apply would yet again find themselves without any effective safeguards or remedies when it comes to their fundamental right to privacy.

THE PARADOX OF PRIVACY AND PEACE

These two Yahoo-related cases amply illustrate the problem of state actors continuing to be hyperactive in cyberspace. In their attempts to detect hostile behaviour or indeed to carry out hostile acts, the states involved infringed on the privacy of approximately five hundred million people in these two case studies alone. The fact that cyberspace has become the battleground for an undeclared war means that hundreds of millions of innocent civilians become caught up in a way that threatens their privacy. Yet, some would argue that these state actor infringements of privacy in cyberspace actually help reduce the risk of a hot war breaking out in «meat-space», i.e. off-line space. A hot war means real-life human casualties. Surely then, some may argue, some loss of privacy is a price worth paying if this avoids conventional wars?

The only alternative would be to declare cyberspace off-limits for hostile behaviour. Online espionage and hostile state actor behavior threatens cyberpeace through or impacting at least three main dimensions to cyberpeace all threatened by on-line espionage or other hostile state actor behaviour:

(i) sabotage and warfare;

(ii) intellectual property rights and economic espionage;

(iii) civil rights and surveillance.

While privacy is mostly concerned with the third dimension, i.e. civil rights and surveillance, this is often also caught up in discussions about the first and second dimensions. In September 2015 it was announced that the USA and China had agreed «that neither government would support or conduct cyber-enabled theft of intellectual property» and that «both countries are committed to finding appropriate norms of state behavior in cyberspace within the international community. The

countries also agreed to create a senior experts group for further cyber affairs discussion.» [15]

Not only did the US and China follow up this important step forward with cyber talks in December 2015 but they seem to have set an example for other countries too: «the U.S. announcement was followed by a similar agreement between the UK and China, and a report that Berlin would sign a «no cyber theft» deal with Beijing in 2016. In November 2015, China, Brazil, Russia, the United States, and other members of the G20 accepted the norm against conducting or supporting the cyber-enabled theft of intellectual property.»[16]

These efforts are still a way off from achieving comprehensive agreements about cyberwar, online surveillance, or the impact of espionage on the privacy of individuals, but at least it is a start.

Which are the realistic steps that can be taken to try to persuade all parties concerned that the discussions should extend to include concrete measures for respect of on-line privacy too? To sum up, if states were to arrive at and respect an international agreement that they would not carry out hostile acts such as those in the Yahoo! Cases cited above, then it could be said that the privacy of billions of internet users would be less at risk. This form of cyberpeace would deny the states concerned the ability to fight proxy wars or other hostilities in cyberspace. On the other hand, while, at this moment in time, there appears to be little chance for state actors to agree not to carry out hostile acts in cyberspace, their doing so, the very fact that a cold war is currently raging in cyberspace may actually be preventing hot war with live bullets breaking out in the offline world. So lack of cyberpeace and an element of cyberwar infringing upon privacy may actually prevent war outside cyberspace. This then is the paradox of privacy and peace.

It is a paradox which is currently preventing the realisation of a dream that cyberspace can truly become a digital space where the citizen can expect both privacy and security,

---

15 This was reported at http://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

16 As reported via http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.

a peaceful space which is not constantly being put in jeopardy by the activities of some nation states over and above the threats posed by terrorists and organised crime.

My greatest worry has long been that the world will continue to split into two broad camps with some countries caught in the middle of those who, on the one hand, genuinely aspire to create a global human-rights and rule-of-law respecting regime, however imperfect, and the other bloc who only pay lip-service to human rights and works hard to consolidate their «rule-by-law» regime, where the law becomes merely a tool of control by the oppressor rather than a strong system of safeguards for the oppressed. My UN mandate's main thrust to counter this has been to follow up our work on government-led surveillance with the growth of IIOF – the International Intelligence Oversight Forum, which the Russians and the Chinese don't participate in, though they have always been invited. The only way to really counter «rule-by-law» through surveillance and state control/abuse in the name of countering cybercrime is to steadily grow the group of countries committed to human rights and safeguards in cyberspace and then persuade them not to collaborate with countries which do not really respect the rule of law.

Privacy has therefore been one of the main casualties in the undeclared cyberwar at the same time that many have been reluctant to consider or even discuss the alternatives to cyberpeace. As we witness more and more attempts at creating laws which require the localisation of data, we are also seeing the creation of a second paradox which is growing out of the attempts to impose 19th century notions of sovereignty onto cyberspace. So, in a cyberspace which currently knows no borders and has problems of jurisdiction in the absence of an agreed international law which governs it, the attempts of several states to either assert their control over «their bits of cyberspace» or to ensure that it can be cut off from the rest of the world whenever they please, will lead to just that i.e. a breakdown of cyberspace as we know it today. For if the group of countries which are genuinely committed to the rule of law and the protection of rights in cyberspace will get to the point where they decide that being connected to the other group of countries is more trouble than it is worth, then the logical if extreme alternative would be to cut the fibre-optic cables linking the two groups of countries together because the values they really adhere to are fundamentally incompatible. Paying lip-service to human rights does not fool anybody if you run an autocratic state where the

internet is an important instrument of control. The rest of the world will notice and will, sooner or later, ostracise you to the group of nations that shares your values of «rule-through-law» as opposed to «rule-of-law».

The development of international and national law in the scenarios depicted above is going to need many lawyers with expertise in technology. As we celebrate some thirty-five years of his contribution to scholarship, it is clear that our friend Erich Schweighofer still has a lot to give whenthinking and teaching about Technology Law. In a world where our life expectancy has happily increased significantly, we dare hope that he will continue to do so well into the future until it is time, in 15 years or so, to prepare the festschrift for his fiftieth anniversary of his contributing to the subject. *Ad multos annos!*