Universität Potsdam

Universitätsverlag Potsdam

Juliane Damen | Lena Köhler | Sean Woodard

The Human Right of Privacy in the Digital Age

Staat, Recht und Politik – Forschungs- und Diskussionspapiere | 3

Staat, Recht und Politik – Forschungs- und Diskussionspapiere | 3

Juliane Damen | Lena Köhler | Sean Woodard

The Human Right of Privacy in the Digital Age

Universitätsverlag Potsdam

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Universitätsverlag Potsdam 2017
http://verlag.ub.uni-potsdam.de/

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 2533 / Fax: 2292
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Staat, Recht und Politik – Forschungs- und Diskussionspapiere** wird herausgegeben von apl. Prof. Dr. iur. Norman Weiß, Universität Potsdam.

ISSN (online) 2509-6974

Kontakt:
weiss@ uni-potsdam.de

Online veröffentlicht auf dem Publikationsserver der Universität Potsdam
URN urn:nbn:de:kobv:517-opus4-399265
http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-399265

Abstract

The right to privacy in the digital age generates new challenges for the international jurisdiction. The following article deals with such challenges. Therefore it firstly defines the term of privacy in general and presents an international legal framework. With whisteblower Snowden a huge political discourse was initiated and the article gives insights into its further development. In 2015 the Human Rights Council for the first time announced a special rapporteur on the right to privacy. However, the discourse is not only taking place on a political level, also civil society organizations advocate more stringent regulations and prosecutions against violations of the right to privacy. Moreover the importance of the technology sector becomes clear. Companies like Microsoft are increasingly taking responsibility to protect digital media against unjustified data misuse, surveillance, collection and storage. But whereas the IT sector is developing very quickly, legislative processes do so rather slowly. Lastly, the individual is also hold to account. To protect oneself against data misuse is to a great extent acting self-responsible. Still, therefore information on protection must be clear and accessible for everyone.

Zusammenfassung

Das Recht auf Privatsphäre im digitalen Zeitalter stellt die internationale Gerichtsbarkeit vor neue Herausforderungen. Der nachfolgende Artikel beschäftigt sich mit diesen Herausforderungen. Er definiert „Privatsphäre“ und zeigt internationale rechtliche Rahmenbedingungen auf. Der seit Whisteblowern wie Snowden angestoßene internationale politische Diskurs und dessen Entwicklung werden beleuchtet. Der Menschenrechtsrat der Vereinten Nationen bestimmte im April 2015 erstmals einen Sonderberichterstatter für das Recht auf Privatsphäre. Jedoch findet der Diskurs nicht nur auf politischer Ebene statt: Auch zivilgesellschaftliche Organisationen setzten sich zunehmend für strengere Vorschriften und Strafverfolgungsmaßnahmen für Verstöße gegen das Recht auf Privatsphäre ein. Zudem wird auch die Bedeutung des IT-Bereichs deutlich. Technologieunternehmen wie Microsoft sehen sich zunehmend in der Verantwortung, digitale Medien gegen nicht gerechtfertigte Datenmissbrauch, Überwachungsmaßnahmen und Datensammlung zu schützen. Der IT-Bereich entwickelt sich sehr schnell – die Gesetzgebung hingegen sehr schleppend. Zuletzt wird auch die einzelne Person in Verantwortung gezogen. Sich selbst weit möglichst gegen Datenmissbrauch zu schützen, liegt bislang in der Hand des Einzelnen. Informationen zum Schutz müssen jedoch deutlich und zugänglich sein.

Information about the authors:

Lena Köhler studied social work in Stuttgart at the Cooperative State University Baden-Württemberg (2009-2012), has working experience with children in orphanages in Bolivia (volunteering), in a probation office and psychiatry for addicted youth (internship within the dual studies), with homeless people (as a professional for 3 years). She is currently studying Intercultural Conflict Management at the Alice-Salomon-University of applied science with interests in human rights, conflict transformation and social change in developing countries.

Sean Woodard studied fine art at the Dante Alighieri School in Florence, Italy and the California College of the Arts in San Francisco, California where he earned his BFA in painting. He has since worked with students of all ages in arts, languages, and social development fields. Since working in nightlife management and electronic arts and events promotion, Woodard has become engaged in Berlin's refugee community as an instructor at Flughafen Tempelhof, one of Berlin's largest refugee asylums. He is currently completing his MFA in Intercultural Conflict Management at the Alice Salomon Hochschule in Berlin, Hellersdorf.

Juliane Damen studied Social Work (B.A.) and Intercultural Responsibility in Regensburg/Germany at the Ostbayrische Technische University of applied sciences. She has work experiences with refugees, families in precarious living situations, children and women both in Germany and abroad. Currently she is completing a course of Intercultural Conflict Management (M.A.) at the Alice Salomon University of applied sciences in Berlin/Germany and intends to work particularly with migrants and women affected by human trafficking and exploitation. She is passionate for international social justice, conflict transformation and human rights.

The Human Right of Privacy in the Digital Age

Juliane Damen, Lena Köhler, Sean Woodard

Outline

I. Introduction

At present – when most information is spread and carried on in a digital form, when communication technologies such as smartphones and free internet access ubiquity have become part of daily life, when commerce, health and financial services, education and entertainment, social platforms and infrastructures are provided online and in real-time – contemporary life is increasingly moving in the direction of becoming a "transparent society". Information technologies and computing systems that record our every keystroke and physical movement are dissolving the borders between the individual, state and private enterprise. We live in the, so called, "digital age".

The Committee on Privacy in the Information Age describes these technologies as "new ways of collecting and handling information that in turn have ramifications throughout society, as they mediate much private and public communication, interaction, and transactions" (Waldo et al. 2007, 27). Civil society might be familiar with online data savings of locations, communications and IP addresses and people might say that there is nothing they need to hide or worry about. Still there is a "lack of transparency" including not only the functioning of search engines, but also "governments' internet surveillance" and data that is nevertheless saved, after it was "deleted" (Bernal 2014, 263).

The current development of information technologies impacts human rights on several levels and has become a controversial subject of much debate.

One side of the discussion argues that present technologies improve the realization of human rights. The United Nations High Commissioner for Human Rights (UNHCR) outlines the ways digital communication technologies have "improved enjoyment of human rights" inasmuch as the Information Age has "boosted freedom of expression, facilitated global debate and fostered democratic participation" (UN 2014a, A/HRC/27/37, 3). Moreover, especially in the debate about terrorism and security, when conducted in compliance with the law, surveillance of electronic communications data can be an effective and operational tool for legitimate law enforcement in order to protect human rights.

Conversely, these technologies have become a threat to human rights by facilitating surveillance, interception and collection of personal data. Worldwide, entities in government, the public, and private sector have become perpetrator and victim of invasive digital surveillance. Though espionage and surveillance have always been a part of sociopolitical reality, the introduction of powerful personal computation technologies to the consumer market have brought the same tactics of interference and manipulation to the individual level, redefining the contemporary frontier of human rights. "[...] the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it" (UN 2014a, A/HRC/27/37, 3). In light of the 2013 revelations by Edward Snowden, detailing mass surveillance by US National Security Agency, the right to privacy and its protection seem to be seriously endangered and create new levels of debate (ibid., 3f). Indeed "one of the most discussed and worried-about aspects of today's Information Age is the subject of privacy" (Waldo et al. 2007, 19).

II. Defining "privacy"

To engage the discourse surrounding the protection of the individual's right to privacy in the digital age, and to deliberate on whether there is a need for more tangible legal framework

and enforcement mechanisms on national and international levels, the concept of "privacy" needs to be defined. The wide scope and lack of a clear and universal definition of privacy thus far obscures legal progress. Relating privacy to the perspective of human rights, scholars argue that privacy,

> "[...] demands respect for a broad range of loosely allied personal interests: physical or bodily integrity; personal identity and lifestyle (at least to some respects), including sexuality and sexual orientation; reputation; family life; the home and home environment." (Herne Hill et al. 2009, 359)

The Committee on Privacy in the Information Age argues that the term used in a general way,

> "includes reference to the types of information available about an individual, whether they are primary or derived from analysis. These types of information include behavioral, financial, medical, biometric, consumer, and biographical" (Waldo et al. 2007, 22).

Privacy, in such an understanding, may also contradict "other values or desires of the individual, subgroups, and society at large" (ibid).

Furthermore, privacy can be examined from the perspective of sociology, psychology, technology, philosophy, ethics or legal theory. To investigate privacy in its full dimension we would have to address a number of further questions: *who* is involved, *when* and *how* is privacy affected, which disciplinary viewpoint do we take, etc. There are whole books written on the different theories, concepts and values of privacy and its (re)construction (e.g. Solove 2008). For the purview of this analysis, privacy can therefore not be seen as an absolute concept and will always need to be weighed in relation to other relevant aspects. However, it is precisely the varying constructions of the definition of privacy which may contribute towards the moral relativism which characterizes its fickle protection by state and private actors, in the face of absolute events, such as 9/11, which define the contours of global sociopolitical discourse. Given the current global reach of state and private interests through digital technologies, overcoming cultural and regional ambiguities in the definition of privacy may aid in creating a robust universal defense of the democratic values which privacy is understood to protect.

III. Legal framework

International law provides a legal framework on the topic of privacy. The human right to privacy and its protection is outlined in Article 12 of the *Universal Declaration of Human Rights (UDHR)* and with the same wording in Article 17 of the *International Covenant on Civil and Political Rights (CCPR):*

> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (UN 1948, 4; UN 1966, 10)

At the regional level there are conventions also promoting the right to privacy. Examples are Article 11 of the *American Convention on Human Rights (*Inter-American Commission on Human Rights 1969 *)* or Article 8 of the *European Convention* (ECHR 1950):

> "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
> (ECHR 1950, 10)

Moreover, on supranational levels, such as that dictated by European Union legislation, there are legal frameworks referring to privacy such as the *General Data Protection Regulation* (GDPR). This regulation aims at protecting all EU citizens "from privacy and data breaches in an increasingly data-driven world" and includes data subject rights as for example breach notification, the right to access or the right to be forgotten (GDPR 2017).

Similarly, the *Convention on the Rights of the Child* (Article 16), as well as the *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families* (Article 14), these legal documents universally extend the protection of one's privacy, family, communications, correspondence and home (UN 1989, 5;UN 1990, 6), while focusing on the protection of neglected persons.

The multitude of supranational, international, state and regional laws, conventions, and norms concerned with the protection of privacy around the world indicate that individual privacy is a universally cherished value with significant socio-political implications. Global civilization, having awakened seemingly overnight in an age of transparency, where individual privacy is more a perceived threat to communal well being than ever, now grapples with an aggressive reconfiguration of hitherto uncompromisable values.

IV. Political Discourse and Development

Within international political discourse, mass data surveillance and storage are legitimized by the "War on Terror" (Cohen/Fisher 2016). Indeed, in some cases of national security and criminal activities, surveillance can be justified. However, fully developed mechanisms for civil society to be protected from such are lacking. If there are no reasonable grounds for suspicion such as terrorist or criminal activities, indiscriminate mass surveillance of all individuals and states is a violation of human rights.

The *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, states that national laws that regulate the involvement of states in communication surveillances often do not exist, or are inadequate (UN 2013, A/HRC/23/40, 3). Moreover, differences in national legal frameworks and their enforcement mechanisms raise worldwide disputes about internationally feasible regulation.

Emphasizing the differences in national frameworks, in the 2015 *Maximilian Schrems v. Data Protection Commissioner* decision of the European Court of Justice a relevant example is provided: Personal data was transferred from a European Facebook account to the United States of America. As US-rights of data protection differ from European rights and do, according to the Data Protection Commissioner of the EU Court of Justice, "not offer sufficient protection

against surveillance by public authorities" (Schrems 2015, 1) the US Safe Harbour Decision was declared invalid (ibid.). The decision reverses the so called "Safe Harbor" agreement between to US and EU in 2000 which effectively smoothed over differences in the legal standards around privacy in the two respective unions. Though this agreement and its 2002 reaffirmation by the EU Commission previously sufficed as a resolution of inadequacies and contradictions, in the post-Snowdon environment a reversion to the adherence to to the supranational Charter of Fundamental Rights of the European Union, and its rigid protection of individual privacy, highlights idiosyncrasies in the collision of multilayered legislation.

Reinforcing the international perspective on this issue, the *Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, concurs with the High Commissioner for Human Rights that where States penetrate infrastructure located outside their territorial jurisdiction, they remain bound by their obligations under the Universal Declaration of Human Right (UN 2014e, A/69/397). A multilevel legal framework reinforces the respective obligations; however it does not begin to resolve the issue of the lack of necessary multilateral enforcement mechanisms.

Compounded with the slippery consensus around legal definitions for culturally sensitive terms, like privacy, technology is quickly growing and therefore international law-making becomes very difficult. The nature of the Internet is borderless and different stakeholders have contradicting interests. Also, legislative processes are relatively slow and lawmakers often lack a technological understanding (Bernal 2014, 82). Still these difficulties do not excuse foregoing the urgent need for more thorough regulations of privacy. Sisk argues, that there is a need for more, and stronger, privacy rights in our digital age (Sisk 2016, 101).

Though concerns for the individual's right to privacy in the digital age have preoccupied analysts en masse since the early 2000's, Snowden's leak of NSA details on digital surveillance programs in 2013 have catalyzed a debate that very quickly escalated to the level of the United Nations.

Before 2013, resolutions from the UN-General Assembly were primarily concerned with bolstering privacy rights under oppressive regimes as a mechanism for protecting the freedom to speech, opinion and expression in a democratic society. For example the Resolution 7/36 from the Human Rights Council (UN 2008, R/7/36), a mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (March 2008) or Resolution L13 , the Promotion, Protection and Enjoyment of Human Rights on the Internet (UN 2012, A/HRC/20/L.13).

Similarly concerned with defending the rights of journalists and dissents from oppressive regimes, a resolution from July 2012

> "affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice [...]." (UN 2012, A/HRC/20/L.13, 2)

These, and other such resolutions, serve as reference points in the defense of online privacy. However, they often failed to address the arbitrary, but important details that would distinguish digital communications from other forms of information.

The US Electronic Communications Privacy Act (ECPA) of 1986 disregarded the distinctions between electronic and traditional communications by extending the privacy provisions of the Act's original Federal Wiretap Act's (1968) drafting from intercepting conversation on "hard" telephone lines to "wire, oral, and electronic communications while those communi-

cations are being made, are in transit, and when they are stored on computers" (Justice Information Sharing 2013).

Whether by discerning eletronic from traditional communication, or by bringing all forms of communications under privacy protection national and international law failed under legislation enacted by the USA Patriot-Act of 2001. As stated by the US Department of Justice, the Patriot Act's effect on the pre-existing ECPA results in the "[...] easing [of] restrictions on law enforcement access to stored communications in some cases" (ibid.). Twelve years later, the international human rights community found itself confronting the uncomfortable fact that the Patriot Act disabled privacy protections on a sweeping global scale.

The new facts the human rights community had to negotiate after Snowden's revelations was not that the US and UK intelligence agencies (NSA and GCHQ) were intercepting and monitoring electronic communications of targeted sources in the "war on terror". Rather the NSA and GCHQ, with use of an agency developed program PRISM, were indiscriminately monitoring the communications of US and UK citizens, as well as foreign nationals. Dating back to 1988, the *United Nations Human Rights Committee* (HRC) has been calling attention to the important distinction between targeted and indiscriminate data collection in the General Comments made on CCPR Article 17 (Right to Privacy).

> "[...] 'arbitrary interference' can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances." (UN 1988, HRI/GEN/1/Rev.9 (Vol. I), 1)

Proponents of increased surveillance will point to the events of 9/11, the decentralization of power within terrorist networks, and the ever evolving nature of digital communications as "particular circumstances" which necessitate the blanket collection of digital communications and data to prevent further terror attacks. However, in direct response to the Snowdon revelations the Special Rapporteur Emmerson reiterated demands that,

> "relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world" (UN 2014e, A/69/397, 20).

The overwhelming majority of voices from the human rights community and civil society on the new threats to personal privacy, namely that the intelligence communities' indiscriminate interception and storage of bulk user data, goes to the very heart of the social contract in modern democracies.

> "Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17 [Right to Privacy]. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law." (UN 2014e, A/69/397, 21)

In its comment on CCPR Article 17, the Human Rights Committee also emphasises the importance of guaranteeing integrity and confidentiality of correspondence "de jure and de facto" (UN 1988, HRI/GEN/1/Rev.9 (Vol. I), 2). Nevertheless the "conscious compromise

through which individuals voluntarily surrender information about themselves and their relationships" (UN 2014a, A/HRC/27/37, 6) while using digital means, was mentioned as well. But the question arises whether consumers are fully aware of the content, way, receiver and purpose of the data they exchange. Furthermore the report reflects on current prioritized investments as it seems like there are far more advanced efforts put into fusing and identifying apparently anonymous data than into technologies enhancing privacy (ibid.).

In its resolution 68/167 of January 2014, the UN-General Assembly stresses therefore the importance of the already existing international framework (e.g. UDHR, Art. 12; CCPR, Art. 17), as it talks about how surveillance and observation of today's communication systems could negatively affect and interfere with individual human rights. It calls on all states to protect and respect the right to privacy in digital communication and to review their methods plus their legitimation of collecting personal data and communication interception. The same rights that people enjoy offline have to be assured when they are online. States are reminded of their responsibility to ensure an effective realization and implementation of this international framework of human rights law (UN 2014b, A/RES/68/167, 2f).

The resolution furthermore requested the High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data, including the mass scale surveillance (UN 2014b, A/RES/68/167, 3).

The report points out that "any capture of communications data is potentially an interference with privacy […] whether or not those data are subsequently consulted or used" (UN 2014a, A/HRC/27/37, 7). The very existence of a mass surveillance programme thus creates an interference with privacy. If states want to keep such a system, it is hereby their duty to demonstrate that such interventions are neither "arbitrary" nor "unlawful" (ibid.). Therefore, arises the question of how "arbitrary" and "unlawful" are to be interpreted.

The term "unlawful" implies that no interference can take place "except in cases envisaged by the law" which means that states' national actions limiting privacy always need to fulfil the provisions, aims and objectives of the CCPR. Also, actions need to be *reasonable, proportional* to the legitimate outcome or goal and *necessary* in the given circumstances. This could be protection of national security and the right to life through a lawful, targeted surveillance of digital communication, establishing a necessary and effective measure for intelligence and law enforcement entities. Governments requiring telephone and internet service providers to store metadata about their customers' communications and location would neither be necessary nor proportionate (ibid., 7ff). When the limitation of privacy does not meet the above mentioned criteria of reasonability, proportionality and necessity, it would be unlawful and the interference therefore "arbitrary".

Furthermore, the report refers to the responsibility of technology companies, as they may risk complicity in human rights violations if they follow government requests for surveillance assistance without adequate safeguards (UN 2014a, A/HRC/27/37, 14f).

Brad Smith, president and chief legal officer of Microsoft pointed out such a responsibility of technology companies at this year's RSA Conference, an IT security conference in San Francisco where "cybersecurity at a critical time" (Smith 2017) was discussed with security professionals. Smith was calling upon technology companies "to do more to protect and defend" (ibid.) customers worldwide and also upon world governments to protect civilians by implementing international rules. He states, that civilians should be protected by governments from nation-states' cyberspace attacks based on a "Digital Geneva Convention" (ibid.), in the same way that civilians have the right to physical protection during times of war by the Fourth Geneva Convention.

Further, Smith stresses, that the active cooperation of the technology sector is necessary to protect civilians against cyberattacks. Continuing his metaphor, Smith states that involvement of the technology sector is now as necessary to protect human rights as the 1949 requirement of "active involvement of the Red Cross" (ibid.) to protect civilians from the primary threat to their human rights, as recognized in the Fourth Geneva Convention. The technology sector, for its part, plays an indispensable role as their companies are the first responders to cyberattacks and threats. Therefore, cybersecurity norms should become global rules of a multilateral agreement between the worlds governments (ibid.)

In April 2015, the Human Rights Council appointed the first Special Rapporteur on the right to privacy, responsible for the mandate of reporting violations of this right and of rising awareness towards the importance of its protection, as well as further threats and challenges arising from new technologies (UN 2015, A/HRC/28/L.27, 3f). This Special Rapporteur, Prof. Joseph Cannataci, of Malta, is collecting information related to the issue of privacy in the digital age – including international and national frameworks and the experiences, practices, trends, challenges and developments of different nations. Cannataci reports to the UN General Assembly and proposes recommendations to ensure the "promotion and protection" (ibid., 4) of the right to privacy.

In March 2016, the Special Rapporteur introduced a 10-Point Action Plan for the period of his mandate. It includes the development of a clear and universal definition for the "right to privacy", which all 21st century global citizens should be able to understand and apply to their own lives - on and offline. The Action Plan also calls for the initiation of a general discourse, and the raising of awareness amongst citizens around the imperatives of managing their own privacy (UN 2016a, A/HRC/31/64, 18f). Cannataci asserts that citizens should have information about the monetization of their data and also learn how to protect themselves and minimize the risk of infringement of privacy. The Special Rapporteur also advocates a structured, comprehensive, effective, transparent and permanent dialogue between stakeholders.

As the corporate IT sector gather the majority of personal data, it is especially important to focus on a "dialogue with the corporate world" (ibid., 18). Cannataci, therefore, sues "safeguards and remedies" (ibid.) and aims at holding the tech community accountable for the "promote the development of effective technical safeguards including encryption, overlay software and various other technical solutions" (ibid.). The 10-Point Action Plan further promotes the "national and regional development" (ibid.) of mechanisms to protect privacy in coordination with representatives of civil society organizations. It also wants to tackle cyber-realities, and - starting with an update of legal instruments - is going to invest in "development of international law relevant to privacy" (ibid.). Therefore, a better understanding of the term "right to privacy" (ibid., 18-19) is necessary.

10-Point Action Plan by the Special Rapporteur on the right to privacy

1. Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect
2. Increasing awareness
3. The creation of a structured, on-going dialogue about privacy
4. A comprehensive approach to legal, procedural and operational safeguards and remedies
5. A renewed emphasis on technical safeguards
6. A specially-focused dialogue with the corporate world
7. Promoting national and regional developments in privacy-protection mechanisms
8. Harnessing the energy and influence of civil society
9. Cyberspace, Cyber-privacy, Cyber-espionage, Cyberwar and Cyberpeace
10. Investing further in International Law

Source: UN 2016, A/HRC/31/64,18ff

In his first report to the General Assembly in August 2016 Prof. Joseph Cannataci identified critical areas in the protection of privacy. Beyond promoting the development of a greater understanding of privacy, the report prioritized awareness around "Thematic Action Streams (TAS) on Big Data and Open Data; Security and Surveillance, Health Data" (UN 2016b, A/71/368, 8) and "Personal data processed by corporations" (ibid.). Different working parties with high expertise shall organize events "to gather evidence and identify options for strategies which would produce improved safeguards and remedies for privacy in a given sector of activity" (ibid., 2).

In his report to the Human Rights Council in March 2017, Cannataci stated that measures of current national legislation to regulate government surveillance are extremely intrusive, inefficient, and non-proportional. Drafted laws have been "rushed through the legislative process" (UN 2017, A/HRC/34/60, 7) in order to legitimize practices of surveillance. Governments thereby make use of the fear of terrorism and manipulate policy-makers to adopt "unduly disproportionate privacy-intrusive laws" (ibid., 15). This sentiment is echoed throughout the many investigations into government surveillance by the UN and the many civil society actors specially engaged around this issue, which characterizes the moral collision course set by intelligence community special interests and regulators defending individual sovereignty.

V. Outlook

The inhabitants of today's dizzyingly complex digital ecosystem can be boiled down to three primary stakeholder groups: "legislators, private (mostly corporate) actors, and citizens" (UN 2016a, A/HRC/31/64, 29). This "triangle of actors" tries to "shape cyberspace using their possibilities in an uncoordinated manner" (ibid.). If progress is to be made improving digital security *and* privacy each of these three levels of actors must further develop and co-

ordinate clear commitments and advocacy mechanisms around the improvement of digital privacy.

First off, international governance needs to play a more effective role in this inherently international issue. The definition of privacy (in the digital age) must be universally clarified and become clear for all parties to be able to fight violations towards the right to digital privacy. An internationally effective legal framework on the right to privacy exists, but there is still much work to be done in order to "be sincere in our efforts to ensure a transparent, free, fair and respectful international intergovernmental mechanism of internet governance and one that also ensures the right to privacy" (Brown 2013). Current international monitoring systems need to be reviewed regarding their efficacy and commitment to protections. International bodies, such as the UN, that have garnered hard-won international consensus around the definition of, and commitment to, human rights and the steadfast protection of the values which they uphold have an acute need to develop stronger implementation mechanisms in order to hold individual signatory states responsible to their commitments. This is a monumental task, given that the multitude of vested interests around surveillance and data collection, in both the private sector and nation states, through military and intelligence communities, increase at rates similar to the exponential growth of digital technology's usage. States' legitimations of collecting personal data and communication interception must be scrutinized by independent regulatory bodies to ensure that they are justified under the universally accepted norms and values.

Secondly, as stated at the RSA Conference, the technology sector plays a key role in fighting violations against cyber-attacks. It is the Internet's architect, content manager and the first responders in case of emergency. Also the tech field has the necessary knowledge and capabilities to tackle and prevent digital attacks at all levels with appropriate preventative and responsive protections.

The mandate of a "Digital Geneva Convention" would ideally meet the needs of the quickly developing and ever-growing problem of eroding individual privacy. In this Convention, states are called on for an implementation of rules protecting the rights of civil society in the digital sphere. Consumers, companies and states worldwide have to be protected and the online-space needs to be a secure space. Therefore, IT providers and developers must take responsibility and respond in "new and innovative ways that disrupt attacks" (Smith 2017).

Thirdly, there is an urgent need for the stronger involvement of civil society. Without the engagement of the citizens, customers, users, and individuals driving the momentum behind digital communications all other efforts to support individual sovereignty through the preservation of digital privacy will be for naught. On the one hand, citizens must become more aware of the information that they "voluntarily surrender [...] in return for digital access to goods, services and information" (UN 2014a, A/HRC.27.37, 6) and how easily their personal data through entertainment, social media, commerce, health and financial services can be surveilled by different stakeholders. The "reality of big data is that once data is collected, it can be very difficult to keep anonymous" (ibid.).

On the other hand, there should be more decisive political activism and joint movements by civil actors that put pressure on the public and the private sector. At no juncture in private commerce, or public policy, development has there ever been movement without clear demand from the consumer base, or body politic, respectively. It is the belief of UN Special Rapporteur Cannataci, and of experts in the field of social development, that when equipped with the relevant information about the collection and use of their personal data, individuals will make informed choices and demand responsive policy making to protect their rights as consumers and citizens.

For example, some private organizations, civil society organizations, and well as experts from all over the world established the "13 International Principles on the Application of Human Rights to Communication Surveillance". With their statement, they are urging governments to conduct communication surveillance that is consistent with human rights. The 13 Principles have been launched at the Human Rights Council in September 2013 (Brown, 2013) which itself is called to "reaffirm its commitment to promoting the right to privacy in light of evolving technologies and establish a framework for national guidelines" (ibid.).

Since the principles were published, more than 400 organizations, as well as thousands of citizens worldwide have co-signed the statement. The stated principles call for a transparent and continuously updated privacy protection legal basis and stronger regulation of surveillance. Proper regulation would entail the necessity for states surveillance to be legitimate, adequate and necessary. The burden of proof for these criteria lies with the respective states. The principles also strive for "prior authorization from a competent judicial authority" (EFF 2013) that is "impartial and independent" (ibid.) before communication surveillance can be executed. All topics related to the violation of the human right to privacy should be available for the public and information given should be sufficient, transparent, accessible and accountable. Individuals are to be more informed about any communication surveillance – except if there is a case of an urgent investigation, that should not be hindered, for example a legitimate threat of violence. In the technological sector, software, hardware and service providers should not collect information for the purpose of state surveillance. Lastly, the principles also call for the punishment of any illegal surveillance, and the development of a legal mechanism for those affected by surveillance (ibid.).

Policy makers, non-governmental organization, companies, as well as activists can make use of the above mentioned principles to create pressure on their governments and strive for a necessary change. The 13 Principles also "provide a benchmark" (EFF 2013) with which to measure the compliance of surveillance practices against the internationally held standard for human rights (ibid.).

Besides the development of the 13 International Principles there are a multitude of other civil society movements related to human rights and internet surveillance. One example is Best Bits, which is a network of worldwide civil society organizations that offers a platform for their members' agenda related to internet and state surveillance (Best Bits 2013). Other important statements on the "impact of surveillance on human rights" (Brown 2013) were written by Amnesty International and several South Korean non-governmental organizations. Such joint statements aim at ensuring "more systematic attention by the UN" (ibid.).

Essentially, the problem of maintaining individual sovereignty though the strengthening of digital security is a multifaceted issue which requires attention from all stakeholders. To be initiated on every level of digital engagement - from the grassroots individual user to the upper echelons of government responsible for overseeing surveillance programs - is a commitment to broadening awareness about the macro and micro management of data, and the strengthening of safeguards for all human rights in the 21st Century.

VI. Bibliography

Brown, Deborah (2013): UN Human Rights Council discusses surveillance and other internet issues at 24th session, retrieved from https://www.accessnow.org/un-human-rights-council-discusses-surveillance-and-other-internet-issues-at/, access: 12.07.2017

American Convention on Human Rights, retrieved from http://www.hrcr.org/docs/American_Convention/oashr4.html, access: 05.07.2017

Best Bits (2013): Civil Society Statement to the Human Rights Council on the impact of State Surveillance on Human Rights addressing the PRISM/NSA case, retrieved from http://bestbits.net/prism-nsa/, access: 03.07.2017.

Bernal, Paul (2014) Internet Privacy Rights. Rights to Protect Autonomy, Cambridge: Cambridge University Press.

Cohen, Rhaina/Fisher, Tyler (2016) Privacy in the Digital Age, retrieved from http://politicsandpolicy.org/article/privacy-digital-age access: 20.06.2017

Deutscher Bundestag (1949) Grundgesetz für die Bundesrepublik Deutschland, retrieved from http://www.gesetze-im-internet.de/bundesrecht/gg/gesamt.pdf, access 05.07.2017

EFF - Electronic Frontier Foundation (2013): Necessary and Proportionate. 13 International Principles on the Application oh Human Rights to Communication Surveillance, retrieved from https://www.eff.org/files/2014/01/05/13p-onepagerfinal.pdf access: 20.06.2017.

ECtHR - European Court of Human Rights/Council of Europe (1950) Convention for the Protection of Human Rights and Fundamental Freedoms, retrieved from http://www.echr.coe.int/Documents/Convention_ENG.pdf, access: 05.07.2017

GDPR - EU General Data Protection Regulation, retrieved from**:** http://www.eugdpr.org/the-regulation.html, access: 24.07.2017

Inter-American Commission on Human Rights (1969) Ameican Convention on Human Rights, retrieved from: http://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm, access: 12.07.2017

Justice Information Sharing - U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance (2013) Electronic Communications Privacy Act of 1986 (ECPA), retrieved from: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285, access: 12.07.2017

Lord Lester of Herne Hill, Anthony; Lord Pannick, David; Herberg, Javan (2009) Human rights law and practice, 3rd edition, London: LexisNexis

Schrems, Maximillian (2015) Court of Justice of the European Union, Press Release No.117/15. The Court of Justice declares that the Commission´s US Safe Harbour Decision is invalid, retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. access: 20.06.2017

Sisk, Edward P. (2016) Technical Difficulties. Protecting Privacy Rights in the Digital Age, in: New England Journal on Criminal & Civil Confinement, 2016, Vol. 42, Boston, p.101-119, retrieved from http://offerofproof.net/wp-content/uploads/42.1.Sisk_.pdf, access: 25.01.2017.

Smith, Brad (2017) The need for a Digital Geneva Convention, retrieved from https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0000tailwl104nflxwy7lipcvch5f, access 30.05.2017.

Solove, Daniel (2008) Understanding privacy. Cambridge/London: Harvard University Press

United Nations 2017, A/HRC/34/60, Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, retrieved from: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx, access: 12.07.2017

United Nations (2016a), A/HRC/31/64, Report of the Special Rapporteur on the right to privacy, retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/262/26/PDF/G1626226.pdf, access: 20.06.2017

United Nations (2016b), A/71/368, Right to privacy. Report of the Special Rapporteur on the right to privacy, retrieved from: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/71/368, access: 20.06.2017

United Nations (2015) A/HRC/28/L.27, Draft Resolution: The right to privacy in the digital age, retreived from: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/64/PDF/G1506164.pdf, access: 20.06.2017

United Nations (2014a) A/HRC/27/37, The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights, retrieved from http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf, access: 20.06.2017

United Nations (2014b) A/RES/68/167, Resolution adopted by the General Assembly on 18 December 2013. The right to privacy in the digital age, retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167, access: 20.06.2017

United Nations (2014c) A/HRC/28/39, Summary of the Human Rights Council panel discussion on the right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights, retrieved from: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39, access. 20.06.2017

United Nations (2014d) Safety of journalists and media worker, retrieved from: http://www.unesco.org/fileadmin/MULTIMEDIA/HQ/CI/CI/images/ci_staff/Safety_of_Journalists.pdf, access: 03.07.2017.

United Nations (2014e) A769/397, Promotion and protection of human rights and fundamental freedoms while countering terrorism. Note by the Secretary-General, retrieved from: https://assets.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf, access: 12.07.2017

United Nations (2013) A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, retrieved from http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, access: 20.06.2017

United Nations (2012) A/HRC/20/L.13, Draft Resolution: Promotion, protection and enjoyment of human rights on the Internet, retrieved from https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf, access: 20.06.2017

United Nations (2008) Human Rights Council Resolution 7/36. Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, retrieved from: http://ap.ohchr.org/documents/E/HRC/resolutions/A_HRC_RES_7_36.pdf, access: 12.07.2017

United Nations (1990) International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, retrieved from http://www.ohchr.org/Documents/ProfessionalInterest/cmw.pdf, access 05.07.2017

United Nations (1989) Convention on the Rights of the Child, retrieved from http://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf, access 05.07.2017

United Nations - Human Rights Committee (HRC) (1988), HRI/GEN/1/Rev.9 (Vol. I), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, retrieved from: http://www.refworld.org/docid/453883f922.html, access: 12.07.2017

United Nations (1966) International Covenant on Civil and Political Rights, retrieved from http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf, access 05.07.2017

United Nations (1948) Universal Declaration of Human Rights, retrieved from http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf, access 20.06.2017

Waldo, James/ Lin, Herbert S. Lin/ Milett, Lynette I. (edts.) (2007) Engaging privacy and information technology in a digital age, National Academies Press: Washington

Staat, Recht und Politik – Forschungs- und Diskussionspapiere

ISSN (online) 1867-9528

http://nbn-resolving.de/urn:nbn:de:kobv:517-series-914

Herausgegeben von apl. Prof. Dr. iur. Norman Weiß, Universität Potsdam.

Zuletzt erschienene Ausgaben: