"The Global Panopticon" – Mass surveillance and data privacy intrusion as a crime against humanity?

Michael Bohlander[*]

> *And do not fear those who kill the body but cannot kill the soul. Rather fear him who can destroy both soul and body in hell.*
>
> Matthew 10:28[1]
>
> *Visibility is a trap.*
>
> Michel Foucault, Discipline and Punish, 1975
>
> *The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*
>
> European Court of Human Rights, *Klass & others v Germany*, para. 49, 1978

L 1 "Fear Eats the Soul"[2]

The Gospel of St Matthew warned people not to get their priorities wrong: The soul was considered more important than the body and hence they should fear God more than men, for he was the only one who could also destroy man's soul. However, about two millennia later it seems God is facing serious competition in that department. George Orwell's "1984" and many similar accounts published since the last century, as well as state regimes based on the exploitation of such ideas, have shown that Man is capable of destroying, or at the very least seriously crippling, the soul of his fellow human beings by making them afraid of the consequences of saying what they think. If such a regime of fear goes on long enough and is supported by sufficiently negative stimuli in the case of non-compliance, the vast majority of us will begin to suffer from a Pavlov reflex and become conditioned to not even think what we think.[3] One powerful negative stimulus is

---

[*] International Co-Investigating Judge, Extraordinary Chambers in the Courts of Cambodia (ECCC); Judge, Kosovo Specialist Chambers; Chair in Comparative and International Criminal Law, Durham Law School (UK). The views expressed are solely those of the author and do not represent the opinion of the United Nations, the ECCC, the Royal Government of the Kingdom of Cambodia, EULEX or the Kosovo Specialist Chambers. – The author would like to thank Otto Lagodny, Phillip Louis Weiner, and Caroline Fournet for comments on an earlier draft. All remaining errors are the author's. All webpages cited were last accessed on 12 April 2017, the date this chapter was finished.

[1] English Standard Version.

[2] English translation of the title of the film *Angst essen Seele auf* by Rainer Werner Fassbinder, from 1974; see http://www.imdb.com/title/tt0071141/.

[3] On the self-censoring effect on our understanding of privacy in the new digital age, see my Blood Music on Darwin's Radio – Musings on social network data transparency, cyborg technology, science fiction and

provided by making sure that any and all relevant data about each and every one of us are known to those who a) have a major political or economic stake in what we think, as well as b) the political or economic power to enforce their own position.

In the early years of this century, the activities of the American NSA and its British sister organisation GCHQ – like those of their counterparts of every ideological shade across the globe – in their "war on terror" have made it amply evident that they are capable of creating a culture of fear even among those who do not engage in any sort of terrorism-related activities. The 2016 UK Tory Government's Investigatory Powers Act, also called a "Snooper's Charter", [4] is an expression of the lengths conservative governments in particular will go to in order to acquire a blanket power of bulk data acquisition unrelated to any specific allegations against the individuals whose data are being syphoned off, and their intention to do away with encryption protections.[5] Coupled with their ability to deploy real-world instruments such as, for example, drones, the same powers who preach the water of the sacrosanct nature of human rights, democracy and the rule of law to others, drink the wine of the torture or extra-judicial killings of those they deem outside the sphere of effective human rights protection, by creating new or previously unknown classes of adversaries, for example, "enemy combatants", [6] or by considering a separate criminal law for them, the so-called *Feindstrafrecht* or "criminal law of the enemy"[7].

The ancient ideal of open democracy is increasingly in danger of succumbing to the stifling overgrowth of executive control of sensitive knowledge about the very foundations of our society, something the Germans call *Herrschaftswissen*, a concept that has been translated as "hegemonic knowledge", [8] and which is seen as unfit for undiluted consumption by the wider body politic, mostly on the basis that such knowledge would harm the national security and endanger public peace.[9] The report of 23 September 2014 of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism states:

> The States engaging in mass surveillance have so far failed to provide a detailed and evidence-based public justification for its necessity […]. Viewed from the perspective of article 17 of the Covenant, this comes close to derogating from the right to privacy altogether in relation to digital communications. For all these reasons, mass surveillance

---

the future perception of human rights, 2013 Global Community Yearbook of International Law and Jurisprudence, 2014, 45-64.

[4] Text at www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[5] See for the UK the criticism by Apple CEO Tim Cook in The Guardian, 21 December 2015, *Apple calls on UK government to scale back snooper's charter* at www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill; and www.computerworlduk.com/news/security/tim-cook-says-there-isnt-a-trade-off-between-security-and-privacy-3632367/ and for the US the recent dispute between the FBI and Apple the references at www.computerworlduk.com/galleries/security/apple-vs-fbi-in-quotes-bill-gates-google-microsoft-edward-snowden-3635572/#2.

[6] See www.cfr.org/international-law/enemy-combatants/p5312.

[7] In Germany, for example, the main proponent of this concept is Günther Jakobs; see his "Zur Theorie des Feindstrafrechts" in Henning Rosenau/Sanyun Kim (eds), *Straftheorie und Strafgerechtigkeit*, Augsburger Studien zum Internationalen Recht, 2010, vol. 7, 167–82; an English translation is available online at www.lawlib.utoronto.ca/bclc/crimweb/foundation/Dubber%20Appendix%20D.PDF.

[8] Translation suggested at www.passagen.at/cms/index.php?id=94&L=1

[9] The German Home Secretary de Maizière stated in November 2015 that making public some of the reasons for cancelling an international football game in Hannover due to an alleged terrorist threat would "disturb" (*verunsichern*) the public; see Stefan Kuzmany, Der Spiegel, 18 November 2015, *Was wir nicht wissen wollen*, at www.spiegel.de/politik/deutschland/de-maiziere-zu-laenderspiel-absage-wuerde-die-bevoelkerung-verunsichern-a-1063439.html.

> of digital content and communications data presents a serious challenge to an established norm of international law. [...] [T]he very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy. Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. [10]

Democracy as a principle ceases to function as soon and inasmuch as the same information is not available to all participants to the discussion – not mentioning their ability to properly digest information of varying degrees of complexity. That was in principle always the case and to that extent, the democratic ideal was always a fragile concept tinged with a *soupçon* of also being an illusion. However, in our age of globalisation the interconnectedness of geopolitical interests, whether parallel or antagonistic, and the unprecedented and steadily increasing power of data processing systems together with the ensuing potential for the widespread and systematic repression, distortion or for any other form of abuse of information concentrated in the hands of a very few people, the ideal is in danger of being absorbed by the *real-politik* cynicism of the powerful on the one hand, and by the increasing aggressiveness in the reactions of the powerless[11] borne of the realisation that all the "democracy-speak" may just have been another "opium for the masses", on the other. The rise since 2010 of unabashedly public populist right-wing politics in Europe, the USA , Russia, Turkey etc. are a symptom of that danger. As I pointed out elsewhere,[12] however, the vast majority of individual data owners are increasingly guilty of contributory negligence by making a mass of sometimes intimate data available freely on social media platforms etc. The combined impact of the above-mentioned data "feeding frenzy", the smorgasbord of data often voluntarily offered by the users of social networks and the apparent increasing disinterest in political engagement and activism among the general population have yet to be fully studied.

This paper will argue that data collection and (ab-)use these days[13] are endemic and occur in a widespread and systematic manner and more often than not based on the policy of governments or – increasingly – of big multinational IT companies and networks such as Google, Facebook etc.[14] It will posit that they affect mainly civilians on a grand scale, whether for discriminatory reasons or simply indiscriminately, and have the potential for seriously violating some fundamental human rights, namely the rights to privacy and as a knock-on effect, the rights to freedom of speech and freedom of belief.[15] The practice of such wholesale data gathering should thus have all the hallmarks for being a contender to a new category of crime against humanity (CAH). Traditionally, CAH and other international crimes have been focussing either on, firstly, distinct violations of certain rules applicable to the conduct of armed hostilities, or, secondly, on physical or mental harm or damage, i.e. violations of the body, the mind or

[10] UN Doc. No. A/69/397 at para 18.

[11] See the rise of activist groups such as Occupy, ATTAC, or PEGIDA.

[12] See above (n. 3).

[13] In fact, latest data show that the practice had already been well established in the 1990s at least for the GCHQ; see The Guardian, 21 April 2016, *UK spy agencies have collected bulk personal data since 1990s, files show* at http://gu.com/p/4tfde?CMP=Share_iOSApp_Other.

[14] See on the interplay between data gathering by Facebook and governmental intrusion through the lens of a spiral of silence, Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring,* (2016) 93 Journalism and Mass Communication Quarterly, 296 – 311.

[15] See for the worsening trend the article by Timothy Garton Ash in The Guardian, 12 May 2016, *Free speech is under attack, from Beijing to Istanbul*, http://gu.com/p/4j6xq?CMP=Share_iOSApp_Other.

of property in the wider sense, as the basis for criminal liability, even if the means used to bring about such consequences are situated in cyber space, i.e. through cyber warfare. Analysed through the Foucauldian lens of hidden technologies of governmentality, their seriousness will be exposed.

Most often, those two categories overlap to a large extent but not necessarily, since some of the rules of warfare are intended to provide for a degree of control over the conduct of military actions purely in the interest of allowing for the chance of a resumption of peaceful relations between the parties after a conflict has ended. Hence there is a need of maintaining a minimum standard of humane conditions during such conflicts, if that can be said to be a realistic option at all. The protection of the symbols of the Red Cross and Red Crescent may be seen as one example. However, with the rapid development of information technology and its virtually unchecked use for unilateral or multilateral intelligence gathering purposes by many governments and major corporations, a new victim may finally have appeared on the scene, namely the above-mentioned bundle of fundamental political rights, the free exercise of which is a non-negotiable and crucial component of the democratic process.

In other words, the violation of these rights may no longer be a mere tool in order to violate the traditional target rights related to physical and mental well-being, but represent a violation of a distinct new target right in and of itself. It is apposite to state at this point that the effects on the traditional and the new target rights do not exclude each other: It may still be feasible to construct a violation of physical or mental well-being as an unavoidable and/or foreseeable consequence of rampant intelligence gathering and use of information obtained in that way.

L 1 The development of government and business information politics on data collection, storage, use and sharing

The recent NSA and GCHQ scandals and the related Snowden affair have brought it to the wider public's attention that for years a data gathering campaign by national intelligence services on an unprecedented scale has been progressing in the shadows. The report by Ben Emmerson, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism sets out in detail the nature and magnitude of these mass surveillance efforts[16]. They are well-known thanks to the efforts of a few insider whistle-blowers such as Snowden and dedicated fearless journalists, and thus need no closer description here. The justification for all of these intrusions into individuals' privacy is the war against terror and organised crime and the professed need to have such sweeping powers to counter the IT capacities of the terrorists and organised criminals.

There is little doubt that there is a conflict on the national and the international stages between the proponents of a judicially protected rights-based approach versus the parliamentary and governmental supporters of an executive-effectiveness-driven stance. The problem increases in states with a strong conservative governing party and a weak or non-existing liberal opposition; in this context, the recent rise in nationalistic and right-wing parties and governments in Europe and the United States must cause more than political unease. The UN Human Rights Council in its Resolution 28/16 of 24 March 2015,[17] which established the office of the UN Special Rapporteur on the right to

[16] UN Doc. No. A/69/397 at paras 20 ff.
[17] UN Doc. No. A/HRC/28/L.27, p. 3.

privacy, and guided by General Assembly Resolution 69/166,[18] expressed its deep concerns over the threats caused by modern data technology and the largely uncontrolled uses it can be put to, and it chose to lay down a few policy ground rules for the way forward. The Council stated that it

> *[r]eaffirms* the right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights;
> *Recognizes* the global and open nature of the Internet and the rapid advancement in information and communications technology as a driving force in accelerating progress towards development in its various forms;
> *Affirms* that the same rights that people have offline must also be protected online, including the right to privacy […][19]

The first report by the newly installed Special Rapporteur of 8 March 2016[20] contained the following conclusions:[21]

> The tensions between security, corporate business models and privacy continue to take centre stage but the last twelve months have been marked by contradictory indicators: some governments have continued […] to take privacy-hostile attitudes while courts world-wide […] have struck clear blows in favour of privacy and especially against disproportionate, privacy-intrusive measures such as mass surveillance or breaking of encryption.
> There are strong indicators that Privacy has become an important commercial consideration with some major vendors adopting it as a selling point. If there is a market for privacy, market forces will provide for that market. […] [C]onsumers world-wide are increasingly aware of risks to their privacy and the fact that they will increasingly choose privacy-friendly products and services over ones which are privacy-neutral or privacy-unfriendly;
> While some governments continue with ill-conceived, ill-advised, ill-judged, ill-timed and occasionally ill-mannered attempts to legitimise or otherwise hang on to disproportionate, unjustifiable privacy-intrusive measures such as bulk collection, bulk hacking, warrantless interception etc. other governments led, in this case by the Netherlands and the USA have moved more openly towards a policy of no back doors to encryption. […]

However, the 2016 litigation[22] in the United States based on the 1789 *All Writs Act*[23] concerning the FBI's request that Apple provide it with a backdoor software for its

---

[18] UN Doc. No. A/69/166.
[19] UN Doc. No. A/HRC/28/L.27, 3.
[20] Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, UN Doc. No. A/HRC/31/64 (advance unedited version).
[21] Ibid., at paras 48 – 52.
[22] Judge Orenstein, US District Court, Eastern District of New York, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, Memorandum and Order of 29 February 2016, Docket no. 15-MC-1902 (JO) – available online at www.eff.org/.../applebrooklyn-2.29.16order.pdf. – Judge Orenstein denied the FBI's motion and held at p. 49 of the order: "How best to balance those interests is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago. But that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive. It would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate, and ended it, in 1789." Judge Orenstein had already rejected an *ex parte* application by the FBI earlier in 2015; see *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015). – The Central District Court of California had, however, entered an *ex parte* order against Apple on 16 February 2016 "to perform even more burdensome and involved

iPhone, and President Obama's remarks[24] about the justifiability of that request in principle – which he evidently even extended to the question of mere tax evasion[25] – puts a question mark over the practical implementation of this policy, at least by the US.

I. 2 Government intrusion

Government intrusion has reached international courts several times in recent decades. Data surveillance issues are not merely a matter for the domain of human rights courts proper, but have found their way into the wider application of EU law, for example. We will look only at some of the most recent cases to illustrate the problem for our purposes. Though not mainly a human rights court, the Court of Justice of the European Union (CJEU) in the case of *Digital Rights Ireland* declared an EU Directive on data retention to be in violation of EU law on 8 April 2014 (see also below on the domestic fate of the German law implementing the Directive). [26] Referring to the related CJEU case of *Schrems*[27] and the ECtHR case of *Zakharov*[28], UN Special Rapporteur Cannataci, in addition to the statements from his report excerpted above, pointed out[29] two fundamental passages of their holdings, namely that in *Schrems* the CJEU stated, at para. 94,

> [i]n particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as *compromising the essence* of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter" [emphasis added],

and in *Zakharov,* at para. 270, the ECtHR opined that

> [t]he Court considers that the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system […], the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to

---

engineering than that sought in the case currently before this Court – *i.e.*, to create and load Apple-signed software onto the subject iPhone device to circumvent the security and anti-tampering features of the device in order to enable the government to hack the passcode to obtain access to the protected data contained therein". See *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M) (the "*California*" action), Order Compelling Apple, Inc. to Assist Agents in Search (C.D. Cal. Feb. 16, 2016).

[23] 28 U.S.C. § 1651(a) as amended on 24 May 1949 reads: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

[24] See Philip Elmer-DeWitt, *Here's What Obama Said at SXSW About Apple vs. FBI*, 12 March 2016, at http://fortune.com/2016/03/12/obama-sxsw-apple-vs-fbi/.

[25] He said: "What mechanisms do we have available that even do simple things like tax enforcement? Because if in fact you can't crack that at all, and government can't get in, then everybody's walking around with a Swiss bank account in their pocket. So there has to be some concession to the need to be able to get to that information somehow." – ibid.

[26] Cases C-293/12 and C-594/12 – online at http://curia.europa.eu/juris/documents.jsf?num=C-293/12.

[27] Case C-362/14 – online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

[28] Application 47143/06 – online at http://hudoc.echr.coe.int/eng?i=001-159324.

[29] A/HRC/31/64 at paras 32 and 37.

> abuse. The *need for safeguards against arbitrariness and abuse* appears therefore to be particularly great [emphasis added].[30]

On 12 January 2016, the ECtHR consolidated its stance in *Szabó and Vissy v Hungary*[31] and criticised the absence of meaningful[32] judicial control of the intelligence operations, and especially the fact that a politically appointed government minister as the head of the relevant branch of the executive made the decision permitting the surveillance measures. The Court said – at para. 53 – that the mere existence of the relevant domestic legislation involved a menace which struck at the freedom of communication between users of the postal and telecommunication services. Citing the technological advances since the *Klass and Others* case[33] from 1978, it held that "the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely". It added that "[i]n the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods … has been accompanied by a simultaneous development of legal safeguards…".[34] It was clearly not impressed by the Hungarian government's arguments, stating that "the possibility occurring on the side of Governments to acquire a detailed profile … of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. … The guarantees required by the extant Convention case-law on interceptions need to be enhanced […]. However, it is not warranted to embark on this matter in the present case, *since the Hungarian system of safeguards appears to fall short even of the previously existing principles*" [emphasis added]. [35] Referring to the standards required for allowing such highly intrusive measures, the ECtHR reminded Hungary of the need for a strict interpretation of the principle of necessity.[36] The Court made very plain its disdain for

---

[30] In this context it is revealing that the former head of the German Intelligence Service, the *Bundesnachrichtendienst* (BND), Gerhard Schindler, told a parliamentary commission of inquiry that the BND's division for "technical intelligence" (*technische Aufklärung*) had used the NSA selectors provided to them with almost no effort at scrutiny as to their lawfulness under German law, and that the division had moved "beyond control". He had, before his dismissal, taken the unprecedented step of tasking a private consultants firm, Roland Berger, with examining the processes in the division and making recommendations for their improvement. See Tagesschau, 12 May 2016, *BND engagiert Beraterfirma Roland Berger* at www.tagesschau.de/inland/bnd-307.html. The Federal Data Protection Ombudsperson, Andrea Voßhoff, had declared the BND's surveillance practices as unconstitutional in February 2016. See Georg Mascolo, Tagesschau, 24 February 2016, *Abhörpraxis des BND "nicht verfassungskonform"* at www.tagesschau.de/inland/datenschutz-bnd-abhoerpraxis-101.html.

[31] Application no. 37138/14, Judgment of 12 January 2016 – A request for referral to the Grand Chamber was pending at the time of writing.

[32] The question is, of course, whether there can ever be any meaningful judicial control when the only source of information is the very same over which the control is to be exercised.

[33] *Klass and Others v. Germany*, 6 September 1978, Series A no. 28.

[34] See above (n 31), at para 68.

[35] ibid. at para 70.

[36] ibid. at paras 73 to 75: "[…] given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, […] the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary […] for the safeguarding the democratic institutions and, moreover, […] for the obtaining of vital intelligence in an individual operation. … A central issue common to both the stage of authorisation of surveillance measures and the one of their application is the absence of judicial supervision. The measures are authorised by the Minister in charge of justice upon a proposal from the executives of the relevant security services … [*scil.* the TEK] … which for its part, is a dedicated tactical department within the police force …. For the Court, this supervision, eminently political … but carried out by the Minister of Justice who appears to be formally independent of both the TEK and of the Minister of

the political executive option that had been chosen.[37] It held as a conclusion, that a violation of Article 8 ECHR had occurred, "[g]iven that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones.[38]

The Advocate General at the CJEU in his opinion of 19 July 2016 in a joint follow-up case on bulk data collection and retention to *Digital Rights Ireland*, namely *Tele2 Sverige AB et al.*, [39] while accepting that bulk collections and data retention regimes are in principle not incompatible with EU law, nonetheless argued that they needed to adhere to a closely circumscribed set of protective criteria. In particular he took the standard set by *Digital Rights Ireland* on the serious level of infringement caused by data retention obligations on online service providers as self-evident and no longer in need of further elucidation[40] and any intrusion was not justified by "[…] the combating of ordinary offences and the smooth conduct of proceedings other than criminal proceedings […]. The considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences and in the conduct of proceedings other than criminal proceedings".[41]

Applying the principles of proportionality and strict necessity, he exhorted the national courts not to "simply verify the mere utility of general data retention obligations, but rigorously verify that no other measure or combination of measures,

---

Home Affairs … is inherently incapable of ensuring the requisite assessment of strict necessity with regard to the aims and the means at stake."

[37] ibid. at paras 76 – 77: "[Although] the Government's argument according to which a government minister is better positioned than a judge to authorise or supervise measures of secret surveillance […] might be arguable from an operational standpoint, the Court is not convinced […] when it comes to an analysis of the aims and means in terms of strict necessity. [T]he political nature of the authorisation and supervision increases the risk of abusive measures. … For the Court, supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees."

[38] ibid. at para 89. – Strong as that language may sound, the majority's final practical application of its principles was not enough for Judge Pinto de Albuquerque, who criticised his brethren in a separate but concurring opinion for departing from the supposedly greater stringency of the *Zakharov* test of the Grand Chamber regarding the degree of suspicion required before measures are authorised, and declared at its para. 35: "Yet while the tone is right, the substance of the judgment risks failing to allay entirely the serious dangers for citizens' privacy, the rule of law and democracy resulting from such a legal framework. Worse still, the choices made by the Chamber introduce a strong dissonant note in the Court's case-law. Paragraph 71 of the judgment departs clearly from paragraphs 260, 262 and 263 of *Roman Zakharov* and paragraph 51 of *Iordachi and Others v. Moldova*, since the Chamber uses a vague, anodyne, unqualified "individual suspicion" to apply the secret intelligence gathering measure, while the Grand Chamber uses the precise, demanding, qualified criterion of "reasonable suspicion". Judicial authorisation and review is watered down if coupled with the Chamber's ubiquitous criterion, because any kind of "suspicion" will suffice to launch the heavy artillery of State mass surveillance on citizens, with the evident risk of the judge becoming a mere rubber-stamper of the governmental social-control strategy. A ubiquitous "individual suspicion" equates to overall suspicion, i.e., to the irrelevance of the suspicion test at all. In practice, the Chamber condones *volenti nolenti* widespread, non-(reasonable) suspicion-based, "strategic surveillance" for the purposes of national security, in spite of the straightforward rebuke that this method of covert intelligence gathering for "national, military, economic or ecological security" purposes received from the Grand Chamber in *Roman Zakharov*. Only the intervention of the Grand Chamber will put things right again."

[39] Cases C-203/15 and C 698/15, Opinion of 19 July 2016 – online at http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=EN

[40] ibid at para 128.

[41] ibid at para 172.

such as a targeted data retention obligation accompanied by other investigatory tools, can be as effectiveness in the fight against serious crime."[42] He emphasised that empirical research had shown that the ubiquitous invocation of necessity in this context was far from justified.[43] He rejected the argument advanced by some parties, among them Germany, that a lack in protection under one part of the criteria could be made up for by a higher level of protection under others, the so-called "communicating vessels" approach; in his view, *all* criteria were mandatory minimum thresholds and could not be traded off against each other.[44] He was rather outspoken in his observations on the dangers of bulk data collection and data retention.[45]

The CJEU in its related judgment of 21 December 2016[46] affirmed its previous stance and followed the Advocate-General's critical view.[47] Under the regimes of the ECHR, arguably the most developed and sophisticated international human rights framework these days, and under the almost equally advanced CJEU jurisprudence, two systems that may be taken as indicative of the judicial attitude on the international level, major concerns exist about the current state of affairs and have, for example, been taken up as representative of the wider picture under general international law by the UN Special Rapporteur.

[42] ibid at para 209.
[43] ibid.
[44] ibid at para 244.
[45] "The disadvantages of general data retention obligations arise from the fact that the vast majority of the data retained will relate to persons who will never be connected in any way with serious crime. […] [I]n an individual context, a general data retention obligation will facilitate equally serious interference as targeted surveillance measures, including those which intercept the content of communications. Whilst the severity of such individual interference should not be underestimated […] the specific risks engendered by a general data retention obligation become apparent in the context of 'mass' interference. [B]y contrast with targeted surveillance measures, a general data retention obligation is liable to facilitate […] interference affecting a substantial portion, or even all of the relevant population. [T]he risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications […] 'metadata' facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not. [T]here is nothing theoretical about the risks of abusive or illegal access to retained data. The risk of abusive access on the part of competent authorities must be put in the context of the extremely high number of requests for access […] Tele2 Sverige has stated that it was receiving approximately 10,000 requests monthly, a figure that does not include requests received by other service providers operating in Sweden. In so far as the United Kingdom […] is concerned, […] an official report […] records 517,236 authorisations and 55,346 urgent oral authorisations for 2014 alone. The risk of illegal access, on the part of any person, is as substantial as the existence of computerised databases is extensive." – Ibid., paras 252, 254 – 256, 259 – 260.
[46] Joined Cases C-203/15 and C-698/15, Judgment of 21 December 2016 – online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203.
[47] Ibid. disposition after para. 134.: "Article 15(1) of Directive 2002/58/EC […], read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication [and] […] as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."

L 2 Non-state actor intrusion

The state sector is not the only actor in the massive use of data. The private sector is almost as voracious as the authorities in not only accumulating, but also commercialising data for private profit. Sometimes it acts on behalf of the government, sometimes for purely private purposes.[48] The actors range from internet companies and social media networks such as Google, Facebook and Twitter, to insurance companies, medical services and employers, who all desire access to the private data of their customers.

The Special Rapporteur, Ben Emmerson, had this to say in his 2014 report regarding the former:

> States increasingly rely on the private sector to facilitate digital surveillance. This is not confined to the enactment of mandatory data retention legislation. Corporates have also been directly complicit in operationalizing bulk access technology through the design of communications infrastructure that facilitates mass surveillance. Telecommunications and Internet service providers have been required to incorporate vulnerabilities into their technologies to ensure that they are wiretap-ready. The High Commissioner for Human Rights has characterized these practices as "a delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of self-regulation and cooperation" (see A/HRC/27/37, para. 42). The Special Rapporteur concurs with this assessment. In order to ensure that they do not become complicit in human rights violations, service providers should ensure that their operations comply with the Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011[…].[49]

Special Rapporteur Cannataci in his three reports to the Human Rights Council[50] and the UN General Assembly[51] also addressed this matter, although he has so far put more of an emphasis on government-sponsored surveillance, where incidentally, he still held serious concerns and saw signs of evasiveness by some states and even attempts at dissuading him from looking into the matter too deeply.[52]

Microsoft in particular has an agenda of enabling the maximum amount of data sharing, as Mic Wright has described in a post[53] on MS Windows 10 of 29 July 2015 in an

---

[48] See, for example, The Guardian, 18 January 2017, *Home Office refuses to enforce privacy code on NHS staff using video* at www.theguardian.com/society/2017/jan/18/home-office-refuses-to-enforce-privacy-code-on-nhs-staff-using-video?CMP=Share_iOSApp_Other; and John Harris, The Guardian, 20 January 2017, *They call it fun, but the digital giants are turning workers into robots, at* www.theguardian.com/commentisfree/2017/jan/20/digital-giants-workers-robots-film-employee-monitoring-the-circle?CMP=Share_iOSApp_Other

[49] ibid at para 57. His more recent report of 22 February 2016 to the Human Rights Council - A/HRC/31/65 – primarily focussed on data issues in the context of the prevention of extremist violence, although at para. 39 he did voice a warning that the regulation of the internet discourse in the context of suppressing extremist propaganda may entail separate restrictions on the free debate of this vital agenda that may lead to researchers, journalists etc. being monitored for bona fide work and included in an overly broad definition of the topic.

[50] A/HRC/31/64 of 8 March 2016 and A/HRC/34/60 of 24 February 2017.

[51] A/71/368 of 30 August 2016.

[52] See A/HRC/34/60, for example, at paras 13, 19 – 29, 42.

[53] Mic Wright, The Next Web, 29 July 2015, *The Windows 10 privacy issues you should know about*, 29 July 2015, at https://thenextweb.com/microsoft/2015/07/29/wind-nos/#.tnw_SvgDxb9G: "[T]here are a few unsettling things nestling in there. […] Microsoft has grabbed some very broad powers to collect things you do, say and create while using its software. Your data won't be staying on your computer, that much is for sure. […] Sign into Windows with your Microsoft account and the operating system immediately syncs settings and data to the company's servers. That includes your browser history, favorites and the websites you currently have open as well as saved app, website and mobile hotspot

illustration of what the individual average end user is up against. Anca Chirita, who advocates the innovative use of competition law to tackle private actors' handling of data, has recently tracked the privacy regimes of a number of providers and social media networks and found a wide variety of more or less unobtrusive mechanisms aimed at collecting data and sharing them as freely as possible with third parties.[54]

In essence, the use of data by non-state actors for commercial interests poses a similar, if not in the long run worse, threat as that conducted by the government. How do we move from the description of the overall situation to a legal characterisation as a CAH ? We shall attempt to carve out some main criteria in the next section.

L 1 Transposing the data abuse scenario into the international law of crimes against humanity (CAH)

L 2 Finding a violated right

In the light of the grave and well-documented concerns held by both international courts and experts set out above, it should not be subject to serious debate that there is a – so far somewhat admittedly ill-defined – red line which is regularly being crossed by state and non-state actors when it comes to collecting private data. Traditionally, arising out of the historical development of CAH and the related laws of armed conflict, the primary aim of the law on CAH had always been the protection against direct physical attacks on life and limb, personal liberty and property in one way or another. CAH, much like war crimes, attach liability to individuals and not to states. However, especially in the context of the CAH of persecution and other inhumane acts, inroads have over time been made into a wider understanding of rights that may be violated, including serious psychological harm.[55] Not least in the context of cyber warfare, it is not difficult to imagine that data abuse can also be used as an instrument for the purpose of violating

---

passwords and Wi-Fi network names and passwords. You can deactivate that by hopping into the settings of Windows, but I'd argue that it should be opt-in rather than on by default. Many users won't get round to turning it off, even though they would probably want to. […] Turn on Cortana, the virtual assistant, and you're also turning on a whole host of data sharing: To enable Cortana to provide personalized experiences and relevant suggestions, Microsoft collects and uses various types of data, such as your device location, data from your calendar, the apps you use, data from your emails and text messages, who you call, your contacts and how often you interact with them on your device. Cortana also learns about you by collecting data about how you use your device and other Microsoft services, such as your music, alarm settings, whether the lock screen is on, what you view and purchase, your browse and Bing search history, and more." Lots of things can live in those two words "and more." Also note that because Cortana analyzes speech data, Microsoft collects "your voice input, as well as your name and nickname, your recent calendar events and the names of people in your appointments, and information about your contacts including names and nicknames." […] Microsoft will collect information "from you and your devices, including for example 'app use data for apps that run on Windows' and 'data about the networks you connect to.'" […] Windows 10 generates a unique advertising ID for each user on each device. That can be used by developers and ad networks to profile you. Again, you can turn this off in settings, but you need to know where to look: […] Microsoft can disclose your data when it feels like it. This is the part you should be most concerned about: Microsoft's new privacy policy […] is very loose when it comes to when it will or won't access and disclose your personal data"

[54] Anca Chirita, The Rise of Big Data and the Loss of Privacy. in *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?*. In Mor Bakhoum., Beatriz Gallego Conde, Mark-Oliver Mackenordt,. & Gintare Surblyte. (eds.) . (Berlin/Heidelberg, Springer, 2017) – pre-publication pdf available at https://ssrn.com/abstract=2795992

[55] For an overview of the case law see Otto Triffterer/Kai Ambos, The Rome Statute of the International Criminal Court – A Commentary, 3rd ed., (C.H. Beck et al, Munich et al, 2016) (hereinafter Triffterer/Ambos), Art. 7 mn. 142.

any of the above-mentioned rights and interests. Given the international customary law's progressively disjunctive view of CAH and the need for them to be factually embedded in an armed conflict, it has long been recognised that they may be committed in peacetime as well; in fact, that is one of the major distinguishing features of CAH as opposed to the historically preceding concept of war crimes. That characteristic is what makes the idea of CAH such an appealing lens through which to interrogate the question of individual criminal responsibility for abuse of powers of or opportunities for data collection from private citizens and, again, possibly legal entities. These abuses happen often, or even mainly, in the absence of an armed conflict, although they may, of course, occur in the context of hostilities, too. However, the instrumental role of data abuse in the context of CAH is not what interests us here: The much more conceptually interesting question is whether the right to privacy as expounded in the above-mentioned decisions of international courts and reports of international experts can or should give rise to liability as a violation of a direct target right itself. When we are pursuing the question of whether privacy can be conceptualised as a new target right for CAH, this may take two forms: Firstly, inclusion as a target right in existing CAH such as persecution and other inhumane acts, secondly as a new category of CAH altogether.

It is immediately apparent that the inclusion into persecution seriously limits the reach of privacy as the target right, because persecution requires a discriminatory element, something which is almost by definition – albeit not necessarily – absent in the scenarios of indiscriminate surveillance and data collection. Other inhumane acts do not require this discriminatory element, yet their concept might seem too closely bound to – often subconsciously – emotionally charged equations to same-degree violations of the traditional protected interests of life and limb, personal liberty and mental harm; indeed, as far as the law of the ICC is concerned, Art. 7(1)(k) ICC-Statute restricts the effect to an impact equating to serious physical or mental injury. Concerns have also been voiced about the specificity of the definition under customary international law from the point of view of the *nullum crimen* principle.[56]

Despite these limitations, it is nonetheless useful to look at the rights and protected interests that have so far been included under persecution in particular, because that CAH explicitly addresses an open-ended category of "fundamental rights". Persecution requires the intentional and severe deprivation of fundamental rights contrary to international law". The General Comment No. 24 of the UN Human Rights Committee from 1994[57] would seem to allow the conclusion that this category is certainly triggered when it comes to peremptory norms in the context of the ICCPR.[58]

---

[56] See Kai Ambos, Treatise on International Criminal Law, vol. II, (OUP, 2014), (hereinafter Ambos, Treatise) 115 f. - There remains the added problem that in the exercise of charging or convicting for multiple legal characterisations based on the same facts, other inhumane acts may routinely be considered as a prime candidate for exclusion under the different-element test traditionally espoused by international criminal courts.

[57] CCPR General Comment No. 24: Issues Relating to Reservations Made upon Ratification or Accession to the Covenant or the Optional Protocols thereto, or in Relation to Declarations under Article 41 of the Covenant *Adopted at the Fifty-second Session of the Human Rights Committee, on 4 November 1994, CCPR/C/21/Rev.1/Add.6, General Comment No. 24. (General Comments).*

[58] ibid para 8: "Accordingly, provisions in the Covenant that represent customary international law (and a fortiori when they have the character of peremptory norms) may not be the subject of reservations. Accordingly, a State may not reserve the right to engage in slavery, to torture, to subject persons to cruel, inhuman or degrading treatment or punishment, to arbitrarily deprive persons of their lives, to arbitrarily arrest and detain persons, *to deny freedom of thought, conscience and religion*, to presume a person guilty unless he proves his innocence, to execute pregnant women or children, to permit the advocacy of national, racial or religious hatred, to deny to persons of marriageable age the right to marry, *or to deny to minorities the right to enjoy their own culture, profess their own religion, or use their own language*. And

What is interesting for our discussion is the nature of the highlighted rights as civil and political rights, rather than rights to personal inviolability of body, mind or liberty. And while they are not listed in General Comment No. 24 because it deals with reservations to the ICCPR especially in the face of peremptory norms, Articles 17(1) and (2), 18(1) and (2) and 19(1) and (2) ICCPR would naturally qualify as foundations for a protection against mass surveillance practices, because their mention in the ICCPR squarely puts them in the bracket of fundamental rights under international law. All of those rights naturally are subject to a qualifying clause that allows encroachments for the sake of overriding public interests. Yet, the link between privacy, freedom of opinion and expression as well as freedom of thought, conscience and religion is strikingly obvious. Instances of recognition by international tribunals include social annex aspects to personal freedom such as freedom to exercise a profession, right to citizenship, participation in national life, or family life.[59] From there it is but a small step to think about the privacy rights as equating those already in the existing catalogue.

L 2 Demonstrating equal severity – A Foucauldian perspective

One criterion that needs to be borne in mind when creating a new target right either within persecution or as a distinct CAH, is the equal severity element, i.e. that the new target right violation must be considered as equally serious as the classic ones, regarding life, limb, freedom and property, all of which are more or less directly linked to the body and the connected physical world. To many, this may not appear immediately obvious when talking about an abstract right such as privacy, which can be seen as a cluster of different aspects, of which data privacy seems even more abstract from the body than the traditional privacy aspects such as family life, (intimate) social interaction including sexual preferences, protection of one's home etc. It is helpful in this regard to analyse the issue of equal severity through the lens of Foucauldian discourse, and in particular his views on the hidden technologies of governmentality inherent in surveillance as an instrument of not merely collecting data as an end in itself, but of collecting them as a means to an end, a mere precursor to controlling the behaviour of their source, human beings, and thus their body (and soul), with the means of control being either external application in the guise of law enforcement, or worse, full internalisation by triggering a course of seemingly voluntary self-subjection by the very person from whose individual sphere the data are being culled, either by knowing alignment with the underlying political agenda ("I have nothing to hide") or through the subconscious acceptance of the hidden framework's agenda. The latter can be, and often is, hidden, for example, in workplace proceduresbased on state-sponsored policies or private commercial environments utilising the neo-liberal aim of objectification of the human, achieved through the adoption, as morally valuable, by the individual of the idea of self-responsibility for competitive striving to produce objectively measurable outputs.[60]

In his seminal work, *Discipline and Punish* – in its original French and in our context much more tellingly entitled *Surveiller et Punir* –, Michel Foucault argues that

---

while reservations to particular clauses of article 14 may be acceptable, a general reservation to the right to a fair trial would not be [my emphasis]". – In the same sense Triffterer/Ambos, Art. 7 mn 142

[59] Triffterer/Ambos, ibid.

[60] See for the developments in UK academia, with reference to the underyling general literature Rosalind Gill, Breaking the silence: The hidden injuries of neo-liberal academia, in Róisin Ryan-Flood/Rosalind Gil. (eds.) *Secrecy and Silence in the Research Process: Feminist Reflections.* (London, Routledge, 2009). 228 – 244.

the corporal punishments of old have been replaced by a system which instead of physically afflicting the body subjects it to continuous and total monitoring, in order to control it and prevent deviant behaviour, and he takes as his prime example the rise of the prison system. In the chapter entitled "Panopticism"[61] in particular, he picks up on Bentham's[62] concept of the panopticon, i.e. a form of prison architecture consisting of individual cells assembled in an annular shape around a central tower from which each cell's inhabitant can be monitored at any given time without noticing himself that he is being watched. He traces the state's desire to monitor everyone as closely as possible back to states of public emergency, at the example of the plague:

> In order to make rights and laws function according to pure theory, the jurists place themselves in imagination in the state of nature; in order to see perfect disciplines functioning, rulers dreamt of the state of plague. Underlying disciplinary projects the image of the plague stands for all forms of confusion and disorder; just as the image of the leper, cut off from all human contact, underlies projects of exclusion.[63]

In essence, as is borne out by the current rhetoric of the counter-terrorism debate, Foucault posits that the public authorities are operating as much as possible on the basis of a continuous state of emergency, or "state of exception", as Giorgio Agamben would put it.[64] The ultimate aim of the Panopticon, just as much as that of data privacy intrusion, is the impression of constant visibility and flowing from that, the creation of self-monitoring by and a consequential adaptation of the person's behaviour:

> Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary;[…], that the inmates should be caught up in a power situation of which they are themselves the bearers. To achieve this, it is at once too much and too little that the prisoner should be constantly observed by an inspector: too little, for what matters is that he knows himself to be observed; too much, because has no need in fact of being so. In view of this, Bentham laid down the principle that power should be visible and unverifiable. Visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. Unverifiable: the inmate must never know whether he is being looked at at any one moment; but he must be sure that he may always be so.[65]

---

[61] The chapter is available online in Race/Ethnicity: Multidisciplinary Global Contexts, Vol. 2, No. 1, The Dynamics of Race and Incarceration: Social Integration, Social Welfare, and Social Control, 1-12, Indiana University Press, at www.jstor.org/stable/25594995.

[62] John Bowring (ed.) The Works of Jeremy Bentham, vol. 4 (Panopticon, Constitution, Colonies, Codification) [1843], available online at http://oll.libertyfund.org/titles/bentham-the-works-of-jeremy-bentham-vol-4.

[63] ibid, 4.

[64] Giorgio Agamben, *State of Exception*. (Chicago, University of Chicago Press, 2005); for a critique see Stephen Humphreys, Legalizing Lawlessness: On Giorgio Agamben's State of Exception, EJIL (2006) 677–687. Malcolm Bull in his review "*States don't really mind their citizens dying (provided they don't all do it at once): they just don't like anyone else to kill them*" in the London Review of Books, vol. 26 no. 24, of 16 December 2014, 3 – 6, had this to say about Agamben's analysis: "We have moved from Athens to Auschwitz: the West's political model is now the concentration camp rather than the city state; we are no longer citizens but detainees, distinguishable from the inmates of Guantanamo not by any difference in legal status, but only by the fact that we have not yet had the misfortune to be incarcerated—or unexpectedly executed by a missile from an unmanned aircraft.…But although his recent examples come from the war on terror, the political development they represent is […] part of a wider range in governance in which the rule of law is routinely displaced by the state of exception, or emergency, and people are increasingly subject to extra-judicial state violence."

[65] ibid, 6.

This behavioural adaptation, in Foucault's view, leads to a state of affairs where the object of the surveillance simultaneously becomes the subject of their own submission:

> He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle *[sic!]* of his own subjection. By this very fact, the external power may throw off its physical weight; it tends to the non-corporal; and, the more it approaches this limit, the more constant, profound and permanent are its effects: it is a perpetual victory that avoids any physical confrontation and which is always decided in advance.[66]

Thomas McMullan, also based on Bentham's Panopticon, has succinctly explained the effect of present-day data intrusion.[67] Much more than the references by McMullan to

---

[66] ibid,7. – However, in the context of massive data privacy intrusion, a phenomenon he was unable to foresee in all its complexity in 1975, Foucault may have been somewhat too optimistic or theoretical in his views that the panopticon could also be opened up to scrutiny by the public and democratic control, when he said: "Furthermore, the arrangement of this machine is such that its enclosed nature does not preclude a permanent presence from the outside: we have seen that anyone may come and exercise in the central tower the functions of surveillance, that, this being the case, he can gain a clear idea of the way which the surveillance is practised. In fact, any panoptic institution, even if it is as rigorously closed as a penitentiary, without difficulty be subjected to such irregular and constant inspections: and not only by the appointed inspectors, but by the public; any member of society will have the right come and see with his own eyes how the schools, hospitals, factories, prisons function. There is no risk, therefore, that the increase of power created by the panoptic machine may degenerate into tyranny; the disciplinary mechanism will be democratically controlled, since it will be constantly accessible 'to the great tribunal committee of the world'. This Panopticon, subtly arranged so that an observer may observe, at a glance, so many different individuals, also enables everyone to come and observe any of the observers. The seeing machine was once a sort of dark room into which individuals spied; it has become a transparent building in which the exercise of power may be supervised by society as a whole." – ibid, 11. There is and always has been every indication that governments will not allow any meaningful outside interference or even scrutiny of the intelligence apparatus. Even ostensibly democratically established control mechanisms will have to rely on the assumption that the intelligence community will serve them with the full facts in any given case; they have no independent way of verifying the truthfulness of the intelligence actors nor of the truth of the information, and are unable to subject the security evaluations based on it they are being given to proper and independent scrutiny, because that requires expertise which only the intelligence service has and which it is unwilling to share. The societal othering scenario, which essentially underlies Foucault's writing in *Discipline and Punish*, is largely absent in the data privacy intrusion debate as such, where everyone is under surveillance by a very few, as opposed to the use of allegedly objectively gathered and reliable intelligence for the purpose of othering certain sections of society.

[67] See Thomas McMullan The Guardian, 23 July 2015, *What does the panopticon mean in the age of digital surveillance?*, at www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham, 23 July 2015: "In the private space of my personal browsing I do not feel exposed – I do not feel that my body of data is under surveillance because I do not know where that body begins or ends. We live so much of our lives online […] but feel nowhere near as much attachment for our data as we do for our bodies. Without physical ownership and without an explicit sense of exposure I do not normalise my actions. […] My data, however, is under surveillance, not only by my government but also by corporations that make enormous amounts of money capitalising on it. […][T]he amount of data on offer to governments and corporations is about to go through the roof, and as it does the panopticon may emerge as a model once more. Why? Because our bodies are about to be brought back into the mix. The […] internet of things […] will change digital surveillance substantially. With the advent of wider networked systems […] everything […] will soon be able to communicate, creating a […] deluge of data […] [which] won't only be passed back and forth between objects but will most likely wind its way towards corporate and government reservoirs. With everything from heart-rate monitors in smartwatches to GPS footwear, a bright light is once again being thrown on our bodies. […] Much of the justification of this is the alleged benefits to health and wellbeing. "Morals reformed – health preserved – industry invigorated" –

the line "[m]orals reformed – health preserved – industry invigorated", the following line from the preface written by Bentham is even more instructive for our purposes: "A new mode of obtaining power of mind over mind, in a quantity hitherto without example".[68] This hidden, in essence neo-liberal, *active* governmentality agenda is amplified in many instances by the *passive* response of the population, namely apathy or lack of awareness. For the UK environment, to take but one example, David Davis – who had actually been one of the persons challenging the previous UK intelligence law before the CJEU in the above-mentioned Case C-698/15 but had then removed himself from the case when he became a government minister under Theresa May – said, with maybe some exaggeration as to the unique position of the UK, "[i]n every other country in the world, post-Snowden, people are holding their government's feet to the fire on these issues, but in Britain we idly let this happen […] Because for the past 200 years we haven't had a Stasi or a Gestapo, we are intellectually lazy about it, so it's an uphill battle"[69], while journalist Heather Brooke asserted that "[t]he spies have gone further than [George Orwell] could have imagined, creating in secret and without democratic authorisation the ultimate panopticon. Now they hope the British public will make it legitimate."[70] Telling in the context of the UK public's apparent lack of resistance and the above-mentioned allegation of being "intellectually lazy" with regard to governmental privacy intrusion is a survey published on 9 February 2015 on yougov.co.uk with the following questions and answers:[71]

[PLACE ILLUSTRATION_The Global Panopticon HERE]

There are two things to be said about these questions, regardless of their statistical significance and reliability: Firstly, they are *vox populi* opinion questions on the lowest intellectual level, in fact almost relating more to moods or general feelings rather than the application of critical thinking, which may be indicative of the corresponding level of intellectual acumen expected and/or displayed of the respondent cohort, something especially highlighted by the Reality TV question, which disingenuously seems to suggest a similarity between such a scenario and mass surveillance by the state[72]. Secondly, the question in the top table cannot be answered without detailed knowledge of the actual threat scenario, which none of the respondents will have had; the only correct answer would have been "don't know"; furthermore it has a subliminal message that seems to say that human rights must take a backseat to security concerns. The fact that 49% of the respondents answered with "yes" shows a worrying tendency to believe the official narrative about the effectiveness of counter-terrorism measures more or less unquestioningly. Similarly, the fact that 53% of the respondents in the second table are simply not "bothered" by the prospect of being spied upon by intelligence services, regardless of whether they believe they are being spied upon now, does not bode well

---

not Apple marketing material but Bentham's words on the panopticon. There may not be a central tower, but there will be communicating sensors in our most intimate objects."

[68] John Bowring (ed.) *The Works of Jeremy Bentham, vol. 4 (Panopticon, Constitution, Colonies, Codification)* [1843], p. 39.

[69] Andrew Sparrows, The Guardian, 8 November 2015, *David Davis: British 'intellectually lazy' about defending liberty*, at www.theguardian.com/politics/2015/nov/08/david-davis-liberty-draft-investigatory-powers-bill-holes.

[70] Heather Brooke, The Guardian, 8 November 2015, *This snooper's charter makes George Orwell look lacking in vision*, at www.theguardian.com/commentisfree/2015/nov/08/surveillance-bill-snoopers-charter-george-orwell.

[71] https://yougov.co.uk/news/2015/02/09/investigatory-powers-tribunal-intelligence-service/

[72] It is open to question how the answers would have changed if the sum had been £ 10,000.

for the likelihood of any principled resistance to government intrusion into the personal data sphere. Here again, the neo-liberal incentive to make people adopt a seemingly self-chosen subservient attitude is demonstrated, exposing the governmental[73] technology of the "objective" public survey as a tool to reinforce a hidden governmentality aim, in that, firstly, the answer can be orchestrated to a large extent by the choice and wording of the questions. Secondly, the ostensibly "automatic" and non-manipulated – because merely mathematically calculated – survey result can then be deployed again as a supposedly objective means of verification of commonly shared societal morals and as an instrument of self-reassurance by the neo-liberal subject that she herself is conforming to expected and majority-validated patterns of thought and behaviour.

In sum, the violation of the right to data privacy is to all intents and purposes invariably intentional and, since it has all the potential for not only creating a passively suffered infringement of a protective shield of the person as a data subject, but much more for using the – mostly nebulous – awareness that the privacy veil is liable to be pierced at any given time as a mainly sub-conscious motivational driver to conform to hidden – and thus at best equally nebulously experienced – expectations transmitted by the governmentality frameworks of the day. Since these frameworks are multi-layered and can range from local city councils' petty use of CCTV cameras as a means of tracking people who discard litter in public spaces, over seemingly innocent commercial applications such as automatic number-plate recognition in car parks, to the more sinister technologies of counter-terrorism and immigration control as well as health-related commercial and employment applications, they produce an effect on the privacy subject that leads to a variated choice of mental and physical responses to actual situations in real life, and an overall wary reluctance to be a fully independent and actively contributing member of society. In other words, they create a fear that eats the soul. It should thus be accepted that massive data privacy intrusion has all the hallmarks of an equally severe violation of a fundamental right.

L 2 The chapeau elements

As with any CAH, there is the need for compliance with the chapeau elements of a widespread or systematic attack on a civilian population, of which the CAH would need to be a part. A nexus to an armed conflict is not necessary under customary international law. The attack need not be of a military character. Most of these elements would seem to be rather straightforward. Given the global, indiscriminate, intentional, planned and deliberate use by state and non-state actors, the attack – which can consist of the very act itself[74] – is both widespread and systematic, even if the framework of reference is reduced to one country or geo-political region. Regardless of whether a policy element is required or not under customary law,[75] the kind of data intrusion this paper is concerned with is hardly imaginable without such a policy – these are not isolated acts. The attack of mass data intrusion is almost in its entirety – apart from specific military espionage – directed against civilians. Considerably more thought needs to be spent on the nature of the acts underlying the attack. The ICC Statute's definition of attack refers to any of the acts mentioned under Art. 7(1), under customary law any multiplicity of acts

[73] One of the founders and former Chief Executive Officer of YouGov is the Conservative MP Nadhim Zahawi; see Chris Tryhorn, The Guardian, 22 February 2010, *YouGov chief executive Nadhim Zahawi to stand down to run as Tory MP*, at www.theguardian.com/media/2010/feb/22/nadhim-zahawi-yougov-election-mp.

[74] Triffterer/Ambos, Art 7 mn 14.

[75] Triffterer/Ambos, Art 7 mn 109.

of unlawful i.e. criminal interference with protected interests can suffice, and violence is not required.[76] Unless the discriminatory criteria for persecution are fulfilled and the violation of data privacy were to be interpreted as an infringement of a fundamental right of sufficiently equal severity, the ICC Statute, for example, would not appear to be able to accommodate violations of the fundamental right to data privacy as an underlying act that could be, or be connected to, an attack.

Whether under general international law the violation of data privacy is sufficiently criminalised at this time, is at best unclear. There is no convention-based international crime of violation of data privacy, and it is questionable whether general customary law doctrine would allow the creation of a new category based on general principles in the criminal laws of individual states related to data protection – precisely because the states' laws will contain often rather broad-ranging public interest exception clauses. Even the *Proposed International Convention on the Prevention and Punishment of Crimes Against Humanity*[77] which might be seen as indicative of such an emerging consensus, does not foresee a residual clause that would make such a conclusion an easy one to draw. Its Art. 3 on the definition of the crime more or less tracks Art. 7 of the ICC Statute, hardly surprising given the need to find a platform on which most states would find it easy to support a Convention aimed at implementation in domestic law. Instead, the last paragraph of the Preamble makes a veiled reference to the idea of the Martens Clause. [78] That, of course, is not sufficient for establishing a fully-fledged CAH. As a matter of fact, the attitudes expressed over several sessions of the Sixth Committee by states to the ILC's Project on CAH[79] and collected by the proponents of the Convention, do not support a more hopeful picture. However, this finding – after what was said above in the context of the Foucauldian discussion – is hardly surprising: States prize the ability to monitor their citizens and other persons within their spheres if interest or influence, whether in the domestic or wider geo-political sense, to the largest degree possible; it is therefore unlikely at best to expect them to subscribe to the creation of a basis of state practice that could reasonably be interpreted as giving rise to an individual liability of their chief agents under international criminal law, with penalties being almost exclusively long custodial sentences.

An example of the cautious approach even in developed international legal systems such as the EU is the recent *Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [80] scheduled to apply from 25 May 2018,[81] which, to begin with, is not applicable to

> […] competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, *including the safeguarding against and the prevention of threats to public security* [my emphasis], [82]

[76] Ambos, Treatise, vol. II, 58 f.
[77] Text at http://law.wustl.edu/harris/cah/docs/EnglishTreatyFinal.pdf.
[78] ibid, 2. – see explanatory note 8 on p.3: "[…] that in cases not covered by the present Convention or by other international agreements, the human person remains under the protection and authority of the principles of international law derived from established customs, from the laws of humanity, and from the dictates of the public conscience, and continues to enjoy the fundamental rights that are recognized by international law […]."
[79] http://law.wustl.edu/harris/crimesagainsthumanity/?p=1944.
[80] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
[81] ibid, Article 99(2).
[82] ibid, Article 2(1)(d).

which eliminates the entire counter-terrorism and public policing aspect from its reach. After proscribing "administrative fines" of up to 20 million € or 4 % of the total worldwide turnover of the offending entity in Article 83, it states in Article 84 on penalties:

> 1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.
> 2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

The central introductory recitals underlying Article 84 are at paras. 148 – 152. The latter states:

> Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, *Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law* [my emphasis].

The Regulation in theory allows but does not explicitly mention imprisonment; the preference appears to be for financial sanctions. The financial penalties seem harsh but depending on the basis of the actual offence may not see the application of their maximum amounts very often; their financial impact may also be easily absorbed by the offending institution. In any event, it is a far cry between classification as a CAH and the imposition of mainly financial penalties, with a mere discretion of the EU Member States to use harsher means that attach to the person's body, i.e. imprisonment, and not their financial assets.

L 1 Conclusion – *Per aspera ad astra*

In this paper, I have tried to interrogate the premise that we may need to move from a traditional understanding of the protected rights under international criminal law, especially in the context of CAH, to a 21st century paradigm. ICL still puts too much emphasis on the kind of harm that everyone can see and immediately relate to – threats to life, limb, liberty and property, with an emerging focus on sexual and gender-based violence.

However, there are rights which are in essence non-corporeal but the violation of which may cause equally tangible damage. The practice by governments and private actors of collecting vast amounts of data almost indiscriminately has, as the Foucauldian analysis in particular has shown, the potential for suppressing freedom of speech and belief, but also the distinct right to privacy, with a potency which equals that of the traditional target rights. The right to privacy has increasingly come to the forefront of public attention in law reform debates, centred mostly on the tropes of crime fighting and counter-terrorism efforts. This supposedly antagonistic relationship between individual freedom and control for the public – greater? – good makes for a formidable obstacle to finding a straightforward and timely solution.

Based on the assumption that despite a certain lack of sharp contours in the conceptual and terminological context, I posited that there has to be a "red line" on the

level of international law when it comes to triggering the protection of (international) criminal law, all things being equal. An analysis of the current case law, however, has shown that any hope of an easy classification as a CAH – with the possible exception of the already existing crime of persecution – would seem to be unfounded. The sufficient degree of awareness that these days privacy may have become a right on a par with the traditional ones underlying CAH and war crimes has so far not materialised. Like any other law on the international level, international criminal law is made by states – that is, by those who, it might be said, are more part of the problem than of the solution. Yet, even in such an environment it is necessary to continue to speak truth to power and hope that, sometimes, the power of truth will eventually prevail.