October 2015, Tallinn, Estonia

NATO CCD COE and INSCT joint workshop on

'HUMAN RIGHTS IN CYBERSPACE'

1st-2nd of October 2015, Tallinn, Estonia

Workshop Report

Eleven international speakers joined the event on Human Rights in Cyberspace, which was organised in Tallinn, Estonia by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) and the Institute of National Security and Counterterrorism (INSCT), Syracuse University.

Thirty participants joined the debates representing a number of diverse governmental institutions (such as the Ministry of Interior of Iceland, and the Ministries of Foreign Affairs and Justice of Estonia) and NGOs (including Amnesty International (Poland) and Privacy International (London), amongst others). We also had the honour to welcome a good number of experts from academia as well as legal advisers from Germany, and the Czech Republic.

It is now our great pleasure to issue the main findings and discussion aspects collected during the workshop and we would like to thank all the speakers and participants for their excellent contribution.

Part A of this report provides a brief overview on the main topics discussed. Full length academic papers on the presentations will be published at the beginning of 2016 on the NATO CCD COE's website and in the Journal of National Security Law and Policy (JNSLP), a journal co-edited by our cooperation partner, INSCT, and Georgetown University Law Centre.

People interested in receiving a notification on the day of publication of these future publications should contact the project leader at Lorena.Trinberg (at) ccdcoe.org.

Part B reflects the agenda of the event which followed a progressive approach. The workshop started with evolutionary aspects, and continued with debates on specific problems such as the extraterritorial application of human rights treaties, ending with an intriguing debate on future developments in cyber law.

Finally, Part C features the presentation abstracts as well as biographies of the speakers and main people involved in this project.

Lorena Trinberg
NATO CCD COE (GER)
(Project leader)

Tomáš Minárik
NATO CCD COE (CZE)

CPT Pascal Brangetto
NATO CCD COE (FRA)

Contents

A) THE FINDINGS of the workshop

How does international human rights law apply in cyberspace?

Cyberspace, as a space originally without governments, borders, legislation and differentiation, brings many opportunities and commodities to its users. Even though there might be no need for new norms or standards in order to enforce 'cyber justice', i.e. a fair and more equal internet, it was emphasised right at the beginning that there is a need for new systems and mechanisms to guarantee and safeguard human rights in cyberspace. In that regard, the multiplicity of international stakeholders, whether from the private or public sector, poses the questions of who has the responsibility to promote human rights, and who apportions this responsibility.

Most of the aspirational norms that the internet relies upon were drafted during the 1990s, such as the proportional multi-stakeholder approach, the international regulation mechanisms, and a global set of transparent norms for good governance.

By now, it is clear that international human rights law (IHRL) does apply in cyberspace although some states, such as the member states of the Shanghai Cooperation Organisation, may not fully agree. The details of how exactly IHRL applies need to be clarified.

Debates continued as to what extent states are responsible for respecting human rights. This was depicted in multiple ways: states have a duty to respect (a negative duty, non-interference), ensure respect (a positive duty, protection), and promote and fulfil (as in most of International Covenant on Economic, Social and Cultural Rights) human rights. Of these categories, the first two duties are perceived as immediate, while the third is realised progressively. There is no universal human right to internet access (yet), although countries in which constitutions are easy to change may lead the way.

Other interesting questions include: the relationship between IHRL and international humanitarian law (IHL) in cyberspace (the rule exclusion concept and the triggering of IHL application by a cyberattack); territorial scope of application of human rights treaties (how does the doctrine of effective control apply to cyberspace?); and the balance of competing rights, especially when dealing with targeted and bulk surveillance.

Extraterritorial aspects of human rights in cyberspace

The Snowden revelations had a lasting effect for two reasons: first, the US government was conducting targeted surveillance of the leaders of friendly and allied countries, and second, the sheer size of the mass surveillance.

The extraterritorial application of human rights treaties, including the citizen/non-citizen distinction by certain states, has therefore become a major topic for discussion. It was reported that the world can expect significant developments in case law regarding human rights in cyberspace in the near future.

All human rights treaties have jurisdiction clauses with varying wording. From the case law of the European Court of Human Rights (ECtHR) and the International Court of Justice (ICJ), two models of extraterritorial application can be constructed – spatial and personal – both of which have their shortcomings with respect to cyberspace. A solution is thus proposed in the form of distinguishing between the territorially unlimited negative obligation to respect human rights and the limited positive obligation to ensure and secure human rights.

Customary IHRL may also help in solving the problem of extraterritoriality. However, there are two major problems: disentangling treaty law from customary law, and the enforcement of customary law. Also in this context, it was noted that legal advisers are the ones in the position to mediate the limits of IHRL which can be miscommunicated or even ignored.

The question of how states deal with data across borders is becoming a bigger part of the discussion. The question becomes of particular importance when it comes to law enforcement. Delays in accessing data across borders can present a severe problem and impede, for example, criminal investigations. Several

nations assert that they need to obtain metadata or content data for law enforcement purposes directly from companies located abroad which is why certain businesses are being approached and asked to hand over data leading to high grade impact in particular for the right to privacy and freedom of expression. These companies are not subject to human rights treaties, they have no legislative framework or even best practices for deciding whether to hand over the data, and they often do not have the resources to appropriately vet the requests by foreign governments. They often have to act under threats from these governments to arrest their local employees or otherwise hamper their business operations.
Since a single standard created by a multilateral treaty is difficult to achieve, a solution could be found in extending the legal framework for domestic requests for data to extraterritorial requests on the basis of bilateral agreements.

Protecting and promoting IHRL in cyberspace

Freedom of expression and the right to privacy go hand in hand, and one can't exist without the other, even though the definitions of expression and privacy are notoriously different from country to country, as can be seen on the difference between Europe and US.
Surveillance has always been there – it is the massiveness of the surveillance that makes the difference. There will always be a need for surveillance, such as in fighting terrorism, but a distinction must be drawn between targeted and untargeted surveillance. Mass surveillance is intrinsically illegal. It's being done because it's easy to do. It was argued that any form of surveillance should follow clear rules. Necessity, proportionality and a clear rule foreseen in a law are the basics every state should have in mind when conducting these activities. Thus, surveillance activities should be approved by an authority, be supervised by an additional authority and be bounded by a time limit. In addition, it was suggested that a person under surveillance should be notified in due course, and the idea of implementing an export control of surveillance technologies was discussed.
Anonymity was one more aspect mentioned and it is considered as one way to fight the trend of major states to conduct mass data collection. Taking away anonymity from people would therefore be dangerous in the current environment. The use of personal data for commercial purposes is also a major issue that can be addressed by anonymising tools.
Civil society, including NGOs, can play a vital role in the development of law and policy. Governments of certain EU countries are trying to weaken their domestic standards of protection of human rights, expanding domestic surveillance without establishing effective accompanying oversight and whistle-blower protection, and using surveillance and police methods to intimidate activists. Promoting encryption and anonymising tools is especially important in such conditions. Some examples of privacy-enhancing technology tools provided by certain websites for journalists, activists and the general public were therefore highlighted as examples of the practical implementation of the right to privacy and the right to freedom of expression.

Sources and kinds of conflicts involving IHRL in cyber

The aspect of anonymity was revived in this panel and questions such as 'Is there actually a right to anonymity related to the right to freedom of expression, and is it in itself a value for democratic development?' were raised. The legal recognition and protection of this 'right' poses difficulty as there are different degrees of anonymity on the Internet.
The Delfi case was in the focus of the debates. In *Delfi v. Estonia*, the Grand Chamber of the ECtHR tried to strike a fair balance between the right to freedom of expression and the right to privacy (including honour and reputation). It is not ready to depart from the traditional approach to media outlets. A middle ground is to be found, because the free flow of ideas must not hinder the investigation of criminal activities. It was ultimately the heinous and extreme nature of the comments that deprived them of protection. Nevertheless, the ECtHR decision continues to attract substantial criticism from human rights scholars.

Source protection and intermediary protection were pointed out later in the discussions as necessary for the maintenance of the freedom of expression. Iceland, for example, is trying to lead the way in promoting digital privacy, since its Parliament passed the 'Icelandic Modern Media Initiative' resolution in 2010, which is to gradually make Iceland a safe haven for journalists. It was remarked that there is also an initiative to create a database of best practices in this regard, focusing on legal texts.
The discussion on this panel ended by bringing up the Inter-Parliamentary Union, the focal point for world-wide parliamentary dialogue as one example of the many fora which voice their opinions on mass surveillance, along with bodies like Parliamentary Assembly of the Council of Europe, United Nations Office of the High Commissioner for Human Rights, and the United Nations General Assembly.

Reforms of cybersecurity norms – future aspects

We have witnessed the commodification of the internet and there is an utter falsification when internet gurus say that it is so unique that it has to be dealt with specific regulations. If we compare it to radio broadcasting, the internet is just another tool to convey information.
However, in the context of national security, the special powers given to the authorities require special legitimation processes in order to respect the checks and balances principles. The oversight of certain activities needs to be absolute and needs to be able to redress the injustices of surveillance.
Ten standards for oversight and transparency of national intelligence services were thus proposed, providing a 360 degree approach. In short, the completeness of oversight regarding all stages of surveillance at all times, prior, ongoing, and subsequent; a strong mandate, independence, and adequate budget of supervisory bodies; and a layered transparency involving civil society and individuals.
National intelligence services are using big data analysis of trans-border data flows for their purposes. This analysis is done on traffic data and other forms of metadata, and can reveal much personal information, perhaps more than content data can – while the content of communications reveals what we say, the metadata reveal what we do. Encryption does not protect against operations involving metadata, and anonymising tools like Tor can be inconvenient when we want to use them all the time.
Big data analysis (data collection and use) can help find terrorists, even though the exact effect is disputed. However, there are differences in law and policy between the EU and the US with respect to data collection. According to Opinion 04/2015 of the European Data Protection Supervisor, even data collection is subject to EU data protection principles. This is contradictory to the US policy (PPD-28), which only regulates the use of collected data and not the collection itself.
The speaker mentioned the 1995 EU Data Protection Directive and the controversies regarding the Safe Harbour decision, which was on 6 October 2015 ruled invalid by the Court of Justice of the European Union (the workshop narrowly preceded the CJEU ruling invalidating the decision). Ultimately, it can be the economic interests of US companies in the EU market that may drive the development towards a better protection of personal data throughout the world.

Food for thought

Lastly, the following comments and statements (not necessarily made by the speakers) came up during our debates and they might serve as food for thought.

- Rather than law leading technology, it is the other way round, as we observe a technological arms race. For better than for worse, technology works faster than law.
- The statements by Mr. Snowden and Mr. Cannataci – the first UN Special Rapporteur on the right to privacy – about a new international treaty on human rights in cyberspace are a 'complete non-starter' which would draw the precious attention of the public towards an unattainable goal.
- A good human rights rapporteur should not be a human rights activist antagonising part of his constituency.
- A government can switch on bulk surveillance for a limited time, such as due to the risk of a terrorist attack, but indiscriminate ubiquitous surveillance is in contravention of IHRL.
- Mass surveillance is like going through the haystack to find out what kind of needle you are looking for.
- An interesting analogy can be drawn between bulk surveillance in IHRL and weapons of indiscriminate effect in IHL.
- If a US company were to comply with the request for data from a foreign government, the US government could bear the responsibility in accordance with Article 5 of Draft Articles on Responsibility of States for Internationally Wrongful Acts due to the fact that it delegated the exercise of its powers to a person or entity.
- The distinction between content and metadata is becoming less important with respect to human rights protection, as a person's life may be reconstructed more easily from metadata ('content data shows what you say, metadata shows what you do').

B) THE AGENDA of the workshop

NATO CCD COE and INSCT joint workshop on

'HUMAN RIGHTS IN CYBERSPACE'

1st-2nd of October 2015, Tallinn, Estonia

Scoping, Protecting, Regulating International Human Rights Law and Tackling Future Aspects of Cyber Norms

DAY I, Thursday, 1st October 2015

08:30-08:45 Opening and Welcome Words

- Lieutenant Colonel Jens van Laak, NATO CCD COE, Deputy Director and Chief of Staff
- William C. Banks, Professor, Founding Director of the Institute for National Security and Counterterrorism (INSCT), Syracuse University, USA
- Gabor Rona, Chair, visiting Professor of Law, Benjamin N. Cardozo School of Law; former International Legal Director of Human Rights First, NY, USA

1. The scope of IHRL as it applies in cyber with a particular focus on the
- ❖ **Right to respect for private life and correspondence as well as**
- ❖ **Right to freedom of opinion and expression**

08:45-09:35

- The rule of law: The meaning and evolution of the right to privacy in the cybersecurity debate
  Anja Mihr, Associate Professor, Netherlands Institute of Human Rights, Faculty of Law, Governance and Economics, Utrecht University, The Netherlands

09:35-10:25

- State Responsibility to Respect, Ensure Respect, and Fulfill Human Rights Obligations in Cyberspace
  Gabor Rona, Chair, visiting Professor of Law, Benjamin N. Cardozo School of Law; former International Legal Director of Human Rights First, NY, USA

2. Extraterritorial aspects of Human Rights

10:45-11:35

- The extraterritorial application of Human Rights treaty obligations
  Marko Milanovic, Associate Professor, University of Nottingham School of Law, UK

11:35-12:25

- Rights in cyberspace: custom and UN law
  Ralph Wilde, Reader in Law, University College London, UK

13:30-14:20

- Law Enforcement Access to Data Across Borders
  Jennifer Daskal, Assistant Professor of Law, American University Washington College of Law, USA

3. Protecting and promoting IHRL in cyberspace – effective enjoyment of IHRL

14:20-15:10

- Communication surveillance and surveillance frameworks
  Frank La Rue, Human Rights lawyer, former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Guatemala

15:30-16:20

- Right to privacy in practice: Privacy enhancing technology- project on a new infosite of the HCLU
  Rita Zágoni, Data Protection Programme Officer, Hungarian Civil Liberties Union, Budapest, Hungary

END OF DAY I

DAY II, Friday, 2nd October 2015

4. Sources and kinds of conflicts involving IHRL in cyber

08:30-09:20

- The right to freedom of expression and the right to anonymity in cyber
  Robert R. Spano, Judge, European Court of Human Rights, Strasbourg, France

09:20-10:10

- Who should protect your digital shadow?
  Birgitta Jónsdóttir, Member of the Icelandic Parliament, Chairperson of the International Modern Media Institution, poetician, Reykjavik, Iceland

5. Reforms of cybersecurity norms – future aspects

10:30-11:20

- Standards for transparency and oversight in national security regulation
  N.A.N.M. van Eijk, Professor of Information Law, University of Amsterdam, The Netherlands

11:20-12:10

- The cyber future of privacy norms in the context of 'traffic-data', particularly cross-border dataflow
  Henning Lahmann, journalist at iRights, lawyer and freelance researcher, Berlin, Germany

END OF THE WORKSHOP

C) BIOGRAPHIES and ABSTRACTS

From left to right:

Professor Gabor Rona; Lorena Trinberg (project leader); Professor William C. Banks; Tomaso Falchetta; Henning Lahmann; Professor N.A.N.M. van Eijk; Rita Zagoni; Associate Professor Marko Milanović; Birgitta Jónsdóttir; Ralph Wilde; Ele-Riin Kullamä (project assistant); Frank La Rue; Professor Anja Mihr; Assistant Professor Jennifer Daskal; Judge Robert R. Spano.

Professor Anja Mihr

Anja Mihr currently replaces the Franz Haniel Chair of Public Policy at the Willy Brandt School for Public Policy at the University of Erfurt. She previously has been Assoc. Professor at the Netherlands Institute of Human Rights (SIM), University of Utrecht, Netherlands; and is founder and Program Director of the HUMBOLDT-VIADRINA Center on Governance through Human Rights in Berlin, Germany.

She is one of two principle investigators and research directors of the European ORA project on the Impact of Transitional Justice on democratic institution building. Her work focuses on Public Policy, Governance, Human Rights and Comparative Studies.

She has been Head of the Rule of Law department at The Hague Institute for Global Justice and carried out a number of Visiting Professorships for Human Rights such as at Peking University Law School in China together with the Raoul Wallenberg Research Institute on Human Rights, Lund University in 2008. From 2006-2008 she was the European Program Director for the European Master Degree in Human Rights and Democratization (E.MA) at the European Inter-University Center for Human Rights in Venice (EIUC), Italy. She received her Ph.D in Political Sciences from the Free University in Berlin, Germany, in 2001.

Mihr has worked for Amnesty International, the GIZ, the United Nations and European Union as well the German Institute for Human Rights. Starting as a assistant professor with UNESCO Chair in Human Rights at the University of Magdeburg in 2002 in Germany, she was later a research director at the Humboldt University of Berlin carrying out the research project "Teaching Human Rights in Europe" from 2003-2006. From 2002-2006 Anja Mihr also served as Chair of Amnesty International Germany.

She has published a number of books and articles on international human rights regimes, human rights education, transitional justice, European human rights system and NGOs and has been co-editor of the

European Yearbook of Human Rights as well as the German Journal for Human Rights.

Abstract: *The rule of law: The meaning and evolution of the right to privacy in the cybersecurity debate*

Cyber Justice as a viable approach for promoting good governance based on human rights norms in the internet and thus establishing a Rule of Law in Cyberspace. Cybersecurity is a specific security issue in cyberspace as a borderless public space without common global rules or government control mechanisms that protect and foster people's activities within that space. In the light of the growing scope of communications and interactions in the internet, the author shows how human rights and governance regimes can be adapted to cyberspace in order to ensure more accountability, transparency and interaction among those who use the internet and those who manage and provide internet services.

Human rights are equally valid offline as they are online, new standards are not needed let alone specific 'cyber rights'. The idea of the rule of law for the internet and cyberspace is based on the existing values, norms and standards. The challenge is how to convert these norms and standards into a legally, politically and socially binding agreement that every 'user' and 'server' can adhere to.

Professor Gabor Rona

Gabor Rona is a member of the International Group of Experts engaged in the Tallinn Manual project.

He is also a Visiting Professor of Law at Cardozo Law School in New York, where he teaches international human rights law, international humanitarian law, and directs the Law and Armed Conflict Project of the Cardozo Law Institute on Holocaust and Human Rights.

Mr. Rona previously served as the International Legal Director of Human Rights First and before that, as a Legal Advisor in the Legal Division of the International Committee of the Red Cross (ICRC) in Geneva. His articles on the application of international humanitarian and human rights law in the context of counter-terrorism policies and practices, among other subjects, have appeared in many journals. He has also taught International Humanitarian Law, International Human Rights Law and International Criminal Law at the International Institute of Human Rights in Strasbourg, France, the University Centre for International Humanitarian Law in Geneva, Switzerland and Columbia Law School in New York. He is also a member of the Board of Directors of the International Justice Resource Center and a member of the Executive Committee of the American Branch of the International Law Association.

Mr. Rona received his B.A. from Brandeis University, J.D. from Vermont Law School and LL.M from Columbia Law School.

Abstract: *State Responsibility to Respect, Ensure Respect and Fulfill Human Rights Obligations in Cyberspace*

Whenever a new technology surfaces, questions arise concerning whether and how old rules of international law apply and whether new rules are needed.

Cyberspace creates tremendous new opportunities for all to enjoy human rights to expression, association, participation in the political process and for the advancement of social, economic, and cultural rights. At the same time, the Internet presents unprecedented challenges to human rights through cyber attacks, surveillance and its ability to function as a platform for crime and incitement of violence through hate

speech and recruitment to terrorism. The universality of the Internet also challenges traditional notions of State sovereignty - the right of each State to decide for itself how to navigate these issues.

These new tensions have caused some to question the very application of human rights law to cyber space, but while technological advances may require new thinking about how human rights apply, there is little doubt that they do apply and that States have obligations to respect, ensure respect and promote rights in cyber space. The obligation to respect is a "negative" obligation, prohibiting or limiting State interference with rights of free expression, association, and privacy, among other rights. The obligation to ensure respect, or protect, is a "positive" obligation requiring States to enact laws and policies that prevent, punish and remedy violations of those rights by third parties. Finally, the obligation to promote, derived from the International Covenant for Economic, Social and Cultural Rights' mandate of 'progressive realization' of such rights, may be the least developed frontier for human rights in cyber space. While there is no present indication that States must provide access to the Internet, the increasing criticality of the internet to all activities of life suggests that there is much law to be developed in respect of States' obligation of progressive realization of human rights in cyber space.

Dr Marko Milanovic

Dr Marko Milanovic is associate professor at the University of Nottingham School of Law. He obtained his first degree in law from the University of Belgrade Faculty of Law, his LL.M from the University of Michigan Law School, and his PhD in international law from the University of Cambridge. He is Vice-President and member of the Executive Board of the European Society of International Law, an Associate of the Belgrade Centre for Human Rights, and co-editor of *EJIL: Talk!*, the blog of the European Journal of International Law, as well as a member of the EJIL's Editorial Board. His has published, inter alia, *Extraterritorial Application of Human Rights Treaties: Law, Principles and Policy* (OUP, 2011) and 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,' (2015) 56 *Harvard International Law Journal* 81.

Abstract: *The extraterritorial application of Human Rights treaty obligations*

This presentation will look at the main strands of international jurisprudence dealing with the extraterritorial application of human rights treaties, and examine how they might apply to electronic surveillance and other cyberspace activities. The only truly coherent approach to the threshold question of applicability, I will argue, is that human rights treaties should apply to virtually all foreign surveillance activities. That the treaties apply to such activities, however, does not mean that they are necessarily unlawful. Rather, the lawfulness of a given foreign surveillance program is subject to a fact-specific examination on the merits of its compliance with the right to privacy, and in that, I submit, foreign surveillance activities are no different from purely domestic ones.

Dr Ralph Wilde

Dr Ralph Wilde is a member of the Faculty of Laws at University College London, University of London. His current research focuses on the extraterritorial application of international human rights law. His book *International Territorial Administration: How Trusteeship and the Civilizing Mission Never Went Away* (Oxford University Press, 2008) was awarded the Certificate of Merit (book prize) of the American Society

of International Law in 2009. He is a member of the Executive Board of the European Society of International Law, having previously served on the Executive Council of the American Society of International Law and, at the International Law Association (ILA), as Co-Rapporteur of the Human Rights Committee, one of the UK representatives on the international Executive Council, Rapporteur of the Study Group on UN Reform, and Joint Honorary Secretary of the British Branch. Ralph has held visiting positions at the Central European University in Budapest, Melbourne University, NYU, Texas University, UCLA, Yale Law School, and the Fundação Casa Rui Barbosa, Rio de Janeiro. He has been awarded grants for his research from the UK Arts and Humanities Council, the British Academy and the Nuffield Foundation; a Research Fellowship and the Philip Leverhulme Prize by the Leverhulme Trust; and a 'Starting Grant' (in the 'Consolidator' Category) from the European Research Council, the EU's academic research funding body. More information: http://www.laws.ucl.ac.uk/people/ralph-wilde/

Professor Jennifer Daskal

Jennifer Daskal is an Assistant Professor of Law at American University Washington College of Law. From 2009-2011, Daskal was counsel to the Assistant Attorney General for National Security at the Department of Justice. Prior to joining DOJ, she was the senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakoff. Daskal is a graduate of Brown University, Harvard Law School, and Cambridge University, where she was a Marshall Scholar. She is an Executive Editor of the Just Security blog.

Abstract: Law Enforcement Access to Data Across Borders: The Evolving Human Rights Issues

The Edward Snowden revelations provoked a wide-ranging debate regarding U.S. surveillance practices—yielding multiple reports, international backlash, and media attention. Meanwhile, an equally important, yet largely overlooked, revolution is underway with respect to *law enforcement* access to data outside its borders. Frustrated by delays in accessing data across territorial borders, several nations—including the U.S., the UK, Brazil, and multiple others—are asserting that they can unilaterally compel the production of emails and other private communications stored in other nation's jurisdictions. This is a critically important issue, with profound implications for privacy, speech, and associational rights, and for the power of the state to mark and control. Yet it has received little attention—overshadowed by the focus on foreign surveillance practice, with little recognition of the interplay between law enforcement and intelligence authorities in this area. Among other concerns, Internet Service Providers and other corporate entities are increasingly being asked to unilaterally vet requests for data and decide—often without any legal framework or even best practices to fall back on—when and under what circumstances to turn over requested data. In some cases, the companies do so under the threat of arrest or prosecution of local workers.

This article seeks to bring attention to the issue of *law enforcement* access to data across borders. Its aims are threefold: (i) to identify the trends; (ii) explore key human rights issues that have emerged; and (iii) suggest some tentative suggestions as to a way forward. The three parts of the article track these three goals.

Mr Frank La Rue

Frank La Rue is the Executive Director of Robert F. Kennedy Human Rights Europe and former UN Special Rapporteur for the promotion and protection of the right to the freedom of opinion and expression (2008-14). He is widely respected as one of the world's foremost human rights advocates, with particular expertise in political analysis; democratic development; and conflict management, negotiation, and resolution.

A lawyer by training, Mr. La Rue is also a journalist, and has served in the Cabinet of the Government in his native Guatemala as Presidential Secretary for Human Rights, and has frequently taught and written about human rights.

Ms Rita Zágoni

Rita Zágoni is Head of Data Protection Program and Officer of Freedom of Information Program at the Hungarian Civil Liberties Union. With a background in sociology, philosophy and programming, her work focuses on the technological and legal aspects of protecting online privacy and on the dangers new technologies pose to privacy. She also holds workshops for journalists and civil society activists on using technology in their work, especially privacy enhancing and data security tools, and tools for data analysis.

Abstract: Right to privacy in practice: Privacy enhancing technology - project on a new infosite of the HCLU

The Hungarian Civil Liberties Union (HCLU) is creating a website to raise awareness among the Hungarian general public, journalists and activists about the importance of protecting privacy online, to provide practical guidance, tools and tips for using privacy enhancing technologies. We think giving a technological answer to a question of right to privacy is legitimate because currently in Hungary the law is not providing adequate protection. The main points of concern are the lack of oversight of surveillance powers and inadequate whistle-blower protection. After detailing the legal context, the presentation will describe the principles we kept in mind when choosing the technological tools to present, give an overview of the site structure and content, and will offer a short demonstration of some privacy enhancing tools.

Judge Robert Spano

Judge Robert Spano was elected to the European Court of Human Rights in 2013 with respect to Iceland. Before taking up his judicial office he served as Parliamentary Ombudsman of Iceland from 2009-2010 and again in 2013. He served as Dean of the Faculty of Law, University of Iceland, from 2010-2013, and was appointed professor of law in 2006. He was chairman of the Standing Committee of Experts in Criminal Law in the Ministry of Justice from 2003-2009 and from 2011-2013. He was also the Icelandic delegate to the European Committee on Crime Problems and an Independent Expert to the Lanzarote Committee of the Council of Europe. He was appointed an ad hoc judge of the EFTA Court in 2012. Judge Spano is a graduate of the University of Iceland and of the University of Oxford.

Ms Birgitta Jónsdóttir

Birgitta Jónsdóttir is a Poetician for the Pirate Party in the Icelandic Parliament & chairman for IMMI (International Modern Media Institute).

Birgitta has helped create two political movements since 2009, the Civic Movement and the Pirate Party, both parties have successfully entered the Icelandic Parliament. The Pirate Party has been scoring in the polls as the most popular party in Iceland in 2015.

She specializes is 21st century lawmaking with focus on direct democracy, freedom of expression, information and digital privacy. She is a hacker in parliament. Birgitta is long time activist and was a WikiLeaks volunteer when the largest leak in human history was dropped into the digital dropbox of the organization by the courageous whistleblower Chelsea Manning. She played a crucial role in WikiLeak's release of *Collateral Murder*.

Birgitta put forward early 2010 the IMMI parliamentary resolution tasking Icelandic governments to write the 10 laws described in the resolution. The aim of resolution is to make Iceland a safe haven for freedom of expression, information and digital privacy. It was unanimously adopted. The creation of the IMMI laws is ongoing.

Birgitta is a regular contributor to the Guardian newspaper and had the honour to guest edit the January edition 2015 of the New Internationalist titled Democracy in the Digital era.

She believes individuals can and should change the world.

Abstract: Who should protect your digital shadow?

When the whistleblower Edward Snowden brought light to the incredible network of mass surveillance by both governmental agencies and private corporations, there were demands to amend this serious breach of privacy and individual freedoms such as freedom of expression and freedom of association. Everyone who understands fundamental rights knows that these rights are the basic conditions for the exercise of functional democracy. The digital era is vastly expanding the opportunities people have to communicate and receive information and to express their opinions. This is beneficial for democracy, as people can more easily participate in debate and decision-making, and can obtain information that helps them to hold governments to account. New forms of political participation are emerging, which may in time lead to changes in the organisation of political parties and the system of representative democracy.

The digital era provides governments and private companies with unprecedented technological means for gathering information about citizens' online activities. This poses a potential threat to privacy and individual freedoms, and therefore to democracy itself.

The UN General Assembly adopted resolutions on the right to privacy in the digital age in December 2013 and December 2014. The resolutions call on all States to respect and protect the right to privacy, including in the context of digital communication. The UN High Commissioner for Human Rights issued a report in June 2014, and continues to follow the issue closely. A significant gap nevertheless remains between the norms set out in international law and practice at national level and it must be up to the world's parliaments and individual parliamentarians to call for changes and better respect for human rights in practice.

Professor Nico van Eijk

Nico van Eijk is Professor of Media and Telecommunications Law and Director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam).

Among other things, he is the Chairman of the Dutch Federation for Media and Communications Law (VMC), a member of the supervisory board of the Dutch public broadcasting organization (NPO) and a member of the 'knowledge circle' of the Dutch Review Committee on the Intelligence and Security Services (CTIVD).

He co-authored a first report on the Patriot Act before the Snowden revelations (http://www.ivir.nl/publicaties/download/684) and the recent study: 'Ten standards for oversight and transparency of national intelligence services' (http://ivir.nl/publicaties/download/1591). More on his work: http://www.ivir.nl/medewerkerpagina/eijk

Abstract: Standards for transparency and oversight in national security regulation

The Snowden revelations have sparked unprecedented interest in the activities of intelligence services. Technological developments have made sophisticated surveillance technologies more accessible to governments across the globe, whereas the revelations demonstrated the impact of these technologies. Partly as a consequence of these developments, policymakers are reviewing the national legal framework for the activities of these services, not only to expand but also to curtail surveillance powers.

In a recently published report ('Ten Standards for oversight and transparency of national intelligence services'), we have identified ten core standards for oversight and transparency. These standards are intended to provide practical guidance for those who seek further input for discussions, policymaking and the review of existing legislation.

The standards are based on an analysis of European human rights jurisprudence of the past decades. While studying the decisions of the European Court of Human Rights and the Court of Justice of the European Union, the project mostly focused on the interception of communication, but the policy recommendations are also applicable to oversight in other areas.

According to the findings of the report, national intelligence services in Europe should be subject to independent oversight, preferably by a judge. Other recommendations include that intelligence services should be subject to prior oversight and that governments should be transparent about the exercise of surveillance powers. In many European countries prior oversight of intelligence services is almost completely lacking. In addition, it's often not allowed to publish statistics on the exercise of surveillance powers.

Sarah Eskens, Ot van Daalen and Nico van Eijk, 'Ten Standards for oversight and transparency of national intelligence services', Institute for Information Law (IViR, University of Amsterdam). Download: http://www.ivir.nl/publicaties/download/1591

Mr Henning Lahmann

Henning Lahmann works as a political analyst at the Berlin-based think tank iRights.Lab, which consults various clients in all matters concerning the digital society such as civil rights on the internet, data protection, and copyright issues. He furthermore is a freelance journalist and has written for Wired Germany and Merkur, among others. From 2008 to 2013, Lahmann was a research fellow at the Walther Schücking Institute for International Law in Kiel and at the University of Potsdam, working for Prof. Andreas Zimmermann. He is about to finish his PhD on international cyber security law.

Professor William C. Banks

Professor William C. Banks is an internationally recognized authority in national security law, counterterrorism, and constitutional law. Banks has helped set the parameters for the growing field of national security law since 1987, co-authoring two leading texts in the field: National Security Law and Counterterrorism Law. In 2008, Banks was named the College of Law Board of Advisors Distinguished Professor at Syracuse University, where he has been a member of the faculty for over 30 years. Banks is also the author or editor of numerous other books, book chapters and articles including Counterinsurgency Law: New Dimensions in Asymmetric Warfare, Combating Terrorism (with Mitchel Wallerstein and Renee de Nevers), New Battlefields/Old Laws: Critical Debates from the Hague Convention to Asymmetric Warfare, "Legal Sanctuaries and Predator Strikes in the War on Terror," "Programmatic Surveillance and FISA – Of Needles in Haystacks," and "Providing 'Supplemental Security' – The Insurrection Act and the Military Role in Responding to Domestic Crises." Since 1998, Banks also has been a Professor of Public Administration in SU's Maxwell School of Citizenship and Public Affairs. He was named the Laura J. and L. Douglas Meredith Professor for Teaching Excellence in 1998, a College of Law Board of Advisors Professor in 2005, and he became the founding director of the Institute for National Security and Counterterrorism at Syracuse University in 2003. He is also the Editor-in-Chief of the Journal of National Security Law & Policy (JNSL&P).

Ms Lorena Trinberg, LL.M.

Lorena Trinberg is a legal analyst of German and Colombian descent at the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). Having passed her bar exam in Düsseldorf, Germany and after having received an LL.M. degree in International Law from the University of Bern, Switzerland, she decided to join the German Federal Armed Forces initially as a litigator. Being deployed, she currently lives in Tallinn, Estonia where she contributes to various projects in the Law & Policy branch of the NATO CCD COE. She is responsible for conducting legal research on topics related to cyber security and cyber defence such as, inter alia, on the legal obligations of critical information infrastructure operators. She is also a frequent contributor to the NATO CCD COE 'Incyder newsletter', where she publishes brief updates on cyber security policy developments of different organisations. As the project leader of this workshop, her current research focuses on the field of 'Human Rights in Cyberspace'.

NATO Cooperative Cyber Defence Centre of Excellence

The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence is a NATO-accredited knowledge hub, think-tank and training facility. The international military organisation focuses on interdisciplinary applied research and development, as well as consultations, trainings and exercises in the field of cyber security. The Centre's mission is to enhance capability, cooperation and information-sharing between NATO, Allies and partners in cyber defence.

Membership of the Centre is open to all Allies. As of October 2015, the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, Greece, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the USA have signed on as sponsoring nations. Austria and Finland have joined the Centre as contributing participants.

The Institute for National Security and Counterterrorism

The Institute for National Security and Counterterrorism (INSCT) is a multidisciplinary, university-based center for the study of national and international security and terrorism, offering law and graduate certificates of advanced study and conducting incisive research and timely policy analysis. Part of Syracuse University's College of Law and Maxwell School of Citizenship and Public Affairs, INSCT's collaborative projects have shaped law and policy dialogues for more than 10 years.