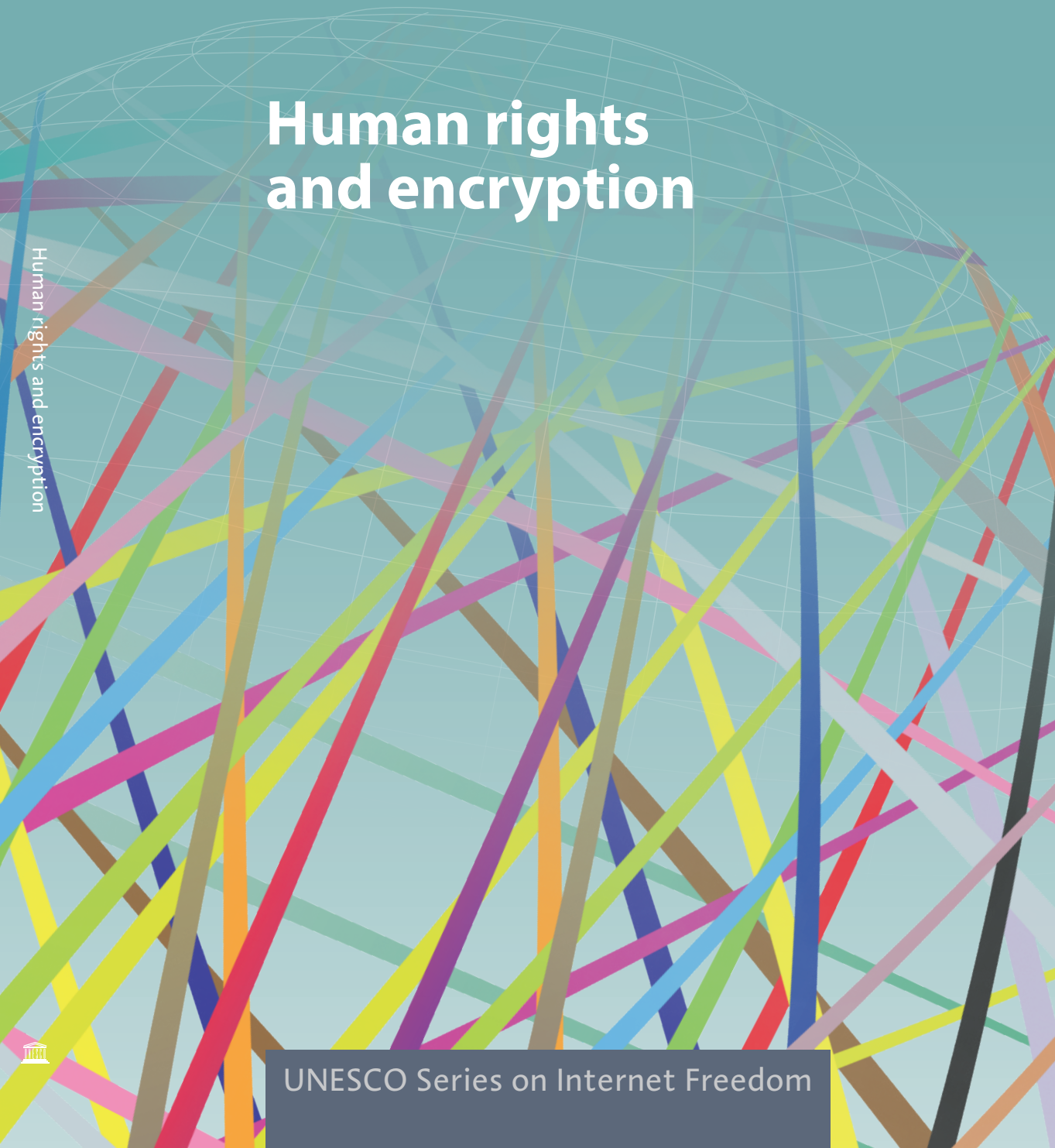
UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

Human rights and encryption

Human rights and encryption



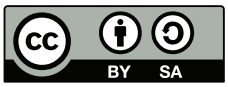
UNESCO Series on Internet Freedom

Wolfgang Schulz
Joris van Hoboken

Human rights and encryption

Published in 2016 by the United Nations Educational, Scientific and Cultural Organization,
7, place de Fontenoy, 75352 Paris 07 SP, France

ISBN 978-92-3-100185-7



The authors thank those reviewers and other contributions on country reports, as well as research assistance.

Reviewers:
- Mr Eduardo Bertoni, Director, National Data Protection Authority, Argentina;
- Ms Deborah Brown, Association for Progressive Communications (APC), South Africa;
- Mr Danilo Doneda, State University of Rio de Janeiro, Brazil;
- Mr Joseph Lorenzo Hall, CDT (Center for Democracy and Technology), U.S.;
- Ms Christine Runnegar, The Internet Society;
- Mr Ben Wagner, Director, Center for Internet & Human Rights, European University, Viadrina, Germany.

Input and sources:
Seda Gürses, Ira Rubinstein, Chinmayi Arun, Sarvjeet Singh, Joshita M. Pai, Eduardo Magrani, Daniel Kahn Gillmor.
Research Assistance:
Felix Krupar, Tobias Mast, Julian Staben.

UNESCO thanks the support of the German Federal Foreign Office for delivering this publication.

Cover illustration: © Shuttershock/greiss design

Typeset and printed by UNESCO
Printed in France

Table of contents

Foreword

This publication follows UNESCO's new approach to Internet issues, as endorsed in November 2015 on the occasion of its 38th General Conference. Our 195 Member States have adopted the CONNECTing the Dots Outcome Document, in which 38 options for future action from UNESCO are set out; and the Internet Universality principles (R.O.A.M.), which advocate for a human-Rights-based, Open and Accessible Internet, governed by Multi-stakeholder participation.

In line with this mandate, UNESCO strives to continuously engage stakeholders across international processes and fora to advance understanding of issues that impact on online freedom of expression, such as safety, privacy, transparency, encryption, source protection, hate speech and radicalisation in the digital age.

The present research was elaborated in the effort to implement Internet Universality framework. Specifically, it also responds to the option recommended by the CONNECTing the Dots Outcome Document that UNESCO "recognizes the role that anonymity and encryption can play as enablers of privacy protection and freedom of expression, and facilitates dialogue on these issues".

In addition, the research draws on the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, which was presented to the Human Rights Council in June 2015.

Encryption is a hot topic in the current global discussion on Internet governance. This research delves into the subject, to outline a global overview of the various means of encryption, their availability and their potential applications in the media and communications landscape. The research explains how the deployment of encryption is affected by different areas of law and policy, and it offers detailed case studies of encryption in selected jurisdictions. It analyzes in-depth the role of encryption in the media and communications landscape, and the impact on different services, entities and end users. Built on this exploration and analysis, the research provides recommendations on encryption policy that are useful for various stakeholders. These include signaling the need to counter the lack of gender sensitivity in the current debate, and also highlighting ideas for enhancing "encryption literacy".

This flagship publications series on Internet Freedom was begun in 2009, with two main goals: to explore the Internet's changing legal and policy issues; and to provide recommendations for Member States and other stakeholders interested in fostering an environment more conducive to freedom of expression online.

In addition to serving as a new knowledge resource to facilitate international dialogue and collaboration on encryption issues, we hope that this new edition will prove valuable in

providing knowledge, policy options and recommendations in the area of encryption – for UNESCO, its Member States, as well as civil society, private sector and academia.

UNESCO expresses its thanks to Prof. Wolfgang Schulz and to Dr. Joris Van Hoboken, for having delivered this comprehensive and in-depth assessment. UNESCO also thanks those international experts who have kindly reviewed the draft and provided their valuable inputs.

Frank La Rue

Assistant Director
General of UNESCO

Executive summary

This study focuses on the availability and use of a technology of particular significance in the field of information and communication: encryption, or more broadly cryptography. Over the last decades, encryption has proven uniquely suitable to be used in the digital environments. It has been widely deployed by a variety of actors to ensure protection of information and communication for commercial, personal and public interests. From a human rights perspective, there is a growing recognition that the availability and deployment of encryption by relevant actors is a necessary ingredient for realizing a free and open internet. Specifically, encryption can support free expression, anonymity, access to information, private communication and privacy. Therefore, limitations on encryption need to be carefully scrutinized. This study addresses the relevance of encryption to human rights in the media and communications field, and the legality of interferences, and it offers recommendations for state practice and other stakeholders.

This publication explores these issues in the context of UNESCO's new approach to Internet issues. The approach was adopted by our 195 Member States in November 2015, and is based on the Outcome Document of an earlier conference called CONNECTing the Dots. Concretely, this means that UNESCO stands for the concept of "Internet Universality" and the related "ROAM principles" which refer to a (human) Rights-based, Open and Accessible Internet that is governed by Multi-stakeholder participation.

In **Section 2**, the study gives an overview of encryption as an increasingly essential element of the media and communications landscape, distinguishing between encryption that is implemented by service providers and encryption that is used by end-users directly. The study also clarifies the diversity of properties of information and communication that encryption can help to guarantee, including confidentiality, privacy, authenticity, availability, integrity and anonymity.

In **Section 3**, the study explains how the deployment of encryption technologies and solutions is affected by different areas of information law and policy, including the law of electronic commerce, data protection law and government access to data and communications. The issue of the design of encryption backdoors in view of lawful government access is considered, as well as the development of norms at the international level, through the OECD guidelines and the official reports of relevant UN Rapporteurs.

Section 4 offers more detailed case studies on the current state of encryption policy in selected jurisdictions (Germany, United States, India, Brazil and the African region). These case studies look at encryption policy seen from the perspective of a general typology of restrictions on encryption (e.g. export controls) as well as positive measures to stimulate encryption availability and adoption (e.g. in data privacy regulation). In none of the selected jurisdictions, is there an outright ban on the use of encryption but the extent to which encryption policy has been liberalized for private sector use differs. More specifically, there can be significant legal uncertainty about the precise legal status of encryption, which functions as a de facto limitation on its use. The study also discusses recent proposals in the USA and elsewhere that would restrict the availability of secure encryption for internet users in view of government access to information and communication.

Section 5 discusses the implications of encryption for human rights and media and communications. Limitations on encryption potentially interfere with the right to freedom of expression and the right to private life as protected at the international level. The study furthers three specific perspectives of concern in this regard.

First, encryption supports the requirement of uninhibited communications by allowing people to protect the integrity, availability and confidentiality of their communications, which would be vulnerable otherwise. This requirement is an important precondition for freedom of communication and needs to find strong recognition at the international level.

Second, when policy or legislation leads to limitations on encryption and its security properties, procedural safeguards, including the principle of transparency should be observed. This is particularly relevant for the situation in which states do not take formal action but rely on the cooperation of private actors and the industry to implement measures that affect encryption.

Third, the study notes the important role of intermediary service providers in providing for the protection of their users' experience on their platforms. Specifically, online intermediaries not only have the role of intermediaries in relation to content and connecting users, but also one of security intermediaries, as their practices and defaults as regards encryption are highly relevant to the user's access to and effective usage of those technologies.

Section 6 offers recommendations as insights that can be useful for various stakeholders, to properly address the human rights issues involved. The recommendations target different stakeholder groups and the particular role they play in the overall system, including governments, international organizations, the technical community, the private sector, and civil society, including users and academia. In its recommendations, the study notes the lack of gender sensitivity in the current debate and existing policy with respect to encryption and the need to address the position of vulnerable communities.

1. Introduction

Context for the study

> "Cryptography rearranges power: it configures who can do what, from what."[1]

We live in a world in which technologies mediate an ever larger portion of society. Innovations in the field of information and communication technologies, services and practices continue to reshape relationships between societal actors. Because of their architectural capabilities, these innovations can result in the furthering of fundamental values, including access to information and knowledge, the protection of privacy or the ability to communicate freely.[2] Clearly, choices about technological design can also result in the erosion or interference with such values, if insufficient energy, time and resources are spent or when policies are adopted that unduly restrict their use or deployment. Thus, the task for policy makers and other stakeholders is to consider the design of architectures and to help ensure the protection of fundamental values at stake at the level of technological infrastructures. Relevant stakeholders should also recognize that those technologies do not completely determine the development, since they are embedded in social practices. Therefore, studying the aforementioned phenomenon involves looking at technologies but should not stop there.

This study focuses on the human rights aspects related to the availability and use of a technology of particular significance for the field of information and communication: encryption, or more broadly cryptography.[3]

Cryptography is a long-standing subject in the field of mathematics, computer science and engineering. It can generally be defined as "the protection of information and computation using mathematical techniques."[4] In the OECD Guidelines, Encryption and Cryptography are defined as follows:

> "Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.
>
> "Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.[5]

Since the 1970s, the availability of digital computing and the invention of so-called public-key cryptography has made encryption more widely available in our societies. Before that, strong versions of encryption, i.e. encryption that is very hard to break, were the domain of nation state actors. However, over the last decades, encryption and the continuing innovations in the field have proven uniquely suitable to be used in the digital environments.

---

1 Philipp Rogaway. The Moral Character of Cryptographic Work. University of California. December 2015. http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf.

2 See e.g. Lessig, Reidenberg; Asscher et al.; Balkin; DeNardis.

3 Ed Felten. Software backdoors and the White House NSA panel report. December 2013: "The two terms are often used synonymously, although "cryptographic" has a broader technical meaning. For example, a digital signature is "cryptographic" but arguably it is not technically "encryption"". https://freedom-to-tinker.com/blog/felten/software-backdoors-and-the-white-house-nsa-panel-report/.

4 Gürses and Preneel 2016.

5 OECD Guidelines.

Cryptographic techniques have been widely deployed by a variety of actors to ensure personal, commercial and public sector protection of information and communication. Cryptographic techniques are also used to protect anonymity of communicating actors and thereby privacy more generally.

The availability and use of encryption continues to lead to complex, important and highly contentious legal policy debates. A first round of debate accompanied by legal and other forms of contestation at the national and international level took place in the 1990s. The world is currently in the midst of a second round of debate about encryption at the international and national level, which signals that the existing policy framework with respect to encryption is in need of an update. The current and second round of debate was ignited by revelations concerning government access to information and communication that resulted from the leaks of Edward Snowden to the media. Since then, there has been a remarkable increase in the availability of end-to-end encryption tools that are being developed and that are available to users.[6] Strong encryption is generally accepted as a necessary and positive part of the media and communications landscape. As the preface of the OECD Guidelines for Cryptography Policy notes, it is "critical to the development and use of national and global information and communications networks and technologies, as well as the development of electronic commerce".[7] Encryption plays a key role in policy frameworks promoting network security and integrity. Still, there are government statements and proposals on the need to curtail such usage and deployment in view of the potential hurdles it could present for access by government agencies. For the purposes of this report, the focus is mainly upon lawful access by state actors, rather than unauthorized access more generally, for instance by malicious hackers. The fact that restrictions on encryption in view of government access can have serious negative repercussions for the ability to prevent unauthorized access more generally, is of course relevant.

At the same time, it is acknowledged that encryption is particularly relevant to cases of illegitimate access outside of legal process, whether by state or non-state actors and who may be domestic or foreign.

Against this background, it can be noted that industry stakeholders have also increased their deployment of cryptographic techniques significantly in the last years to increase the protection of the information and communications of their users and to promote trust in their services. This development should be kept in perspective. Different studies on encryption have noted that ubiquitous adoption of end-to-end encryption by relevant industry actors is unlikely considering the reliance on user data in business models.[8] Nevertheless, the rise of commercial services offering end-to-end encryption and the calls for restrictions and solutions in view of law enforcement access are re-fueling the current round of debates around the use of encryption and the legal status of the deployment of cryptography more generally.

From a human rights perspective, there is a growing awareness that encryption is an important piece of the puzzle for realizing a free, open and trustworthy Internet. This is also true for UNESCO. In the UNESCO publication "Keystones to foster inclusive Knowledge Societies",[9] encryption is discussed and identified as an area for future action. The Keystones

6 End-to-end encryption refers to the application of encryption to communication tools and services, such that only the users of the tool or service have access to the plain-text messages. For in-depth discussion, see Section 2.

7 See OECD Guidelines.

8 See e.g. Soghoian 2009, Van Hoboken and Rubinstein 2014, Berkman Center 2016.

9 See http://www.unesco.org/new/en/internetstudy.

study was concerned with contributing to the establishment of a vision for "a free, open and trusted Internet that enables people to not only have the ability to access information resources from around the world, but to also contribute information and knowledge to local and global communities".[10] To move towards the realization of this vision, there is recognition of "the role that anonymity and encryption can play as enablers of privacy protection and freedom of expression", as well as the value of UNESCO's work "to facilitate dialogue on these issues".[11] This publication follows UNESCO's new approach to Internet issues, as endorsed in November 2015 on the occasion of its 38th General Conference. Our 195 Member States have adopted the CONNECTing the Dots Outcome Document, in which 38 options for future action from UNESCO are set out; and the Internet Universality principles (R.O.A.M.)[12], which advocates for a Human-rights-based, Open and Accessible Internet, governed by Multi-stakeholder participation.

The current and the previous UN Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression also confirm encryption as an enabler of human rights in the field of information and communication. In his 2013 Report on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, the rapporteur at that time, Frank La Rue concluded that

> States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.[13]

His successor, UN Rapporteur David Kaye, recently specifically dedicated a report to assess the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age, and he presented this to the Human Rights Council in June, 2015. [14] Kaye observed that encryption and anonymity deserve a protected status under the rights to privacy and freedom of expression:

> Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.[15]

The report also addressed the question about the connections to human rights, the legality of possible interferences and offered recommendations for state practice and other relevant stakeholders.[16]

---

10 UNESCO. Keystones to foster inclusive Knowledge Societies. Paris 2015. http://unesdoc.unesco.org/images/0023/002325/232563E.pdf.

11 Ibid. p. 66.

12 Both the UNESCO Connecting the Dots Outcome Document and the concept paper of Internet Universality are attached as Appendix to this publication.

13 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

14 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

15 David Kaye. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. May 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

16 For further discussion, see Section 3.

Research question, scope and goals of the study

From the above it is clear that there is a valuable contribution that can be made by studies that can serve as a neutral basis for an informed international discussion about encryption as a means to support human rights in the media and communications landscape. In particular, there is great value in connecting ongoing debates at the national and international level and to consider the role of industry stakeholders. To further this goal, this study will address the following key questions:

- What is the current state of deployment of encryption technologies and solutions in the media and communications landscape, by relevant industry stakeholders and by communities of end-users more generally? (Section 2)
- How is the deployment of encryption technologies and solutions affected by different areas of information law and policy? (Section 3)
- What is the current state of encryption policy in selected jurisdictions among five continents, including the African region, as seen through a general typology of restrictions on encryption and positive measures? (Section 4)
- How does the deployment of encryption technologies and solutions relate to the protection of human rights in the media and communications landscape? (Section 5)
- Which policy options and stakeholder actions can best ensure the respect for human rights in the context of encryption? (Section 6)

Before addressing these questions in more detail, it is worth spending a moment on definitions and the general scope of this study. Ultimately, this study is concerned with furthering the discussion on the supporting role of encryption for the protection of human rights, in particular the right to privacy and the right to freedom of expression as protected at the international level. As has been noted in recent reports, measures ensuring anonymity can be observed to play a similar role as encryption in supporting these rights. But to avoid confusion, this study consistently distinguishes between the normative values at stake (e.g. protection of one's private information or communication, protection of access to information) and the possible technological means to protect these values (encryption, authentication, obfuscation). In addition, this study consistently clarifies the precise cryptographic techniques that are at issue, considering the variety of available options.

Encryption, as defined above, refers to a subset of cryptographic techniques for the protection of information and computation. The normative value of encryption, however, is not fixed but varies with the type of cryptographic method that is used or deployed and for which purposes. Traditionally, encryption (cypher) techniques were used to ensure the confidentiality of communications and prevent access to information and communications by others than intended recipients. This is the use of encryption that is most common in the debates about encryption today and the primary focus of this study. This is, however, only a subset of cryptographic techniques. Cryptography can also ensure the authenticity of communicating parties and the integrity of communications contents, providing a key ingredient for enabling trust in the digital environment. Another subset of techniques is concerned with the protection of *meta-data,* including providing protection of the anonymity of users of the Internet and Internet-based specific services.

Accordingly, this study will address the issues on the interface of human rights and encryption with the following observation in mind. What ultimately matters is not

'encryption' per se, or any particular cryptographic method. What matters from a human rights perspective are the establishment and possible interference with human-facing communications (and information) properties, like confidentiality, privacy, authenticity, availability, integrity, anonymity. Cryptographic methods are important, thus interferences with their use and deployment should be carefully scrutinized, because these methods allow the technical guarantee of these important properties, even over untrustworthy communications platforms such as the Internet. For instance, while an internet access provider may not encrypt traffic between end-users, communication applications can still implement encryption protocols that can guarantee the property of 'confidentiality' of their communications.

Encryption can be used to enhance user control over personal information and correspondence and this type of use is the focus of this study. This study will put particular emphasis on the role of encryption as used and deployed by different kinds of services and organizations in protecting user data security and supporting human rights, next to recognizing the availability of end-user tools and applications and the importance of community-driven projects. It should be noted here that encryption can also be used to harm people, keep people from accessing information they should have access to or keep people from using tools that should be available to them. An example is the use of device encryption attacks (ransomware) that encrypt the device of a user with a key that is kept by the attacker and only revealed in exchange for a ransom. Another example is the unduly restrictive use of Digital Rights Management (DRM) in ways that disproportionately affect access to information and communication.

There are communities that warrant particular attention when discussing the human rights implications of encryption, such as political activists and journalists, and the related institutions and organizations they are part of. When considering the question of who are the human rights beneficiaries of encryption, it may be noted that much of the debate about encryption has, until now, been gender-blind, or perhaps worse, male-dominated. It is well recognized that women and girls may be especially subjected to violations of their rights to expression, privacy, dignity and safety in the online arena.[17] It is worth noting that the encryption can facilitate the protection of women and girls and vulnerable communities, which is clearly an important area of further work and investigation to provide an in-depth account on this. Generally, the wider societal debate about human rights and encryption should also seek to be informed by the experiences of those subjected to targeted surveillance and associated human rights abuses, including racial, ethnic and religious minorities, journalists, bloggers, women and girls, LGBT communities, etc.[18]

Those that have followed the ongoing debate about encryption (and the asserted need to restrict it) cannot help but notice a recurring tendency for false debate. It is important that the benefits of encryption need to be placed in context. The benefits of encryption, by itself, can otherwise be misperceived or may not provide the expected protections in context. Encrypting communications between two communicating parties, for instance, does not prevent any of the parties that has access from handing the information over to a third party. Unfortunately, encryption may also inadvertently attract attention or raise suspicion

17 See e.g. UNESCO, 'UNESCO calls to combat online and offline violence against women and girls', September 25, 2015. Available at http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/all-news/news/launch_of_the_broadband_commissions_report (last accessed: 14 September 2016).

18 See e.g. Gürses, S., Kundnani, A. and Van Hoboken, J., 2016. Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture & Society*, 38(4), pp. 576-590.

in ways that are detrimental to the effective enjoyment of human rights, especially in situations in which general rule of law safeguards are lacking. Thus, the mere possibility to use encryption is not, by itself, a sufficient safeguard to communicate freely.

Conversely, assumptions related to the benefits to government actors of the power to decrypt communications also deserve close scrutiny. First, there are serious questions about the technical challenge of implementing such powers. Even then, communications about planned illegal acts may simply hide in plain sight through using apparently everyday innocuous speech. Second, the role of encryption in obstructing access to information or communication may be significantly overstated by interested actors. Perhaps it is in the mathematical nature of encryption that gives some of its guarantees a seemingly absolute nature. When needed, however, state actors and criminals have a range of capabilities they can deploy to side-step or circumvent encryption techniques (by exploiting implementation deficiencies or side-channels) and the resources and computing power of certain state actors is such that many advanced encryption technologies may ultimately fail to ensure protection against them. In addition, even when using more secure information and communication tools, users may remain vulnerable in several ways. An illustration of this is found in how attackers were using Whatsapp to direct users to a non-secure application, during Hong Kong protests in the past year.[19] The information disclosed through the recent disclosure of Hacking Team documents illustrate that a market has emerged for using such measures against civil society, journalists and activists.[20] These developments suggest that encryption is necessary but not sufficient to protect people and sensitive information in a networked world. They also illustrate the accelerated pace of developments surrounding cryptographic methods and technologies, which should caution against blanket statements or policies concerning these issues.

2. Encryption in the media and communications landscape

What follows is a concise overview of state-of-the-art of relevant cryptographic methods as applied in the media and communications landscape. The text refers to specific cryptographic methods and applications to make it possible to draw a number of important distinctions, while trying to make sure it remains accessible to a non-technical audience. Particular emphasis is placed on developments with respect to the actual deployment and use of cryptographic methods by service providers as well as their practical availability to individuals and relevant professionals.

In these discussions, the following two underlying distinctions are central.[21] First, a distinction on the basis of who is *responsible* for the deployment of encryption: is encryption used as a result of the choice of a service provider, or is it deployed by (communities of) internet users? In discussing the deployment of user or client-side encryption tools and technologies, it is important to keep in mind those communities of users that have special security needs that are relevant from a human rights perspective, such as human rights

19 Jim Finkle. Advanced iOS virus targeting Hong Kong protestors -security firm, Reuters, September 2014. Available at http://www.reuters.com/article/hongkong-china-cybersecurity-apple-idUSL2N0RV2D320140930 (last accessed: 14 September 2016).

20 Alex Hern. Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. *The Guardian*. 6th July 2015. http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (Accessed: 14th December, 2015).

21 Following Ira Rubinstein and Joris van Hoboken. Privacy and Security in the Cloud. Maine Law Review 2014, pp. 488 et seq. and Claudia Diaz, Omer Tene and Seda Gürses. Hero or Villain: The Data Controller in Privacy Law and Technologies, 74 (2013) Ohio State Law Journal, pp. 923 et seq.

defenders, marginalized communities, journalists and other online media actors practicing journalism.

A second distinction is a distinction between end-to-end encryption and other methods of encryption. Considering the central issue of the possibility to legally compel service providers to provide access to user information, this is an important distinction when looking at the human rights implications of encryption in particular. Many forms of encryption are deployed by service providers to secure communications in a way that prevents unauthorized *third party* access, but the service provider implementing it still has access to the relevant user data. With end-to-end encryption, we refer to encryption that also prevents service providers *themselves* from having access to the user's communications. The implementation of these forms of encryption have recently sparked the most debate.

Service provider deployed techniques to prevent unauthorized third-party access

Amongst the most widely deployed cryptographic techniques is the technique to secure the communications channel between internet users and specific service providers from unauthorized third party access. These cryptographic techniques must be run jointly by a user and the service provider to work. This means that they require service providers, such as an online news publisher or a social network, to actively integrate them into service design and implementation. Users cannot deploy these techniques unilaterally; their deployment is contingent on active participation by the service provider.

For example, a web-service provider, such as an electronic bank or an online library, may decide to secure the communication with the users. Service providers can do so by relying on the so-called Transport Layer Security (TLS) standard. TLS allows the service provider to keep the communication between the client and the server *confidential* from all third parties. Notably, it also allows both sides to *authenticate* the communicating parties -- typically only the server-- and check the communication content for alterations.[22] When TLS is turned on, users are able to trust that they are providing their banking login credentials to their actual bank. Readers visiting a news site are able to trust that they are not reading altered news articles.

The TLS protocol, which becomes visible to the normal internet user through the HTTPS header, is widely used for securing online commerce, e-government services and health applications as well as devices that make up networked infrastructures, e.g., routers, cameras. However, although the standard has been around for almost 20 years, the wider spread and evolution of the technology has been slow, picking up most significantly in recent years.

As with other cryptographic methods and protocols, the practical challenges related to proper, secure and (wider) deployment are significant and have to be considered. Many service providers still do not implement TLS or do not implement it well. Many servers may not offer the secure version of the protocol, i.e., with TLS, by default or at all. Furthermore, servers may choose to use the same encryption key for a long period, instead of switching keys every session and discarding used keys. The latter version, called perfect forward secrecy, is generally considered best practice. It has the advantage that disclosure of a

22 See also Eitan Konigsburg. Embracing HTTPS. November 2014. http://open.blogs.nytimes.com/2014/11/13/embracing-https/ (last accessed: 14 September 2016).

key only reveals the content of communications for the corresponding session. Still, many implementations rely on long-term keys.

Encryption that protects communication between users and Internet services provides great improvements to user privacy and security vis-a-vis malicious third parties. The recent revelations about mass surveillance programs have resurfaced the reality that when relevant companies do not secure communications between users and their servers, government agencies around the world are able to scoop up communication data in bulk.[23] This situation has been subject to substantial change since then. Many companies have now deployed TLS-like solutions to improve the security of their services in view of potential unauthorized access to data.[24] In some public cases, this has also included securing data in transit between data centers of service providers and between different service providers. Civil society actors have started publicly monitoring TLS deployment of prominent services, e.g., see EFF "Encrypt the Web Report".[25] Google has monitors the deployment of HTTPS on the top 100 destinations on the web in a special section of its Transparency Report.[26]

The increased roll-out of TLS has been especially valuable for professionals like journalists[27], civil society and other institutions that place value in confidential communications with users and sources[28], and providing their content to readers without subjecting them to unnecessary risks of eavesdropping and content manipulation. The list of prominent service providers that switched to HTTPS implicates more than a billion users as it includes twitter, Facebook, Google search, Gmail, Tumblr and eventually also Yahoo!.

There are notable improvements in the deployment of encryption to protect user communication towards third parties. Still, research and investigations demonstrate that deploying and maintaining security measures is not an art that each online service is willing or able to master. Furthermore, the increased focus on TLS has surfaced large-scale vulnerabilities in the related protocols, e.g. the 'Heartbleed' and the 'FREAK attack'.[29] The emergence of these vulnerabilities has underlined that concerted and continuous efforts across the globe within the relevant technical expert communities are necessary to ensure and maintain the security of communications through encryption. Initiatives like Let's Encrypt respond to some of these challenges, including the ease of implementation.[30]

In the context of wireless communications, the use of cryptographic techniques that protect communications from third parties are also important. Different standards have been developed to protect wireless communications: 2G, 3G and 4G standards for communication between mobile phones, base stations and base stations controllers; standards to protect communications between mobile devices and wireless routers ('WLAN'); and standards for

23 Internet Architecture Board (IAB). Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement. August 2015. http://tools.ietf.org/html/rfc7624. For backgrounds and a discussion, see Arnbak 2016.

24 See also Van Hoboken and Rubinstein. op. cit.

25 Electronic Frontier Foundation. EFF's Encrypt the Web Report. November 2014. https://www.eff.org/encrypt-the-web-report (last accessed: 29 August 2016).

26 Google, Transparency Report, HTTPS on Top Sites, https://www.google.com/transparencyreport/https/grid/?hl=en.

27 Kevin Gallagher. Why aren't more news organizations protecting their e-mail with STARTTLS encryption?. 24th February 2015. https://freedom.press/blog/2015/02/why-arent-more-news-organizations-protecting-e-mail-with-starttls (last accessed: 29 August 2016.

28 For sources, a journalist typically wants protection of anonymity, in addition to protection of the confidentiality of the content of communications. This requires additional measures related to meta-data.

29 See https://freakattack.com (last accessed: 29 August 2016).

30 See https://letsencrypt.org (last accessed: 29 August 2016).

local computer networks. Earlier versions of wireless security standards had weaknesses, while in recent versions substantial improvements have been made.[31]

One common weakness in these designs is that the transmission points of the wireless communication can access all communications, e.g., the telecommunications provider.[32] This vulnerability is exacerbated when wireless protocols only authenticate user devices, but not the wireless access point. For example, early mobile communication standards (GSM) are such that only mobile phones are authenticated, but not the base stations that mobile phones connect to. Malicious actors or government agencies can take advantage of this weakness to intercept communications and track mobile users at a given location, by means of setting up a new, fake, base stations. These fake base stations are commonly referred to as 'IMSI catchers'.[33, 34, 35]

Because of the pervasive use of wireless in local environments such as the home, the question of wireless security is increasing in urgency with the rise of the "Internet of Things". The Internet of Things refers to the development that not only computers, but more and more objects (and the sensors installed in them, including microphones and cameras) become connected to the Internet. When people find themselves surrounded by everyday objects that capture environmental information and communicate with networks, the presence or absence of security and privacy measures in wireless systems becomes even more essential.[36] As the recent Berkman Center study on encryption mentions, the Internet of Things may open new channels to monitor. This also implies that "an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel".[37]

The techniques discussed above can protect the users' information in transit or at rest from third parties. The techniques may be differently applied at both points, or only at one point. There is also a distinction between 'at rest' in regard to whether the data is stored on a device, or on a local server as in the cloud. Given the vulnerability of cellphones to theft for instance, particular attention may be given to limiting even service provided access (see below). In general, this does not exclude the situation that the service provider discloses this information to third parties like other commercial entities or governments. In other words, the user needs to trust the service provider to act in its interests. The possibility that a service provider is legally compelled to hand over user information or to interfere with particular communications with particular users, remains. In the following section, we discuss methods that ensure that the service provider itself does not have access to the inputs from the user. There are services that specifically market themselves with claims not to have access to the content of their users' communication.

---

31 GSMMap provides an overview by country and telecommunication provider on the implementation of these measures. See http://gsmmap.org (last accessed: 29 August 2016).

32 Gürses and Preneel, 2016.

33 ACLU. Stingray Tracking Devices: Who's Got Them?. https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last accessed: 29 August 2016).

34 Eric King and Matthew Rice. Behind the curve: When will the UK stop pretending IMSI catchers don't exist?, 5th November, 2014. https://www.privacyinternational.org/node/454 (last accessed: 29 August 2016).

35 Dan Goodin. Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations, arsTechnica. 28th October 2015. http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/ (last accessed: 29 August 2016).

36 Yulong Zou, Xianbin Wang and Lajos Hanzo. A survey on wireless security: technical challenges, recent advances and future trends. Proceedings of the IEEE. May 2015. http://arxiv.org/pdf/1505.07919.pdf.

37 Berkman Center 2016.

Service provider deployed techniques that limit service provider access

Service Providers can also take measures that restrict their ability to access information and communication, thereby further increasing the protection of users against access to their information and communications. The integrity of such measures, also called Privacy Enhancing Technologies (PETs), depends on delicate design decisions as well as the willingness of the service provider to be transparent and accountable. Privacy Enhancing Technologies are designed to provide functionality while minimizing the user data that becomes accessible to the service provider. The most popular examples can now be found in the market of private messaging.

It is worth noting at the outset that for many of these services, the service provider may offer some additional features (besides the ability to communicate), for example contact list management -- meaning that they can observe who is communicating with whom-- but take technical measures so that they cannot read the contents of the messages. This has potentially negative implications for users. For instance, since the service provider has to take action to connect users who want to communicate using the service, it will also have the power to prevent users from communicating in the first place.

The current landscape of private messaging services is a fast moving landscape in terms of encryption that is deployed, in which very subtle differences in design can have a significant impact on the privacy guarantees of a given application. Facebook's Whatsapp and Apple's iMessage[38] are examples of a large-scale deployment of private messaging. However, for both services, the security used to be designed in ways such that Facebook and Apple could theoretically still have a way to assist in intercepting unencrypted communications by exploiting the additional features that they offer.[39, 40] In a very strict sense, this disqualified both these applications from being categorized as end-to-end private secure communications providers. Recently, Whatsapp has finalized its deployment of end-to-end encryption, which is now the default of its (more than a billion) users.[41] WhatsApp relies on the Signal Protocol designed by Open Whisper Systems for its technical implementation of end-to-end encryption.[42]

Considering that subtle technical differences can have significant implications for the protection of users, it is common practice in the security and privacy engineering community to demand transparency and technical audits for services that claim to provide security or privacy guarantees. Some services have been exemplary in this regard. For instance, the open source project and company Open Whisper System offers Signal end-to-end encryption, and this can be validated since their code is open to public scrutiny and has also been subject to code review.[43] Following the discovery of vulnerabilities, there is a growing awareness that there needs to be more investment in the auditing of widely used code coming out of the free and open software community.

38 Apple, Our Approach to Privacy, http://www.apple.com/privacy/approach-to-privacy/.

39 Joseph Cox. Apple's iMessage Defense Against Spying Has One Flaw. Wired. 8th September 2015. http://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/ (last accessed: 29 August 2016).

40 Fabian Scherschel. Keeping Tabs on WhatsApp's Encryption. c't. 30th April 2015. http://m.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html (last accessed: 29 August 2016, 2015).

41 See Cade Metz, Forget Apple vs. the FBI: Whatsapp just switched on encryption for a billion users. April 5, 2016. Available at http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

42 WhatsApp, WhatsApp Encryption Overview, Technical White Paper, April 4th, 2016.

43 EFF. Secure Messaging Scorecard. Version on 3rd November 2015. https://www.eff.org/secure-messaging-scorecard (last accessed: 29 August 2016).

In addition to securing communications, service providers may also play a role in protecting data at rest in ways that do not allow them to access the unencrypted data. By now, many users have to manage a number of devices, laptops, mobile phones, disk drives, which can be lost, stolen or sold. If no further measures are taken, anyone with access to the device may be able to extract information stored on these devices. Such leakages may have significant consequences for the owner of the device, and to all other parties whose information was stored on the device.

In order to protect information on devices, authenticated encryption can be applied. The adoption of device encryption used to be limited and few users are competent enough or aware of the possibility, to turn on encryption. More recently, relevant companies, including Google and Apple have started to increase device encryption capabilities.[44] Also in this instance design decisions about where to place the key are relevant: storing keys on the device is unlikely to be effective towards an adversary that has or can obtain access to the device.[45] The case of Apple's device encryption is worth noting in particular, as it has caused a major public debate, including internationally, on the repercussions for law enforcement access. The widely discussed case between Apple and the FBI about the possibility to compel Apple to produce a workaround to unlock the device illustrated many of the complexities as well as the lack of common understanding between opposing sites in the encryption debates.[46] While the new measures can cause issues for government agencies in some cases, the fact that user data tends to be synced with the cloud alleviates such concerns.[47]

Industry players recognize that managing and loss of devices is a problem for users, and rather than emphasizing confidentiality, the continuation of their services through seamless availability of user data tends to be a primary concern. As a consequence, service providers now typically address issues around the management and loss of devices by replicating user data into the cloud. While storing data in the cloud helps to guarantee availability over time and across devices, it also increases the risk of exposing this information to third party access through compulsion or through hacking, and makes it available for use and profiling by service providers. Also when data is stored in the cloud, authenticated encryption only offers full and effective protection to the user under the condition that the decryption key is stored locally under control of the data owner rather than in the cloud.

The pervasiveness of business models that depend on collection and processing of user data can be an obstacle for adopting cryptographic mechanisms for protecting information at rest. In fact, as Bruce Schneier, has stated:

---

44 Samuel Gibbs. Google can unlock some Android devices remotely, district attorney says. The Guardian. 24th November 2015, http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted (last accessed: 29 August 2016).

45 Andy Greenberg. Cops Don't Need a Crypto Backdoor to Get Into Your iPhone. 12th October, 2015. http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/ (last accessed: 29 August 2016).

46 For further discussion, see Section 3 and 4.

47 Micah Lee. Apple still has plenty of your data for the feds. The Intercept. 22nd September 2014. https://theintercept.com/2014/09/22/apple-data/ (last accessed: 29 August 2016). Notably, when data is stored in the cloud, this can present its own unique issues for law enforcement to obtain access. See e.g. the Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: challenges, Discussion paper, Strasbourg, France, 26 May 2015.

> "[s]urveillance is the business model of the Internet. This has evolved into a shockingly extensive, robust, and profitable surveillance architecture. You are being tracked pretty much everywhere you go on the Internet, by many companies and data brokers: ten different companies on one site, a dozen on another."[48]

As a result, end-to-end encryption is unlikely to be pervasively deployed by commercial service providers that depend on profiling users through cloud applications. Recent advances in cryptographic techniques do, however, make it feasible to provide some services "in the encrypted domain". For example, using advanced cryptographic techniques it is possible to search encrypted data: if the search terms are known in advance, one can encrypt data in such a way that the encryption is secure but one can still search the cipher text for the search terms, a service also known as Private Information Retrieval. Further advances show that it may also be possible to perform other operations on encrypted data. Such advances in so-called homomorphic encryption mean that the service provider can run computations on encrypted data, but only the user can decrypt the results.[49]

Finally, cryptographic methods play a key role in online identity management. Digital credential systems can be used to allow anonymous yet authenticated and accountable transactions between users and service providers, and can be used to build privacy-preserving identity management systems.[50]

End-user and community-driven encryption and collaborative services

A powerful characteristic of the Internet is that it allows end-users to develop applications and uses of the network without having to coordinate with the relevant internet service providers. Related to this characteristic, many of the available encryption tools are not developed or offered by traditional service providers or organizations but by experts in the free and open software and the Internet engineering communities. A major focus of these initiatives is to produce Privacy Enhancing Technologies (PETs) that can be unilaterally or collaboratively deployed by interested -- and presumably technically competent-- users who are ready, willing, and able to look after their own privacy interests when interacting with service providers.

These PETs include standalone encryption applications as well as browser add-ons that help maintain the confidentiality of web-based communications or permit anonymous access to online services. PGP, i.e. Pretty Good Privacy, encryption for email is one of the best known and earliest examples of such a technology. Users can make use of PGP by installing additional software on their computers, in addition to their email reader. Technologies in this category are architected to provide end-to-end encryption as well as other protections without relying on a centralized service provider. In particular, the client-side solutions, like the GnuPG software, which relies on PGP, are designed to allow sender and receiver to make use of an untrusted and potentially adversarial intermediary such as their broadband provider, a social network, or a web-based email service without relying on them to enable encrypted services. There are also examples for communications other than email. Scramble! and Cryptogram are examples of plugins for social networks that offer users end-to-end

48 Bruce Schneier. How We Sold Our Souls - and More - to the Internet Giants. May 2015. https://www.schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html.

49 Also from Gürses and Preneel. op cit.

50 Claudia Diaz, Omer Tene and Seda Gürses, Hero or Villain: The Data Controller in Privacy Law and Technologies, 74 Ohio State Law Journal pp. 923, 2013.

encryption of their communications.[51] On the other hand, technologies such as keystroke loggers can intercept content as it is entered before encryption is applied, thereby falling short of offering protection. Hacking into information systems and devices to access data at or after the moment of decryption may have the same effect.

Another category of tools for users are tools for instant messaging that can be installed by the user. These tools integrate so-called Off-the-Record (OTR) encryption protocols,[52] and provide confidentiality of the communications, as well as *perfect forward secrecy*, and *deniability*. Perfect forward secrecy minimizes the amount of communications that is compromised when an encryption key is compromised. It does so by ensuring that the confidentiality of the communication throughout time is not dependent on the secrecy of a single key but multiple session keys that are discarded after use. Deniability refers to the guarantee that once a communication has ended, no one—not even the users involved in the chat conversation—can use further technical means to technically prove whether a specific user actually sent a particular message. These different properties are designed to enable online chat services that resemble verbal conversations. By concealing the content, they also help diminish the ability of service providers, connectivity providers or governments to censor users' communications and curtail free speech based on the content of communications. For example, by using OTR on Facebook chat, citizen journalists may be able to communicate content without being subject to the enforcement of restrictive country-specific terms of service and related content removal practices.

Certain PETs require collaboration among different parties to enable the service. For instance, anonymous communication systems like The Onion Router (Tor)[53] are built upon the key idea that the users of the system join in order to provide cover for each other and thereby offers anonymity.[54] Governments or other malicious actors who are recording and analyzing traffic data in such systems cannot determine which of the users in the anonymity set is associated with a specific action and are not able to recover communication patterns between users (i.e., the communication graph).[55] The following subsection discusses such protection of metadata in more depth.

The different PETs discussed above do not require any implementation by service providers, although service providers have been known to encourage or discourage their use by making services interoperable or blocking the use of such technologies. For instance, service providers can increase interoperability with users of anonymous browsing software by offering access through a special .onion address.[56] This increases the security for users.

Multi-party computation (MPC) techniques are yet another example of collaborative solutions that allow parties, for example multiple NGOs with sensitive data, to do data analytics without revealing their datasets to each other. All of these designs have in common that they leverage encryption to provide privacy and security assurances in the absence of a trustworthy centralized authority.

---

51 http://cryptogram.prglab.org (last accessed: 29 August 2016).

52 https://otr.cypherpunks.ca (last accessed: 29 August 2016).

53 https://www.torproject.org (last accessed: 29 August 2016).

54 For a discussion of the technical terminology relating to anonymity, see Pfitzmann and Hansen, 2005.

55 In Diaz, Tene and Gürses. op cit.

56 Tom Fox-Brewster. Facebook opens up to anonymous Tor users with .onion address. The Guardian. 31st October 2014. http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion (last accessed: 29 August 2016).

Finally, it is worth mentioning the application of encryption to financial transactions. There are many recent developments in the implementations of crypto-currencies using so-called blockchain protocols. These systems can have many benefits and these protocols can also be useful for novel forms of contracts and electronic attestation, useful aids when legal infrastructure are not readily available. As to the protection of privacy related to payments, it is a common misconception that the cryptographic techniques that are used in Bitcoin ensure anonymous payments. Technically, however, the only protection offered by Bitcoin is pseudonimity.[57]

The cryptographic protection of metadata

The availability of metadata, i.e. the information relating to a user's information and communications behavior, can pose a particular threat to users. By metadata in this context we refer to information that service providers can observe through the provisioning of services: when, how frequently, how long, and with whom users are communicating. It is possible to infer communication graphs as well as in depth behavioral patterns from such data.[58] Metadata can also be used to track people geographically and can interfere with their ability to communicate anonymously. As noted by the Berkman Center report, metadata is generally not encrypted in ways that make it inaccessible for governments, and accordingly "provides an enormous amount of surveillance data that was unavailable before [internet communication technologies] became widespread."[59]

The tools and solutions we discussed in the previous sections by themselves do not provide protection of metadata from traffic analysis by service providers. Thus, by using an end-to-end encrypted messaging service, a user does protect the content of her communications but makes his or her communications metadata (when communications took place and between whom) available to service providers. Regardless of whether communications are encrypted and authenticated, a variety of connectivity and service providers may be in a position to observe such encrypted communications. In order to minimize exposure of meaningful metadata, encryption tools may need to be used in combination with technologies that provide communication anonymity.

The Onion Router, most commonly known as Tor, offers the ability to access websites and online services anonymously. Tor requires a community of volunteers to run intermediary proxies which channel a user's communication with a website so that third parties cannot observe who the user is communicating with. Through the use of encryption, each proxy is only aware of part of the communication path meaning that none of the proxies can by itself infer both the user and the website she is visiting. From the perspective of the service provider, Tor can be seen as a client-side tool, since individuals can use it unilaterally without requiring modifications to the service. As mentioned, service providers can increase interoperability with Tor by opening access to their website through a special .onion address.

When a user accesses a website through Tor, it is not possible for the service provider to determine the user's identity, which is masked behind a series of proxies. Furthermore, it is not possible for websites to link different sessions to a single user, effectively disabling any

57 See Bitcoin is NOT anonymous, http://www.bitcoinisnotanonymous.com/ (last accessed: 14 September 2016).

58 See e.g. Tokmetzis, D. 'How your innocent smartphone passes on almost your entire life to the secret service', 2014. English translation published at https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/ (Accessed 15 May 2016).

59 Berkman Center 2016.

tracking capability. Of course, Tor does not protect the anonymity in relation to the service provider once the user identities him or herself directly to a service.

Besides protecting anonymity, Tor is also useful when the user's ISP blocks access to content. Users can make use of Tor to reach the blocked websites: the user's ISP can observe that the user is connecting to one of the Tor proxies, but they cannot see or block the website that the user is actually communicating with. This is similar as the protection that can be offered by a VPN. On the other hand, service providers, such as websites, can block connections that come from the Tor network. Because certain malicious traffic may reach service providers as Tor traffic and because Tor traffic may also interfere with the business models, service providers may have an incentive to do so. This interference can prevent users from using the most effective means to protect their anonymity online.

The Tor browser allows users to obfuscate the origin and end-points of their communications when they communicate on the internet. Here, *obfuscation* refers to the automated generation of "fake" signals that are indistinguishable from users' actual online activities, providing users with a noisy "cover" under which their real information and communication behavior remains unobservable. Obfuscation has received more attention as a method to protect users online recently.[60] TrackMeNot is an obfuscation tool for search engine users: the plugin sends fake search queries to the search engine, affecting the ability of the search engine provider to build an accurate profile of the user. Although TrackMeNot and other search obfuscation tools have been found to be vulnerable to certain attacks that allow search engines to distinguish between user-generated and computer-generated queries, further advances in obfuscation are likely to play a positive role in protecting users when disclosure of information is inevitable, as in the case of search or location-based services. Given the pervasive availability of metadata and the possibility to use metadata to make inferences about people and user behavior, there are likely to be further research and developments in increased coupling of encryption and obfuscation methods to protect users in digitally mediated environments.

3. Cryptography, law and human rights: background

This section provides a concise overview of the way in which current international law and policy relates to encryption technologies, their availability and their deployment in services or by users. The section will start with a reference to the prominent discussion of the framing of encryption as a hurdle to lawful government access to information and communication. This argument, that encryption prevents relevant government agencies from gaining lawful access to information or communication relevant to an ongoing investigation is summarized as the 'going dark' of the communication and information behavior of malicious actors.

What follows then is a brief clarification of the position of encryption regulation in general e-commerce, data protection and security policy as well as of the fact that encryption is a subject in standard setting bodies and frameworks. This helps to provide the bigger picture that clarifies the many ways in which regulation is, and in fact, should be, by and large centrally concerned with the promotion, adoption and deployment of encryption, in ways that stimulate its use to protect security and privacy, allow for global commerce, secure government operations and establish trust in the digital environment more generally.

60 See Brunton, Finn, and Helen Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press, 2015.

The section concludes with a short discussion of international norms with respect to encryption and the recent attention to the supporting role of encryption for protecting human rights to privacy and freedom of expression.

'Going dark' or a 'Golden age of surveillance'

It is the debate about encryption and its impact on lawful government access to information and communication that most succinctly raises the question about whether there is a need for restrictions on the general availability of strong encryption. This is because of the possible hurdle it could present in the investigation of crime and the protection of national security. The idea that effective access could be blocked by encryption, even when all procedural and substantive safeguards have been fulfilled for gaining access to information and communications, for instance through a Court-approved warrant establishing probable cause in the evidence for a specific investigation, has consistently raised concerns about the implications for public safety and national security. This was the case in the first round of debate about the public availability of strong cryptographic methods in the 1990s and it is the case now. It has led Government officials of the highest level to make statements about what they see as an unacceptable state of affairs. And it has led to a stream of proposals to restrict strong encryption on the grounds that would present hurdles to access and lead to a going dark of malicious activity, or to establish some form of exceptional access for relevant government authorities.[61] Recent incidents of terrorism have led to further calls for restrictions on encryption, [62] while certain countries, such as Germany or the Netherlands have taken a strong position against restrictions on encryption on the Internet.[63] In a joint statement, the European Agency for Network and Information Security (ENISA) and Europol have also taken a stance against the introduction of backdoors in encryption products.[64] Recently, the Ministers of the Interior of France and Germany have jointly stated the need to work on solutions for the challenges law enforcement can face as a result of end-to-end encryption, in particular, when offered from a foreign jurisdiction.[65]

This is not the place to address this debate in full, but for the purposes of this study it is important to clarify that there is overwhelming agreement in the technical community about the fundamental downsides that would accompany exceptional access for relevant government agencies in terms of the security that properly implemented cryptographic methods are able to establish.[66] In addition to the fact that many proposals are simply technically unfeasible or impossible to enforce effectively, they would lower security for all by opening up vulnerabilities to unintended actors and would fail to achieve their ultimate goals.[67] In addition, restrictions would have serious detrimental effects on cyber security, trade and e-commerce.[68]

61 See references.
62 Berkman 2016.
63 McCarthy 2016. For a discussion of Germany, see Section 4.
64 ENISA and Europol. On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement. 20 May 2016.
65 Cazeneuve 2016.
66 See e.g. Harold Abelson et al. Keys Under Doormats: mandating insecurity by requiring government access to all data and communications. July 2015. http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf.
67 Bruce Schneier. op. cit.
68 Swire. See also Chicago Tribune. Encryption and the terrorists' tracks, available at http://www.chicagotribune.com/news/opinion/editorials/ct-fbi-terror-encrypt-apple-google-edit-1214-20151211-story.html (last accessed (29 August 2016);Nicholas Weaver. We think encryption allows terrorists to hide. It doesn't. December 2015. https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think-encryption-allows-terrorists-to-hide-it-doesnt.

Thus, the challenge that the deployment of encryption can pose for law enforcement authorities and other state agencies seeking access to secured data and communications remains on the agenda without an easy solution.[69]The question of how big the actual problem is for law enforcement, in establishing sufficient levels of lawful government access to information and communication for crime prevention, public safety and national security purposes, *because of encryption,* cannot be glossed over. US-based expert Peter Swire testified in a hearing on the matter in the US Congress that the current situation in which governments find themselves may be characterized as a golden age for surveillance.[70] Christopher Kuner, a prominent legal practitioner, when reflecting on the first round of debate about encryption and lawful government access in the 1990s, states they were proven wrong, when reflecting about the general perception that encryption proponents had won that round of debate.[71] The Harvard Berkman Center for Internet and Society also concludes that there is no situation that one can characterize as going dark.[72] It argues that: "the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will 'go dark' and beyond reach."[73]

To summarize, even though there are many proposals to interfere with the free deployment of strong encryption, in the interest of public safety, when evaluated on their merits, these proposals do not hold against close scientific scrutiny. In addition, these proposals side-step a more fundamental point, related to what is at stake for users. More advanced security measures are warranted and necessary, considering the existing threat landscape for users of digital communications and computing. This is particularly true for users with special needs with respect to the confidentiality of their communications. This existing threat landscape, which includes an international broad ensemble of state and non-state actors informs the increased adoption by services of strong encryption in the interest of users in services and tools that increase the protection of their information and communication.[74] To undo this development towards better security would be a serious step backward.

Encryption and the law: the broader landscape

An overview of all the many ways in which law relates to the deployment, use and development of cryptographic protocols is beyond the scope of this study. Still it is important to realize the enormous breadth of application in order to sketch the general landscape.

Strongly related to the protection of human rights is legislation with respect to privacy and data protection. The number of countries with data protection laws now amounts to more

69 For a discussion of the challenges in the context of organized crime, see e.g. Europol 2015, specifically Appendix 1: The encryption debate.

70 Testimony by Peter Swire. Senate Judiciary Committee Hearing." Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy". 8th July 2015. See also Peter Swire. Encryption and Globalization. Columbia Science and Technology Law Review, Vol. 23, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602.

71 Kuner 2013.

72 Berkman Center 2016.

73 Idem.

74 See also the following technology assessment for the European Parliament, which discusses and lists a range of policy options to address disproprtionate threats of government surveillance for individuals http://www.stoa.europarl.europa.eu/stoa/webdav/site/cms/shared/2_events/workshops/2015/20151208/EPRS_STU(2015)527410_REV1_EN.pdf (last accessed: 14 September 2016).

than 100.[75] One of the key principles for the fair and lawful processing of personal information regulated by such data protection laws is the principle of security. This principle implies that proper security measures are taken to ensure the protection of personal data against unlawful access by others than intended recipients. The new European Union General Data Protection Regulation, which was adopted in 2016 and will enter into force in 2018, contains an advanced set of rules with respect to the security of personal data. Encryption can be an important safeguard against personal data breaches, which can affect millions of people. Furthermore, encryption is of particular relevance for the implementation of privacy and data protection by design. These principles, which are more and more accepted as cornerstones for the protection of privacy and data protection in the 21st Century can only be realized through the innovations and implementations of cryptographic techniques.

Cryptography has also been an absolutely essential ingredient for establishing the conditions for e-Commerce over the Internet. The OECD Principles, discussed further below, were adopted to ensure that national cryptography policy would not interfere with this and to ensure the conditions for international developments in e-Commerce as well.

An overarching policy objective with respect to e-Commerce as well as data protection has been the promotion of trust in the online environment. It must be noted that from a human rights perspective, the promotion of trust cannot be a goal in itself. Ultimately, what matters here most is not that people have trust, but that there is a knowledge base with respect to the measures taken that does justice to the actual risks and harms that exist with respect to autonomy and human dignity.[76]

International cryptography policy and human rights

The policy debate about encryption has a significant international dimension because of the international nature of the communications networks and the Internet as well as trade, globalization and the national security dimensions. In fact, global trade and networked communications make it so difficult to untangle the international dimensions from the national ones, that encryption policy norms need to be agreed upon internationally to be sustainable for the online environment. Recognizing this, international organizations have contributed to the development of international norms related to encryption, in the field of data protection, economic policy, export controls, Internet governance and more recently on the supporting role of encryption for the protection of human rights. The technical internet community, including the IETF, W3C and the Internet Society has also since long made important contributions to the international developments related to encryption policy, through policy statements and standards.

The OECD Recommendation Concerning Guidelines for Cryptography Policy was adopted on 27 March 1997. The OECD states that reviews conducted since their adoption have concluded that they continue to be adequate to address the issues and purpose for which they were developed.[77] There are three components to this policy intervention of the OECD, which is primarily aimed at its Member Countries: a recommendation of the OECD Council, Guidelines for Cryptography Policy (as an Annex to the Recommendation) and a Report on Background and Issues of Cryptography Policy to explain the context for the Guidelines and the basic issues involved in the cryptography law and policy debate.

75 Greenleaf 2015. For this count, the inclusion of rules on security was a criterion.
76 As Kaye reports, "The trend lines regarding security and privacy online are deeply worrying.". op. cit. p. 12.
77 OECD Guidelines.

The key driver for the OECD was that its Member States' policy making with respect to the use of cryptographic methods in the commercial sphere was creating "obstacles to the evolution of national and global information and communications networks" and could "hinder the development of international trade".

The Principle which is most explicit about the connection to human rights is Principle 5 on the Protection of Privacy and Personal Data:

> The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

As with the other principles, an explanation is offered. It states: "Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimize the collection of personal data, by enabling secure but anonymous payments, transactions and interactions." Notably, the principle also raises the privacy and data protection issues that can be the result of the use of cryptographic methods in electronic transactions to ensure the integrity of those transactions. As is mentioned, these "include the collection of personal data and the creation of systems for personal identification" and therefore warrant the consideration of necessary privacy safeguards to be established accordingly.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods. With respect to lawful access, the principles call for a balanced approach, leaving the Member States considerable room for interpretation.

> National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.[78]

The focus of the principles was placed on the facilitation and the prevention of barriers to trade and e-commerce. Reflecting this focus, the most developed principle is the one addressing international co-operation. The OECD Principle states that:

> As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

As David Kaye summarizes, early in the digital age, "Governments recognized the essential role played by encryption in securing the global economy, using or encouraging its use to secure Government-issued identity numbers, credit card and banking information, business proprietary documents and investigations into online crime itself." The use of cryptographic methods in the media and communications environment in other domains is less developed, and the digital transformation of media and communications is at a relatively early stage.

In its study on the vision for the knowledge society, UNESCO, after consulting stakeholders, identified encryption as a relevant element for policy on privacy and freedom of expression. The Keystones report articulates that "to the extent that our data can be considered

78 The explanation states that: "This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.".

representative of ourselves, encryption has a role to play in protecting who we are, and in preventing abuse of user content. It also allows for somewhat greater protection of privacy and anonymity in transit by ensuring that the contents (and sometimes also the metadata) of communications are only seen by the intended recipient."[79] The report finally recognizes "the role that anonymity and encryption can play as enablers of privacy protection and freedom of expression", and proposes that UNESCO facilitates dialogue on these issues.

The Necessary and Proportionate Principles developed and adopted by civil society actors stipulates the protection of the integrity of communications systems as one of its 13 principles.[80] The principles themselves do not provide for explicit guidance on specific cryptographic policy issues such as backdoors or restrictions on the deployment of encryption.

The recent report of UN Special Rapporteur David Kaye provides the UN's first authoritative in-depth account of the human rights status of encryption as well as anonymity.[81] The report first discusses the contemporary landscape of encryption and anonymity tools. It relates these to the right to privacy as a gateway for freedom of expression and opinion, the right to hold opinions without interference and the right to freedom of expression. It evaluates different restrictions on encryption and anonymity, and provides for conclusions and recommendations paving the way for better protection in practice as well as further debate and stakeholder action.

Kaye notes for instance how encryption provides security so that individuals are able "to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion" (see A/HRC/23/40 and Corr.1, para. 23). He clarifies how encryption allows individuals to avoid undue restrictions on access to information and supports the freedom of expression and access to information and ideas regardless of frontiers. With respect to the application of the legal framework to interferences with encryption, the report outlines the general requirements in this context and provides the following:

> […] a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (see A/69/397, para. 12).

The Report's main conclusion is that "encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age". The Rapporteur acknowledges that "such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity". In view of possible limitations, the Report states that "restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective (see A/69/397, para. 56)". Specifically, it concludes that "court-ordered decryption […] may only be permissible when it results

79 UNESCO. Keystones to foster inclusive Knowledge Societies. Paris 2015.

80 International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles". Available at https://necessaryandproportionate.org.

81 David Kaye. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. May 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals".

The guidance that is offered by the OECD principles and the recent positions of the UN Rapporteur on encryption clearly states the importance of encryption for the protection of human rights. While it does not give a definitive answer to the question of whether a mandate for encryption 'backdoors' is to be considered incompatible with international law, it does point in that direction. Generally, the available guidance at the international level clarifies that when limitations are imposed on encryption, relevant human rights guarantees have to be strictly observed. After a selection of country studies in Section 4, Section 5 of this report discusses the application of international human rights instruments on freedom of expression and privacy to limitations on encryption in more depth.

4. National level developments in selected countries

Drawing on the literature,[82] one can discern many ways in which different laws and policies affect the regulatory governance of encryption. While it is outside of the scope of this study to give an in depth discussion of all the different legal dimensions, it is useful to consider a general typology of possible limitations and general positive measures with respect to encryption in relevant law and policy, before providing a number of country-specific case studies.

On the one hand, there are a wide variety of possible limitations imposed on encryption. Such limitations could amount to very serious and direct limitations on encryption, such as a blanket ban for use of secure encryption by individuals and private sector entities, and the criminalization of the use of encryption. They can also amount to conditions on the use of secure encryption, such as registration requirements for certain permitted entities and purposes, as well as government licensing requirements and export controls. Other relevant limitations include legal powers of circumvention (for instance, through the use of security vulnerabilities that have been discovered but have not been disclosed and addressed[83]), encryption key disclosure powers and decryption orders. Certain decryption orders, such as a mandate on electronic communications providers to be able to assist in lawful access to communications content, de facto amount to a ban on the deployment of end-to-end encryption solutions by service providers. In practice, there is a danger that certain problematic legal assumptions are attached to the use of encryption, such as the assumption that users of encryption are hiding criminal conduct. Finally, outside of legal restrictions, it is possible that informal agreements between the public and private sector lead to limitations on secure encryption for users in practice.

On the other hand, existing law and policy contains a wealth of positive measures that stimulate the adoption of encryption measures by different actors. As mentioned in Section 3, data privacy and e-Commerce laws require and incentivize the deployment of encryption and one can find relevant security requirements in the law elsewhere. In addition, the laws on standard setting can facilitate the development of encryption standards and stimulate their adoption across industries. Public policy can also contribute positively to encryption through user education programs, the financial support of tool development

82 The UN Rapporteur Report on Encryption and Anonymity and the underlying submissions contains a wealth of information about different limitations and positive measures.

83 Such security vulnerabilities are also called zero-days.

and distribution, and encryption-related research funding in the fields of mathematics, computer science and engineering.

In what follows, five country case studies are examined concerning the national state of affairs with respect to the legal and policy framework for encryption policy. The case studies follow the general typology discussed above in discussing limitations and positive measures. Specifically, these case studies address whether there are specific limitations in place or being debated on the use of encryption in the media and communications environment by users and organizations, and/or whether there are positive measures taken to promote the adoption and use of encryption in the media and communications environment. The studies go into some more depth on national level policy specifics that have particular relevance from an international perspective. The countries that were selected for these country reports are the United States, India, Germany and Brazil. The selection was based on geography and the accessibility of relevant materials. For the African region an approach was followed that presents information from different African regions, to overcome the challenge of finding enough relevant specific sources on encryption policy in one country in the region. The case studies thereby cover five continents. The specific countries within each region were also chosen based on their relative elaboration of encryption policy.

United States of America

There has been a broad, active and contentious policy debate on encryption in the USA since the 1990s. A first round of debate and developments, often called the 'Crypto Wars' took place in the 1990s. This involved the adoption of the Communications Assistance for Law Enforcement Act (CALEA), containing requirements for telecommunications providers and equipment manufacturers to ensure the possibility of effective wiretapping.[84] It also involved a debate over existing export controls on strong encryption products (considering their classification as munition) and a criminal investigation into cryptographic email software developer and activist Phil Zimmermann. This particular case was dropped and the general debate resolved after the liberalization of export controls on most commercial products with strong encryption features and the transfer of these items from the U.S.A. Munitions List (USML), administered by the Department of State, to the Commerce Control List (CCL), administered by the Department of Commerce.[85] The USA Department of Commerce maintains some controls over items on the CCL, including registration, technical reviews and reporting obligations, and continues to impose licensing and other requirements for sensitive encryption items and sales of such items to foreign governments.

Amongst experts, proposals have continued to be made to address the asserted issue of 'Going Dark' as a result of the shift in communications from telecommunications to internet-based communications services. The debate has become more prominent recently, reaching the level of several Presidential remarks on the issue. The current debate ignited after the Snowden revelations and the well-documented increase in deployed encryption measures by Internet services, device makers and users, as well as a concerted call from the technical community and civil society to increase encryption use and security to address

84 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010)

85 See USA Department of Commerce, Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility. June 2010. See also Ira Rubinstein and Michael Hintze. Export Controls on Encryption Software. http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm (last accessed: 14 September 2016).

mass surveillance practices.[86] The increased adoption of encryption by the industry has been received critically by certain government actors, the FBI in particular. They have led to the widely reported legal dispute between Apple and the FBI over the possibility to gain access to information on the iPhone in assistance to law enforcement.[87] In 2016, several bills were introduced in the US Congress that would place new limits encryption under USA law.

By and large, the USA's legal system promotes and requires security measures to be implemented in the relevant contexts, including cryptographic methods of various kinds, to ensure security in commerce and trade. An overview of such laws is beyond the scope of this country report but USA law contains a variety of laws promoting and requiring cryptographic methods. Relevant laws are the Federal Information Security Modernization Act (FISMA) of 2014, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA) and also the Federal Trade Commission Act. These acts contain security requirements and thereby indirectly require or stimulate the use of encryption in certain circumstances. Finally, many state breach notification laws treat encrypted data as a safe harbor by exempting firms that have encrypted data from notice obligations.

The support for the deployment and use of cryptographic methods also extends to the international context, in which the USA has been amongst the chief supporters of international coordination. The USA government supports research and development of cryptographic methods and standards through Departmental funding initiatives as well as through the National Science Foundation. Finally, the USA. State Department's Bureau of Democracy, Human Rights, and Labor (DRL) funds a broad range of internet freedom related projects whose goal is to "promote fundamental freedoms, human rights, and the free flow of information online, this includes government funding for strong encryption solutions to address restrictions and limitations on access to online information.[88]

Constitutional considerations and human rights play a role of significance in the USA debate about the legal treatment of encryption methods. Restrictions on distribution of cryptographic protocols, and the publication of cryptographic methods are considered an interference with the First Amendment, the USA constitutional safeguard protecting freedom of expression. Specifically, the Ninth Circuit Court of Appeals ruled that software source code is protected speech by the First Amendment and that the government's regulations preventing its publication were unconstitutional.[89] In addition, USA law and policy on encryption is strongly informed by considerations of USA competitiveness (for highly successful US-based companies to operate abroad and have access and excel in Internet service related markets) as well as lawful government access interests of law enforcement, national security and the intelligence community. A third factor that significantly implicates encryption policy is the objective of securing USA critical infrastructure.

---

86 See Ira Rubinstein and Joris van Hoboken. Privacy and Security in the Cloud, *Maine Law Review* 2014. Notably, the debate on encryption was already taking place before the Snowden revelations, as US law enforcement actors were arguing for the extension of wiretap obligations (CALEA) for internet services. For a discussion, see Adida et al. 2013.

87 Eric Geller 2016.

88 For an evaluation of funded projects and the program's effectiveness, see Ryan Henry, Stacie Pettyjohn and Erin York. Portfolio Assessment of Department of State Internet Freedom Program. RAND National Security Research Division. February 2014. http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1035/RAND_WR1035.pdf. A more recent study evaluates the question whether such projects could benefit illicit use Sasha Romanosky, Martin C. Libicki, Zev Winkelman, Olesya Tkacheva. Internet Freedom Software and Illicit Activity, Supporting Human Rights Without Enabling Criminals. Rand Corporation. 2015. http://www.rand.org/pubs/research_reports/RR1151.html.

89 Bernstein v. US Department of Justice, Ninth Circuit. Decided: 6th May 1999.

The USA has particularly active and strongly developed civil society actors involved in cryptographic policy and practice. The country is a primary site for cryptology research and engineering, development and implementation of cryptographic service innovations. In addition, there is a vibrant community of Non-Governmental Organizations engaged in the national and international debate on encryption policy.[90]

The predominant interferences with strong encryption that take place or are being considered take place in the field of national security, law enforcement and foreign affairs. In this area and in answering the contentious question of whether and how lawful access to specific communications could be ensured, the USA Government has internationally explained its policy as one aiming to ensure that 'responsibly deployed encryption' helps to "secure many aspects of our daily lives, including our private communications and commerce", but also "to ensure that malicious actors can be held to account without weakening our commitment to strong encryption".

Some specifics of how this difficult balance is currently struck in practice in the USA are available, through the following modalities (apart from the possibility that sufficient evidence can be obtained outside of the realm of potentially encrypted information and communication):

Technical assistance provisions

When the conditions for lawful access to information or communications are met, USA law, like other legal systems, provides for legal assistance obligations on relevant service providers to assist in the production of relevant information or communications sought by respective authorities. As mentioned above, CALEA imposes requirements on the telecommunications sector to ensure that service providers can assist with wiretapping communications. The Electronic Communications Privacy Act requires that service providers and certain other entities furnish "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference" with the services that the provider is providing to the targeted individual".[91] More recently, the FBI has been testing the boundaries of the All Writs Act to be used as the basis of court orders on service providers to circumvent device access. The widely reported legal dispute between Apple and the FBI is the best known example of this new line of cases, but similar requests have been made in different courts around the USA.

Informal cooperation

The USA legal framework offers a variety of legislative, constitutional and regulatory protections that ensure the protection of user data and communications against undue government access. USA law does provide legal space for voluntary cooperation and informal agreement between companies and government agencies, including to ensure optimal cooperation in criminal investigations and national security matters. ECPA does contain certain restrictions on voluntary disclosure for services that are covered, but they

90 See e.g. the Encrypt all the Things Campaign.

91 For discussion, see []. FISAAA 2008 contains slightly different language requiring that the assistance remains hidden from the user. In addition, Courts can use the general provisions in the All Writs Act to require assistance. For a discussion of a recent case, see Jennifer Granick. Federal Judge shines a spotlight on the "going dark" debate. The Center for Internet and Society. October 2015. http://cyberlaw.stanford.edu/blog/2015/10/federal-judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate (last accessed: 14 September 2016).

involve the production of data and not cooperation with respect to the ability to produce such data. Generally, USA constitutional safeguards do not apply in cases of voluntary cooperation for lack of required State action.[92] Senior officials in the intelligence community have clarified that one of the biggest impacts of recent revelations about government surveillance has been the growing unwillingness of major industry players to continue to cooperate voluntarily.[93] Internationally, the USA's Government finds itself in a unique position in comparison with other states, since many of the internationally most successful internet companies are based in the country.

Circumvention and breaking of protection

Finally, encryption of stored or transmitted data, even when implemented and done right, can be circumvented or cracked by relevant authorities to ensure lawful access to information and communications, without the involvement of a user or service provider. For instance, relevant authorities can gain access to unencrypted information on end-user devices through installation of key loggers or other means such as side-channel attacks. They could take advantage of implementation flaws in cryptographic software and implementations. There is an active debate about the ways in which the exploitation of software vulnerabilities (called 'zero-days') instead of fixing the insecurities, prolongs insecurity for Internet users more generally. Finally, the most contentious of the options above has been the documented interference with the security of cryptographic standards in standard setting contexts. This has led to deeply concerned reactions from the technical community[94] and international experts have questioned the lack of separation of offensive encryption related capabilities from information assurance in relevant USA agencies.[95] Specifically, the worry is that the mission to ensure defensive security is undermined by those in the same agency who focus on offensive capabilities. The legal regulation and constitutional scrutiny under USA law of the use of different methods to circumvent or break the security of encryption is in its infancy.

Considering these different options and the various challenges associated with them, the USA's landscape in this regard remains highly dynamic, and senior officials in the law

92 Compare Derek Bambauer. Orwell's Armchair. The University of Chicago Law Review 79 (2012), 3, pp. 863-944. https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/79_3/01%20Bambauer%20ART.pdf (last accessed: 14 September 2016). See also Solove 2002.

93 See Wilson Center Symposium. How Have We Changed? Evolving Views in the U.S. on Security and Liberty. Remarks of Bob Litt, https://www.youtube.com/watch?list=PLzM1iiQhVrdHHZPSZ1z_ztTrUuRPMUtRb&v=PWj8eqKKB64 ("There has been a long long history of cooperative relationships between American business and American government in the interest of protecting the nation and its citizens. [..] Companies have not been asked to do anything illegal. They have their own lawyers, they are pretty good at protecting their own interests. But just as you talked about that there are technological gaps that the NSA looks to fill, there are legal gaps. There can be an area of space between what is specifically authorized by statute and what is specifically prohibited by law and then there is a grey area in between, where we have been very successful over the years in securing voluntary cooperation. I think it has been an unquestionable loss for our ability to protect the nation if companies will stop that kind of voluntary cooperation."). See also Michaels, Jon D., All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror (October 6, 2008). California Law Review, Vol. 96, p. 901, 2008. Available at SSRN: http://ssrn.com/abstract=1279867.

94 Ed Felten. On Security Backdoors. Freedom to Tinker. 11th September 2013. https://freedom-to-tinker.com/blog/felten/on-security-backdoors/; Neal Koblitz and Alfred Menezes. A Riddle wrapped in an Enigma. December 2015. http://eprint.iacr.org/2015/1018.pdf; Daniel Bernstein, Tanja Lange and Ruben Niederhagen. Dual EC: A Standardized Back Door. Cryptology ePrint Archive: Report 2015/767.

95 Amir Mizroch, Surveillance and Silicon Valley Are 'Destroying' Europe's Privacy Balance. 11th December 2015. http://blogs.wsj.com/digits/2015/12/11/surveillance-silicon-valley-destroying-europes-privacy-balance.

enforcement and intelligence community have called for additional safeguards to ensure access to unencrypted communications and information. These proposals come in different varieties, including the extension of CALEA requirements, currently only applicable to telecommunications (including mobile phone) services, to Internet services, requirements of key escrow,[96] golden keys[97] as well as outright bans on end-to-end encryption functionality. At the time of writing, the position of the White House has been moderately against the introduction of new regulatory requirements. A draft policy document of the White House that was published by the *Washington Post* clarifies that it generally considers disavowing or deferring from introducing legislation.[98] This document also shows that the informal routes available to ensure optimal levels of lawful government access from a law enforcement and national security perspective remain central considerations.

Germany

As part of the global debate on encryption in the late 90's, a debate also took place in Germany about the need and legitimacy of imposing a general ban on the encryption of communications because of the impact on criminal investigations.[99] Unlike for example in the United Kingdom, a similar ban is no longer seriously considered.[100] There are profound doubts concerning the constitutional legitimacy as well as concerns about negative factual consequences of such a ban.[101] In qualitative terms, a number of fundamental rights are considered to be affected by restrictions on encryption: the secrecy of telecommunications, expressions of the general right of personality and, indirectly, all communicative freedoms that are exercisable over the Internet.[102] That is why the Federal Government set key points in 1999 for the German cryptographic policy which should especially provide confidence in the security of encryption instead of restricting it.[103]

Broadly speaking and besides the statements of the German Minister of the Interior towards possible future restrictions, Germany aligns with the position of the UN Special Rapporteur David Kaye and adopts policies of non-restriction or comprehensive protection and only adopts restrictions on a case-specific basis.[104] In the submission to David Kaye, it is clarified that the German cybersecurity strategy is about ensuring the security of businesses and private individuals on the Internet. The Federal Government therefore encourages and supports the use of encryption technology.[105]

96 Key escrow involves requirements that encryption keys are stored by third parties so to be available in case of lawful government access requests.

97 Golden key is another term that has been used for the creation of a backdoor to encryption security. The golden key proposal imagines the creation of a secure backdoor, the key of which is only known to authorized parties. The possibility to create secure golden key solutions is contested by the technical community.

98 NSC draft options paper on strategic approaches to encryption. Summer 2015. http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/.

99 Alexander Koch. Grundrecht auf Verschlüsselung?. CR 1997, p. 106.

100 Gerrit Hornung. Die Krypto-Debatte: Wiederkehr einer Untoten. MMR 2015, 145 et seq.; Kuner/Hladjk in Hoeren/Sieber. Multimedia-Recht. part 17, recital 62 et seq.

101 cf. Koch op cit. p. 108 et seq.

102 See Julia Gerhards. (Grund-)Recht auf Verschlüsselung?. 2010. p. 123 et seq.

103 Kuner/Hladjk in Hoeren/Sieber Multimedia-Recht. part 17, recital 64.

104 David Kaye. op cit. § 57.

105 Submission to UN Special Rapporteur David Kaye about the legal status of encryption technology in Germany.

Related to this, there have been recurring discussions on whether or not a master key for security agencies ('backdoor') is sensible and feasible. The debate also recognized the availability and possibility of more targeted solutions by discussing lawful access regimes that are not directed towards encryption algorithms themselves, but rather tend to be directed towards spying out passwords and keys using "sniffer"-software or "keyloggers".[106] There is a growing body of case law about these means of government access to data and the safeguards required on the basis of the German Basic Law (Constitution).[107]

The German population is often referred to, internationally, as attaching particular weight to the right to privacy and personal data protection. Germany may thus be remarkable in the general attitude of the population with respect to the protection of privacy and related safeguards. A survey conducted by BITKOM in Germany showed that the number of respondents who encrypt their emails increased from 6 % in 2013 to 16% in 2014. Although the poll of 1000 respondents may not be representative, the trend towards more encryption is recognizable.[108] There are several niche encrypted communications services and developer projects active in Germany, such as the German-based email provider Posteo that wants to set new standards in dealing with the data of its users.[109]

There is for example the Internet messaging service Telegram with headquarters in Berlin, that recently caused a stir because it was rumored that member of ISIS were using the service.[110] Gpg4win (GNU Privacy Guard for Windows), an encryption software for files and emails is another example with ties to German developers. It can be said that as a result of the Snowden leaks, a new generation of startups has grown in Germany.[111]

In November 2015 governmental representatives as well as representatives of the private sector signed a "Charter to strengthen the trusted communication "(Charta zur Stärkung der vertrauenswürdigen Kommunikation) together, in which they proclaimed: "We want to be Encryption Site No. 1 in the world".[112] Unlike elsewhere on a European level or in the USA, the recent attacks in Paris did not lead to a new national debate on encryption.[113] The German Federal Office of Information Security has provided new guidelines on the implementation of email standards, endorsing new technical standards of the IETF on secure email.[114] The German government has also used its foreign policy to promote international privacy

106 Gerhards. op cit. p. 409.
107 Cross reference to discussion of case law further on.
108 BITKOM Survey 08/2014. Cybercrime. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2014/August/140827-BITKOM-Charts-PK-Cybercrime-mit-BKA-28-07-14.pdf.
109 See Michael Scaturro, Protect your email the German way, The Guardian, 24 August 2016, https://www.theguardian.com/technology/2014/aug/24/posteo-protect-email-the-german-way-patrik-lohr (last accessed: 14 September 2016).
110 Markus Böhm. Messenger Telegram: Lieblings-App der IS-Terroristen sperrt Propagandakanäle. 18th November 2015.http://www.spiegel.de/netzwelt/apps/is-auf-telegram-messenger-app-kuendigt-massnahmen-an-a-1063535.html.
111 Isabelle de Pommereau. In Snowden's wake, crypto-startups take root in Germany. 3th August 2015. http://www.csmonitor.com/World/Passcode/2015/0803/In-Snowden-s-wake-crypto-startups-take-root-in-Germany.
112 Digital Agenda 2014-2017, p. 33.
113 See Fabian Warislohner. Tatort: Verschlüsselung. Die Schuldfrage nach Paris. 19th November 2015. https://netzpolitik.org/2015/tatort-verschluesselungstechnik-die-schuldfrage-nach-paris. But, see Cazeneuve 2016 for a recent joint call for action of the German Minister of the Interior with his French counterpart.
114 Richard Chirgwin, German infosec bureaucrats want mail providers to encrypt, The Register, 21 October 2015, http://www.theregister.co.uk/2015/10/21/german_infosec_bureaucrats_want_mail_providers_to_encrypt/ (last accessed: 14 September 2016).

standards. In particular, Germany, in a joint effort with Brazil, committed itself in the Human Rights Council for the appointment of an UN Special Rapporteur on Privacy.[115]

There are multiple examples of how there have been efforts by the government to implement encryption policy. They range from informal actions, to laws and regulations.

IT Security Act

The IT Security Act (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) that went into effect in July 2015 is the consequence of the Cyber-Security-Strategy that was decided upon in 2011. This law obligates carriers of particularly critical infrastructures, e.g. in the telecommunication sector, to provide adequate network security through minimum standards and notification requirements of IT-security-incidents.[116]

The 'De-Mail' law

A further example of a law explicitly dealing with encryption techniques is the so called 'De-Mail' law (*De-Mail Gesetz*), apparently named after the .de top level domain for Germany. This law's legislative goal was to establish a new electronic communication functionality with increased trust and reliability through signature and encryption techniques. Specifically, the law also constitutes and regulates a new form of Internet communication for private entities. [117] De-Mail-services require an accreditation for their service provision and are overseen by the authorities (§§ 17-21 De-Mail law). The De-Mail functionality has not been successful in terms of use, partly because of its incompatibility with conventional e-mail. It has also been criticized for offering suboptimal security, since it does not implement end-to-end encryption.[118]

Industry-specific regulations on encryption and information security

There are also several sector-specific rules for encryption and information security in Germany. So, for example, the Telecommunications Act (TKG) contains standards for telecommunications and the Energy Act (EnWG) for the energy sector. But on a European level, the Network and Information Security (NIS) Directive will force Essential Services and Digital Service Providers to be more secure in the future.[119] In anticipation of this, the Act on the Federal Office for Information Security (BSIG) was already updated on the national level. The law provides common obligations for "critical infrastructure" (see § 8 c BSIG for the scope).

Media pedagogical warnings and recommendations

Internet security, including information on encryption, is part of the education of the general public through media pedagogical warnings and recommendations, which are

115 See Monika Ermert, NSA-Skandal: UN-Sonderberichterstatter für Datenschutz in der digitalen Welt angestrebt, Heise Online, 23 March 2015, http://www.heise.de/newsticker/meldung/NSA-Skandal-UN-Sonderberichterstatter-fuer-Datenschutz-in-der-digitalen-Welt-angestrebt-2582480.html.

116 Detailed presentation at Philipp Roos MMR. Das IT-Sicherheitsgesetz, MMR 2015, p. 636.

117 With regard to the actual situation and history, see Alexander Roßnagel. Das De-Mail-Gesetz. NJW 2011, pp. 1473 et seq.

118 Cf. Andreas Voßhoff and Peter Büttgen. Verschlüsselung tut Not. ZRP 2014, p. 234.

119 See https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.

served through governmental institutions. Thus, the Federal Office for Information Security (BSI) and the state media authorities for instance give advice on sensible Social Media usage and warn about phishing traps, i.e. attempts to trick Internet users into providing their credentials through fake email messages. The state media authority of Saarland for example offers a seminar to encrypt data securely.[120]

The German fundamental right to the integrity of IT systems

As regards the constitutional basis, the ruling of the German Constitutional Court from 2008 concerning online searches[121] and its jurisprudence on informational self-determination may provide valuable input for the international legal handling of encryption techniques. The basis for the ruling was an authorization norm of an intelligence service (Verfassungsschutz Nordrhein-Westphalen) that was allowed secret access to information technology systems. The norm consisted of two elements, allowing the secret monitoring and other unveilings of the Internet (Alt. 1) as well as the secret access to information technology systems (Alt. 2). Scrutinizing these provisions under the German Constitution, the court took this as an opportunity to establish high standards for the infiltration and manipulation that reached far beyond the facts of the case at hand.

Specifically, the court created a new dimension to the general right of privacy: the *right to the protection of confidentiality and the integrity of information technology systems* (the so-called "IT basic right"). It concluded that an interference with this right by secret infiltration was only permissible if factual indications of a concrete danger for a predominantly important legal interest exist. Infiltration is in principle subject to judicial warrant.[122] The dimension of protection, and the progression as a result of technological advancement, that was pursued by the Court was widely acknowledged and appreciated.[123] It constitutes an adequate complement to telecommunications secrecy, which protects only the ongoing communication, not the system itself.

With the IT basic right, the constitutional court recognizes – metaphorically speaking - that parts of one's personality go into IT systems and therefore the applied protection has to travel with it. In the digital field this idea is being specified by the ruling of the Constitutional Court that already established the right to informational self-determination in 1983.[124]

It is worth discussing the specifics of the new right in a bit more detail. In the present-day digital environment, the self-determination that is protected requires the possibility of self-protection. An important way of achieving this protection is through the use of various encryption techniques in the digital environment. However, by infiltrating the IT-system, this self-protection is circumvented. This leads to an enhanced dependence of the individual on mechanisms and technological systems that lie outside of his or her control.

---

120 https://www.lmsaar.de/medienkompetenz/seminare/seminare-nach-themen-2/?mkz-action=details&seminarid=243.

121 BVerfG NJW 2008, 822.

122 BVerfG NJW 2008, 822 (831 et seq.); Some legal commentators have criticized the formulation as implying a fundamental right itself, rather than being an advancement to the existing right to informational self-determination, Cf. Martin Eifert. Informationelle Selbstbestimmung im Internet. Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, p. 521; Gabriele Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, p. 441..

123 Cf. Thomas Böckenförde. Auf dem Weg zur elektronischen Privatsphäre. JZ 2008, p. 925 et seq.; Gerrit Hornung. Ein neues Grundrecht. CR 2008, p. 299 et seq.; Thomas Stögmüller. Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen. CR 2008, p. 435 et seq.

124 BVerfGE 65, 1; e.g. the foundation of data protection in the constitution.

The Constitutional Court acknowledges this in regard to access by the intelligence service, which is specifically directed towards circumventing encryption technology and thereby circumventing self-protection provisions against unwanted data access of the targeted individual or his or her service provider. It views such infiltration as a particularly heavy infringement.[125] In other words, the individual was essentially granted the right to defend himself or herself autonomously against infiltration and manipulation of his personal data. In summary, it can be said that in the digital environment, the right to informational self-determination in Germany implies the right to use encryption with regard to its IT system.

However, another question that has to be asked is whether the Basic Law itself contains a "right to encryption", which applies comprehensively. This can possibly be derived from the combination of individual fundamental rights. Thus, the secrecy of telecommunications (Art. 10 I GG) and the inviolability of the home (Art. 13 I GG) are both affected by certain constellations as well. Through the technology-neutral secrecy of telecommunications, current telecommunications are protected from governmental insights. To ensure the confidentiality of data during transmission, it seems logical to consider the use of encryption methods protected by this right, too.[126]

The phrasing of the new IT basic right carries an element of a "guarantee". This illustrates that the ruling goes beyond the dimension of the fundamental rights as a defense against government interference. According to the court, the State also bears the responsibility of protecting the integrity and trustworthiness of information technology systems used by individuals against infringements by non-state actors.

Another constitutional goal is to prevent "chilling effects" on the exercise of communicative liberties. This negative effect was already mentioned by the Constitutional Court in 1983 (Volkszählung).[127] In this respect, there is a connection between the factual protection through encryption and the individual exercise of freedom, such as is the case, for example, with the free exercise of freedom of expression. Only a fearless exercise of one's communicative liberties can thus be described as truly free under the concept of the German constitution.

Additionally, a core insight of the ruling is that modern communication relies mostly on technology. Consequently, an effective protection of the fundamental rights in this area also requires protection of the technological communication infrastructure and its usage.[128] This objectified and functional approach to human rights protection is strongly developed in German constitutional law. The importance of technological design for freedom of speech is recognized in the international debate as well.[129]

Germany's work on privacy by design and data protection through technology

The acknowledgement of individual powerlessness against increasingly dynamic developments in complex IT-systems also leads to data protection concepts of privacy and data protection through technology and design, which apply in German law and at the

125 BVerfG NJW 2008, 822 (830).
126 Gerhards. op cit. p. 126 et seq.
127 BVerfGE 65, 1 (43).
128 Wolfgang Hoffmann-Riem. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. JZ 2008, p. 1009 et seq.
129 Cf. Jack Balkin. Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society. NYU Law Review 79 (2004).

EU level. The goal of these principles is to consider privacy interests and data protection proactively in early stages of conception and design of systems in order to prevent a frequently irreversible negative development regarding data security law.[130] Privacy by design can be a supportive factor on data security, data minimization and the development capability of its protection.

Because of this relevance, data protection through technology and data protection friendly defaults represent a significant element of the *General Data Protection Regulation* that has recently been adopted at the European level. Technological and organizational measures and procedures are required to ensure that the processing meets the requirements of the enactment and also the protection of the individual in question (Art. 23 GDPR). This approach is already hinted at on a national level in §§ 3a, 9 *Federal Data Protection Act* (Bundesdatenschutzgesetz, BDSG), whereas § 3a is centered around System Data Protection and § 9 around Data Security.[131] Although the German national law thus contains innovative approaches, they are not yet mature. For example, the non-observance of § 3a neither automatically leads to substantive illegality of the data processing, nor to a sanction.[132] As a result, it is hard to assess how effective the approaches actually are at the moment.

India

Although Indian law and policy promotes and requires the implementation of strong encryption as a security measure, such as in banking, ecommerce and by organizations handling sensitive personal information, there are a number of limitations on the free deployment of encryption by electronic communications services. Specifically, license agreements with services regulated under the telecommunications framework contain restrictions permitting only 40-bit encryption levels (details explained below). When strong encryption is deployed by these services, there is a practice of registration and key escrow in the interest of lawful government access to plaintext communications. There is notable legal uncertainty about the precise legal scope of these license requirements and to what extent they could have legal effect on (the use of or deployment of) services by the end-users of covered services. This legal uncertainty appears to be detrimental to the development, deployment and use of strong encryption in India for communications:

> risk-averse businesses may not exceed their encryption levels beyond 40-bit, otherwise they may run the risk of disclosing the "decryption key" to the Government of India and seek its prior approval.[133]

The encryption debate recently ignited publicly in India after the Government published a draft proposal with a number of envisioned limitations on the use of encryption. The policy,[134] issued under Section 84A of the Indian Information Technology (Amendment) Act, 2008[135] was short-lived, but worries remain about the lack of safeguards for privacy

130 Cf. Voßhoff/Büttgen op. cit. p. 232.

131 Ernestus in Simitis. Bundesdatenschutzgesetz. § 9 retical 1 et seq; Gola/Klug/Körffer in Gola/Schomerus. Bundesdatenschutzgesetz. § 9 retical 1 et seq; Jörg Pohle criticizes this prevailing opinion in: Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens. FlfF-Kommunikation 2/15, 41 seq.

132 Schulz op. cit. p. 208.

133 Apar Gupta. How many bits are enough? the legality of encryption. November 2011. http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

134 Indian Government Draft Policy. September 2015. Available at http://www.scribd.com/doc/282239916/DRAFT-NATIONAL-ENCRYPTION-POLICY (last accessed: 14 September 2016).

135 Available at http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (last accessed: 14 September 2016).

and freedom of expression that the draft illustrated.[136] In response to the outcry, the Indian government first exempted "mass use encryption products, which are currently being used in web applications, social media sites, and social media applications such as Whatsapp, Facebook, Twitter etc."[137] Soon thereafter, it withdrew the proposed policy and a new policy has not been made public yet.

Section 84A of the Indian Information Technology (Amendment) Act, 2008 empowers the government to formulate rules on modes of encryption for the electronic medium. It provides that: "The Central Government may, for secure use of the electronic medium and for promotion of e-governance, prescribe the modes or methods for encryption." The text of this provision suggests that it is aimed at authorizing the Central Government to make rules in the interest of network security, the promotion of e-commerce and e-government use. From the draft policy, it seems that the Indian Government considers Article 84A as a legal basis for restricting the use of strong encryption, instead of requiring or promoting it, or as an acknowledgement that use of encryption in the commercial or private sphere requires Government authorization, signaling the existence of a general ban without permission.

Legal commentators have noted the lack of transparency about what types of encryption use and deployment are permitted and required under Indian law, especially in the field of electronic communications services.[138] One reason for the legal uncertainty stems from the area of telecommunications law. A broad stipulation of exclusive government power over the establishment, maintenance and working of telegraphs is granted in the Indian Telegraph Act, 1885 (and amendments), which provides the principal regulatory framework for communications services in India (Section 4(1)). Section 3(1) of the Act, defines the term 'telegraph' broadly to include

> … any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, visual, or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means.[139]

Thus, the Central Indian Government has, in theory, a broad exclusive monopoly over electronic communications which includes the privilege to provide telecommunication and Internet services in India. This provision remains applicable to the provision of services that fall within the scope of the telecommunications regulations, the liberalization of telecommunications since 1999 notwithstanding.[140] The Government of India has allowed private players to provide relevant telecommunication and Internet services by entering into licensing agreements with them. These license agreements contain stipulations on the use of encryption.[141] Specifically, the License Agreement for the Provision of Internet Services (Clause 2.1(vii)) states that:

---

136 Bhairav Acharya. The Short-lived Adventure of India's Encryption Policy. December 2015. https://www.ocf.berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption-policy/.

137 Nandagopal Rajan. Encryption Policy: WhatsApp, web services out of draft encryption policy after outcry. September 2015. http://indianexpress.com/article/technology/tech-news-technology/draft-national-encryption-policy-you-might-need-to-store-whatsapp-messages-for-90-days/. (last accessed: 14 September 2016). On twitter, concerned users rallied around the hashtag #ModiDontReadMyWhatsapp.

138 Apar Gupta. How many bits are enough? the legality of encryption. November 2011. http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

139 India Telecom Laws and Regulations Handbook, 2013. Volume 1, p. 179.

140 Cf. Indian National Telecom Policy of 1999 http://www.dot.gov.in/telecom-polices/new-telecom-policy-1999; and more recent version of 2012. http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final.pdf.

141 Apar Gupta. op. cit.

> (vii) The Licensee shall ensure that Bulk Encryption is not deployed by ISPs. Further, Individuals/ Groups/ Organizations are permitted to use encryption up to 40 bit key length in the symmetric key algorithms or its equivalent in other algorithms without obtaining permission from the Licensor. However, if encryption equipments higher than this limit are to be deployed, individuals/groups/organizations shall obtain prior written permission of the Licensor and deposit the decryption key, split into two parts, with the Licensor.

These prescribed levels of generally permitted (symmetric) encryption (40-bit) may be considered insecure. Notably, the 40-bit level corresponds to the level of encryption that was permitted under former US export controls. Recently, a security vulnerability was discovered in the implementation of secure communications with websites. This vulnerability exploited the possibility to force connections between users and websites to degrade encryption to these former export proof levels. This shows how the negative impact of restrictions on security in practice can long outlast their legal lifespan.

Furthermore, the language in the license agreements on the use of stronger encryption reflects the practice of key escrow in India. Key escrow was illustrated by the widely discussed case of Blackberry's operations in India which is discussed further below.[142] The Cellular Mobile Telephone Service License Agreement contains similar restrictions on encryption use and requires inspection and approval of end-user devices deploying strong encryption.[143] While these license provisions signal a more restrictive environment, private industry has implemented strong versions of encryption exceeding the 40-bit level.

The draft proposals for encryption policy based on Section 84A that were published by the Indian Government follow a consultative process that took place after the adoption of this provision in 2008. Notably, in 2009, the Data Security Council of India issued recommendations for encryption policy.[144] Human rights considerations are relatively undeveloped in this recommendation, which discussed the needs of Indian law government agencies in gaining access to unencrypted text in some detail. The recommendation states the following about the interests at stake:

> Encryption policy requires consideration of various technical issues, national security issues, business privacy, and international competitive pressures for the growth of e-commerce and e-governance applications. Continued economic growth of Indian industries and business in an increasingly global economy require availability of cryptography to all legitimate users that include employees and business associates of the corporate sector.

This signals strong considerations in policies of Indian economic competitiveness internationally. Specifically, the Data Security Council notes that "foreign companies are likely to restrict outsourcing to India if plain text is asked for by law enforcement agencies without due process and/or court orders".[145] The recommendation proposes to further promote and liberalize encryption, not to adopt registration requirements and stipulates the way in which plain text access by law enforcement can generally be ensured while adhering to due process safeguards.

142 Cf. Paul Taylor. Security that makes spies feel insecure. *Financial Times*. 2nd August 2010, http://www.ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a.html#axzz3R5nCIW6I.

143 Apar Gupta. op cit.

144 See the Recommendations for Encryption Policy u/s 84A of the IT (Amendment) Act, 2008.

145 Recommendations for Encryption Policy u/s 84A of the IT (Amendment) Act, 2008, p. 11.

An illustration of key escrow and licensing practices in the Indian legal system and the way in which they interact with internationally operating communication service companies is the case of Blackberry which was discussed in international media.[146] The Indian Government required BlackBerry to allow monitoring of its e-mails and SMS.[147] To handle the lawful access requests from Indian authorities, BlackBerry set up domestic office in Mumbai. Although the precise details are not known, it appears that in this case the keys were held in escrow by Blackberry itself.

In the area of financial services and trading, there are specific regulations on required levels of encryption by relevant stakeholders. As per the Reserve Bank of India guidelines, for all banking transactions a minimum of 128-bit SSL (Secure Socket Layers) encryption is expected. The Securities Exchange Board of India (SEBI) prescribes a 64-bit/128-bit encryption for standard network security and mandates the use of encryption technology for security, reliability and confidentiality of data.[148] In the Information Technology (Certifying Authorities) Rules of 2000, the Indian Central Government stipulates a framework for cryptographic methods for digital signatures and related public-key cryptographic standards.[149] There are also the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, which are based on Article 43A of the IT Act, which require the implementation of reasonable data protection and security practices with respect to sensitive information by commercial actors, including for biometrics, medical information, sexual orientation and passwords.[150]

In the last decade, there has been some international support for India to join the Wassenaar Arrangement on Export Controls on dual use goods.[151] Indian regulations on foreign trade provide for export restrictions on "Information technology including information security", including "data processing security equipment, data security equipment and transmission and signaling line security equipment, using ciphering processes.",[152] which is language identical as used in the Wassenaar Arrangement, Munitions List.[153] There is no data on interpretation and enforcement of these rules in practice.

146 For discussion, see also Citizen Lab (Munk School of Global Affairs, University of Toronto) and Collin Anderson t. The Need for Democratization of Digital Security Solutions to Ensure the Right to Freedom of Expression. 10th February 2015. http://www.ohchr.org/Documents/Issues/Opinion/Communications/CitizenLab.pdf.

147 A. Parvathy, Ravi Shankar Choudhary and Vrijendra Singh. Legal Issues Involving Cryptography in India. April 2013. *International Journal of Computer Application*, Issue 3, Volume 2, http://rspublication.com/ijca/april13/6.pdf. See also Citizen Lab and Collin Anderson 2015.

148 Section 3(a) and referenced DOT Policy, http://www.nseindia.com/invest/resources/download/sebi_circ_27082010.pdf.

149 Information Technology (Certifying Authorities) Rules of 2000, http://cca.gov.in/cca/sites/default/files/files/rules.pdf (last accessed: 14 September 2016).

150 Ministry of Communications and Information Technology, Notification, New Delhi, 11 April 2011, http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (last accessed: 14 September 2016).

151 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. See http://www.nti.org/treaties-and-regimes/wassenaar-arrangement/ on India membership support.

152 Ministry of Commerce & Industry, Notification No. 14 (RE-05)/ 2004-2009, New Delhi; 15 July 2005, available at http://www.vertic.org/media/National%20Legislation/India/IN_Amendment_of_ITC_HS_Export_and_Import_Classification_2005.pdf (last accessed: 14 September 2016).

153 http://www.wassenaar.org/wp-content/uploads/2015/06/WA-LIST-13-1.pdf.

Brazil

After the Snowden revelations, Brazil was at the forefront of a global coalition promoting the right to privacy at the UN and condemning USA mass surveillance. In recent events, Brazil has demonstrated diverse aims when it comes to the use and implementation of encryption. On the one side, the country is a leader in providing a legal framework of rules for the Internet. On the other, it has taken several measures that may be seen to restrict the dissemination of encryption technology.

At this moment, there are no export/import controls on encryption technology in Brazil, be it at the level of software as well as hardware. There are also no controls as to the use of cryptographic technology. In 2015, in a process that was open for public comments and discussions, Brazil's legislator drafted a new privacy bill ("proteção de dados pessoais"),[154] which was sent to Brazil's Federal Congress on 13 May 2016 and came into force as Bill 5276 of 2016. It regulates and protects personal data and privacy, including online practices and includes provisions for more secure methods such as encryption on the treatment of personal data. The law also addresses security issues and a duty for companies to report any attacks and security breaches. In Article 44 (III) it states:

> *The controller shall immediately report any security incident which might damage the data subjects to the competent body.*
>
> *The notification shall include, at least: [...]*
>
> *III – Specification of the security measures used for protection of the data, including any encryption procedures;*[155]

Other than that, no provisions about encryption are included in the bill.

At the time of writing, the governmental crisis and the country-wide protests caused by several uncovered corruption affairs, which not only include parts of the government but also military and judiciary[156], awaken new fears in civil society as to a weakening of the rule of law. It remains to be seen whether these developments prove to have a wider impact on information and communication policy, including encryption.

The Marco Civil

With the Marco Civil, the Brazilian Civil Rights Framework for the Internet, Brazil was one of the first countries to ever introduce a law, that aims at combining all Internet rules in one bundle. With the Senate's approval and sanctioned by then president Dilma Rousseff, it went into effect in April 2014.[157] Although principles like freedom of expression and privacy are already protected by the Brazilian constitution, the new law specifies how these principles apply to the online environment. Moreover, it introduces and stipulates new principles like net neutrality:

---

154 Available at http://pensando.mj.gov.br/dadospessoais/ (last accessed: 14 September 2016).

155 Draft Law, On the processing of personal data to protect the personality and dignity of natural persons. Available at http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/02/Brazil_pdp_bill_Eng1.pdf (last accessed: 14 September 2016).

156 Glenn Greenwald, Andrew Fishman and David Miranda, 'New Political Earthquake in Brazil: Is It Now Time for Media Outlets to Call This a "Coup"?', The Intercept, 23 May 2016, https://theintercept.com/2016/05/23/new-political-earthquake-in-brazil-is-it-now-time-for-media-outlets-to-call-this-a-coup/.

157 The Brazilian Civil Rights Framework for the Internet, available at http://direitorio.fgv.br/noticia/the-brazilian-civil-rights-framework-for-the-internet.

Art. 9: The party responsible for the transmission, switching or routing has the duty to process, on an isonomic basis, any data packages, regardless of content, origin and destination, service, terminal or application.

In Art. 7 X the Marco Civil clarifies that the protection of personal data is important from a privacy standpoint and demands their elimination either by request of the user or after the end of the relationship between the parties.

Art. 7: The access to the internet is essential to the exercise of citizenship, and the following rights are guaranteed to the users:

(X) the definitive elimination of the personal data provided to a certain internet application, at the request of the users, at the end of the relationship between the parties, except in the cases of mandatory log retention, as set forth in this Law;

Although there are no verbatim provisions as to the right to encryption, the Marco Civil provides for the protection of the secrecy of the user's communication in several provisions, cf. Art. 7 II, III, Art. 11. It remains unclear however, whether this includes encryption.

Art. 7: The access to the internet is essential to the exercise of citizenship, and the following rights are guaranteed to the users:

(II) inviolability and secrecy of the flow of users' communications through the Internet, except by court order, as provided by law;

(III) inviolability and secrecy of user's stored private communications, except upon a court order;

and

"Art. 11: In any operation of collection, storage, retention and treating of personal data or communications data by connection providers and internet applications providers where, at least, one of these acts takes place in the national territory, the Brazilian law must be mandatorily respected, including in regard the rights to privacy, to protection of personal data, and to secrecy of private communications and of logs."

Encryption technology in the Brazilian private sector

Compared to some other countries, encryption still plays only a minor role for Brazilian companies. Therefore, the legislator is trying to introduce encryption and privacy measures, cf. above.

Meanwhile, many companies have a fragile security profile. On average, Brazilian organizations devote a smaller percentage of their IT budgets to encryption technologies than a number of other countries.[158] It seems, therefore, that the biggest challenge in Brazil regarding encryption is the implementation of existing methods and standards by relevant organizations, including in government and the industry.

A big incentive for companies to use cryptography, right after the compliance with regulations, is to protect the brand or avoid the reputational damage resulting from a data breach. Yet, a recent report showed that a staggering 46 % of the interviewed companies in

158 cf. Thales 2016 Global Encryption Trends Study: Brazil, https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study.

Brazil admitted to only have a limited or no encryption plan or strategy.[159] Over half of them stated that they do not have a functional leader who is responsible for determining the use of encryption. All in all, identity and access management, followed by discovery of data at risk, are the two largest data protection priorities.[160]

e-Government and participation

Regarding modern forms of interaction between citizens and the government, Brazil has a well-established e-government model: The Brazilian Public Key Infrastructure (Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil).[161] It was introduced in August 2001 with the Provisional Measure 2.200-2. The law itself is mostly concerned about the security of relevant infrastructure. In Article 10, however, it establishes the legal validity of ICP-Brasil certificates based on digital signatures. The certificate itself is generated and signed by a trusted third party, i.e. a Certification Authority. It contains the data of the holder, such as name and civil registration number and the signature of the Certificate Authority. Since 2010 ICP-Brasil certificates can be partly integrated in Brazilian IDs, which can then be used for several services like tax revenue service, judicial services or bank related services. In practice, the ICP-Brasil digital certificate acts as a virtual identity that enables secure and unique identification of the author of a message or transaction made in an electronic medium such as the web. However, the level of integration is still low.

The blocking of WhatsApp

In recent events, certain Brazilian courts have taken a stance against encryption in private messaging services by repeatedly ordering the blocking of the messaging service WhatsApp.[162] Ever since it switched to a full end-to-end encryption, the service has been periodically blocked as a result of a court order in an attempt to make the company comply with demands for information. As a result, other encrypted messaging services like Telegram or Viber have seen surges in reported sign ups. Telegram stated it had gained more than one million new users within days after the block became public (the service has over 100 million active users all in all).[163] It is apparent that there is a widespread demand for encrypted communications amongst Brazilians. This trend seems to be only reinforced by attempts to prevent the use of encrypted services.

159 Thales 2016 Global Encryption Trends Study: Brazil, https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study.

160 Although this was probably not the intention, some effects of the Marco Civil are already being felt in a negative way. The provisions demanding net neutrality, that were meant to protect the freedom of the internet, have already backfired, when it comes to access to information. As it prohibits private companies from offering open and free access to the internet, smartphone apps that offer free access to certain pages are seen to go against the code. Most notably the "Project Wikipedia Zero", aiming to promote the access to information via Wikipedia.org on mobile devices free of charge, is prohibited by the Marco Civil's net neutrality principles.

161 For more information, see http://www.iti.gov.br/icp-brasil.

162 Stephanie Mlot, Brazil Bans WhatsApp (Again) Over Encryption, pcmag, 3 May 2016, http://www.pcmag.com/news/344200/brazil-bans-whatsapp-again-over-encryption.

163 Telegram Messenger (@telegram), Twitter, 2 May 2016, https://twitter.com/telegram/status/727200237308227585.

The African region

As a result of the choice in this study not to discuss encryption policy in a specific country in the African region, the evidence provided below relates to a wide variety of countries in the African continent. The African region is diverse when it comes to the existing national legal frameworks at the national level. For the purposes of providing some evidence on encryption policy and the context thereof, this case study divides the African region into different groups of countries, after providing some general information on the African continent, These African sub-regions reflect regional economic communities like ECOWAS (Economic Community of West African States), EAC (East African Community), COMESA (Common Market for Eastern and Southern Africa), ECCAS (Economic Community of Central African States).

The African Union is the regional African intergovernmental organization (including North Africa) that has provided some specific legal and normative guidance for the African continent. The African (Banjul) Charter on Human and People's Rights, was adopted in the context of the African Union in 1981.[164] The oversight and interpretation of the Banjul Charter is the task of the African Commission Human and Peoples' Rights. A Protocol to the Charter, establishing the African Court on Human and Peoples' Rights was adopted in 1998 and came into effect in 2005. Only seven Member States of the African Union have recognized the right to bring cases to the Court, while as of February 2016, 30 of the 54 Member States have ratified the protocol. In the area of information policy, the African Union has adopted the African Union Convention on Cyber Security and Personal Data Protection.[165] The provisions on personal data protection in this Convention generally follow the European model for the protection of data privacy and contains a number of provisions on the security of personal data processing. A civil society initiative has adopted a specific African Declaration on Internet Rights and Freedoms "to help shape approaches to Internet policy-making and governance across the continent".[166]

The impact of model laws promoted by international governmental organizations, including the Commonwealth and le Francophonie, as well as international standard bodies for telecommunications, could be of significant influence on the specific policy issues discussed in this report, but an analysis of such influence goes beyond the scope of this study.

The percentage of Internet users in Africa is still much lower than the world average, which explains the (relative) lack of relevant legislation. Whereas the rest of the world sees a penetration of almost 50 % of Internet users of the whole population as of 2015, the African continent remains at 28,6 %.[167] It is expected that the ongoing mobile revolution will be able to change these figures, but it is likely that internet access will remain the dominant challenge in the internet policy area.

164 African (Banjul) Charter on Human and People's Rights, Adopted 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21 October 1986.

165 African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014. The Convention has currently been signed by 8 of the Member States.

166 See African Declaration on Internet Rights and Freedoms, available at http://africaninternetrights.org/ (last accessed 14 September 2016).

167 Internet World Stats, http://www.internetworldstats.com/stats1.htm (last accessed 14 September 2016).

North Africa[168]

Different countries in the North-African region have not seen a significant rise in legal actions aiming at the suppression of encryption in the transformations that started in 2011. However, although legislation often dates back to before the transformations, the enforcement has become stricter since then. No difference in the position towards cryptography can be seen between the countries that had successful revolutions and went through regime changes, like Tunisia, and those that did not.

Tunisia has several laws that limit online anonymity. Articles 9 and 87 of the 2001 Telecommunication Code ban the use of encryption and provide a sanction of up to five years in prison for the unauthorized sale and use of such techniques.[169] Although these laws were enacted still under the rule of the former government, so far there have been no successful efforts to make the relevant provisions more permissive. There have also been, however, no recent reports of these laws being enforced. Yet, their confirmed existence could be taken as evidence of the countries' hesitation to follow a more permissive approach towards the use of cryptographic techniques in the media and communication environment.

In Algeria, users have legally needed authorization for the use of cryptographic technology from the relevant telecommunications authority ARPT (Autorité de Régulation de la Poste et des Télécommunications) since 2012.[170] In Egypt, Article 64 of the 2003 Telecommunication Regulation Law states that the use of encryption devices is prohibited without the written consent of the NTRA, the military, and national security authorities.[171] Although enacted during the previous era, the law is still in effect. Additionally, the users of cybercafés have to obtain a PIN to access the internet. Therefore, they need to register with their name, email address and mobile number. All of this online information can be accessed by offices of the Presidency, Security, Intelligence, and the Administrative Control Authority without prior consent by court, if national security is of issue.

Egypt is reported use a software called "Remote Control System", which can capture data on the target's computer; monitor encrypted Internet communications; record Skype calls, emails, messages, and passwords typed into a browser; and remotely turn on a device's webcam and microphone.[172] Reportedly, when Egypt blocked Facebook's 'free basics' service in the end of 2015, it did so after it failed to obtain the cooperation of Facebook in matters relating to access to the data of Facebook users.[173]

---

168 The SMEX project on Arab Legislation and Orders Affecting Digital Rights, provides some references to relevant laws in the region, although not specifically on the issue of encryption. See https://smex.silk.co/ (last accessed 14 September 2016).

169 Loi n° 1-2001 du 15 janvier 2001 portant promulgation du code des télécommunications (Tunesia), available at http://www.wipo.int/wipolex/en/text.jsp?file_id=204160 (last accessed: 14 September 2016).

170 Decision No 17 du 11 June 2012, http://www.arpt.dz/fr/doc/reg/dec/2012/DEC_N17_11_06_2012.pdf (last accessed: 14 September 2016).

171 Egypt Telecommunications Regulation Law (Translation), available at http://hrlibrary.umn.edu/research/Egypt/Egypt%20Telecommunication%20Regulation%20Law.pdf (last accessed: 14 September 2016).

172 See Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware, Monk School of Global Affairs, 17 February 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/ (last accessed: 14 September 2016). See also Emir Nader, Egypt's purchase of hacking software documented in new leaks, Daily News Egypt, 6 July 2015, http://www.dailynewsegypt.com/2015/07/06/egypts-purchase-of-hacking-software-documented-in-new-leaks/ (last accessed: 14 September 2016).

173 See Yasmeen Abutaleb and Joseph Menn, Exclusive: Egypt blocked Facebook Internet service over surveillance – sources, Reuters, 1 April 2016, http://www.reuters.com/article/us-facebook-egypt-idUSKCN0WY3JZ (last accessed 14 September 2016).

In Morocco, the import and export of cryptographic technology, be it soft- or hardware, requires a license from the government. The relevant law No. 53-05 (Loi n° 53-05 relative à l'échange électronique de données juridiques) went into effect in December 2007. Art. 13 states:

> *In order to prevent its use for illegal purposes, and to protect the interests of national defence and the internal or external security of the State, the import, export, supply, operation or use of means for cryptographic services are subject to: a) a prior statement, when using this service has the sole purpose of authenticating transmission or ensure the integrity of data transmitted electronically; b) a prior approval from the administration, when it pertains to a purpose other than that specified in paragraph a) above.*

Articles 32, 33 and 34 stipulate penalties for breaches of Article 13 amounting to one-year imprisonment and fines of 100.000 MAD or about 10.000 US dollars. Since February 2015 the relevant authority for the approval and monitoring of encryption technology is no longer a civilian agency, but a military one, the DGSSI (Direction General de la Securité des Systèmes d'Information).[174]

In conclusion, a trend that limits encryption in favor of government surveillance is observable in the northern African states. The use of encryption technology is either banned or severely restricted.

East Africa

There do not seem to be any specific provisions to be in effect in countries in the East-African region restricting the use of encryption technology. Nevertheless, the surveillance powers of state appear to be expanding. As in other African countries, the main reason is the prevention of terroristic attacks. Kenya with its proximity to Somalia, has cited this threat for adopting restrictive actions. The country has recently fast-tracked a Computer and Cybercrime Law, to be adopted in the end of 2016.[175] The draft law, which builds on the European Cybercrime Convention, contains specific provisions on encryption, in the context of law enforcement access to data in the context of investigations. These provisions allow for an order to decrypt stored information and communication, on service providers that have such capability to decrypt. In Ethiopia, which is known for strict laws with respect to online activities, a number of bloggers charged with terrorism charges were also accused of encrypting their communications.[176]

In Uganda a number of laws and ICT policies have been passed over the past three years, none of them however deal with encryption. In 2016, following the Presidential Elections, the Ugandan government shut down social networks such as Twitter, Facebook

174 Bulletin officiel n° 6332 du 15 rabii II 1436 (5 February 2015), available at http://adala.justice.gov.ma/production/html/Fr/liens/..%5C188896.htm (last accessed: 14 September 2016).

175 See MyGov, Computer and cybercrime law to be in place before end year, 29 June 2016, http://www.mygov.go.ke/?p=10848 (last accessed: 14 September 2016).

176 See Endalk Chala, What You Need to Know About Ethiopia v. Zone9 Bloggers: Verdict Expected July 20, Global Voices Advox, 17 July 2015, https://advox.globalvoices.org/2015/07/17/what-you-need-to-know-about-ethiopia-v-zone9-bloggers-verdict-expected-july-20/ (last accessed 14 September 2016). See also Freedom House, Freedom on the Net 2015: Ethiopia, https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Ethiopia.pdf (last accessed: 14 September 2016).

and WhatsApp.[177] No difference seems to have been made between services using end-to-end encryption and others. As many users have opted for the use of VPN services, to circumvent restrictions, they were able to limit the extent to which they were affected by these restrictive actions.

West Africa

Nigeria, the most populous country on the continent, has by now the highest number of total Internet users in all of Africa: 51 % of its population.[178] In countries like Ghana and Côte d'Ivoire, the percentage of the population "online" is reported to just be around 20 %[179]. Although West-African countries appear to neither limit the import or export of encryption technology, nor its use, most national and foreign companies still rely on the use of VPNs for their communication.

Ghana recently introduced a draft law aiming at intercepting electronic and postal communications of citizens, ostensibly to aid crime prevention. Section 4(3) of the proposed bill gives the government permission to intercept anyone's communication upon only receiving oral order from a public officer.[180] Although other provisions stipulate the need for a judicial decision, section 4(3) overrides all of them, basically granting the government unlimited power for monitoring communication without court order. Considering these concerns, the UN Human Rights Committee has asked Ghana to provide legal safeguards to prevent the abuse of the bill.[181]

Recently the Nigerian Communications Commission has drafted a bill regarding Lawful Interception of Communications Regulations.[182] If passed, the bill allows the interception of all communication without judicial oversight or court order and forces mobile phone companies to store voice and data communication for three years. Furthermore, the draft plans to give the National Security Agency a right to ask for a key to decrypt all encrypted communication. Specifically, Section 13(1) of the draft bill states:

> *Where the Communication intercepted is an Encrypted or Protected Communication, the Licensee shall provide the National Security Adviser and the State Security Service with the key, code or access to the Protected or Encrypted Communication;*

Other countries in the West African region show significantly lower use of the Internet, ranging from just over 5 % in Togo to over 20 % in Côte d'Ivoire.[183]

---

177 See BBC News, Uganda Election: Facebook and Whatsapp blocked, 18 February 2016, http://www.bbc.com/news/world-africa-35601220 (last accessed: 14 September 2016). See also Nshira Turkson, A Social-Media Shutdown in Uganda's Presidential Elections, The Atlantic, 18 February 2016, http://www.theatlantic.com/international/archive/2016/02/uganda-election-social-media-shutdown/463407/ (last accessed: 14 September 2016).

178 See Internet World Stats, http://www.internetworldstats.com/stats1.htm (last accessed: 14 September 2016).

179 See Internet World Stats, http://www.internetworldstats.com/stats1.htm (last accessed: 14 September 2016).

180 Ajibola Adigun, Affront on Freedom in Ghana with the Introduction of Spy Bill, Student For Liberty, 29 March 2016, https://studentsforliberty.org/africa/2016/03/29/affront-on-freedom-in-ghana-with-the-introduction-of-spy-bill/ (last accessed: 14 September 2016).

181 News Ghana, UN Demands Statistics on Ghana's Spy Bill, 11 March 2016, https://www.newsghana.com.gh/un-demands-statistics-on-ghanas-spy-bill/ (last accessed: 14 September 2016).

182 Nigerian Communications Commission, Draft Lawful Interception of Communications Regulations, available at http://bit.ly/1du7UKO (last accessed: 14 September 2016).

183 See Internet World Stats, http://www.internetworldstats.com/stats1.htm (last accessed: 14 September 2016).

Southern Africa[184]

Users in South Africa are not prohibited from using encryption.[185] The provision of such technology, however, is strictly regulated by the Electronic Communications and Transactions Act, 2002.[186] Providers of encryption technology need to register with Director-General of the Department of Communications including providing detailed profiles of trusted personnel with supervisory or managerial responsibilities. Penalties range up to two-years imprisonment for any violation.

Since 2003, the Regulation of Interception of Communications and Provision of Communication-Related Information Act is in effect.[187] It empowers the police to demand decryption in any case of encrypted telecommunication after a court order. The addressee of the court order has to comply by providing a decryption key or at least assisting with the decryption. Penalties range from two Million Rand (ca. 140 thousand US Dollar) up to ten-years imprisonment, and a five Million Rand (ca. 340 thousand US Dollar) ceiling for companies.

Central Africa

Countries in Central Africa, like the Democratic Republic of Congo, the Central African Republic, Gabon and Cameroon do not yet have a well-developed legal framework addressing Internet policy issues. The Internet remains a relatively unregulated sphere. No actual legislation is known that limits the use of online media or prohibits the use of encryption technology. Only 3 % of the DRC's and 4 % of the CAR's population are active internet users, and 11 % in Cameroon.[188]

5. Human rights frameworks related to cryptography

International human rights instruments on freedom of expression and privacy

While a very broad range of human rights is touched upon by digital technologies, the human rights to freedom of expression (Art. 19 International Covenant on Civil and Political Rights [ICCPR]) and the right to private life (Art. 17 ICCPR) are of particular relevance to the protection of cryptographic methods. Unlike the Universal Declaration of Human Rights (UDHR) which is international 'soft law', the ICCPR is a legally binding international treaty.[189]

184 As no specific relevant information could be found on the other 4 countries in the Southern African region (Botswana, Namibia, Lesotho and Swasiland), the evidence presented relates to South Africa only.

185 See Freedom House, Freedom on the Net 2015: South Africa, https://freedomhouse.org/report/freedom-net/2015/south-africa (last accessed: 14 September 2016).

186 See Electronic Communications and Transactions Act, 2002 No. 25 of 2002, http://www.internet.org.za/ect_act.html (last accessed: 14 September 2016).

187 See Regulation of Interception of Communication and Provision of Communication-Related Information Act, Government Gazette, No. 24286, 22 January 2003, Act No. 70, 2002, http://www.internet.org.za/ricpci.html (last accessed: 14 September 2016).

188 See Internet World Stats, http://www.internetworldstats.com/stats1.htm (last accessed: 14 September 2016).

189 Toby Mendel. *The UN Special Rapporteur on freedom of opinion and expression: progressive development of international standards relating to freedom of expression*. in: McGonagle and Donders. The United Nations and Freedom of Expression and Information. chapter 8, p. 238.

The following analysis focuses on the universal system of human rights, however, it makes use of arguments developed for regional or national rights wherever they are useful.

Freedom of expression[190], including the freedom of information, protects the right of people to send and receive ideas and information.[191] While the holding of an opinion is a passive conduct and an absolute freedom[192], the right to freedom of expression includes the activities of seeking, receiving and imparting information and ideas.[193] Access to information is a precondition for free forming of opinion. Together with the freedom of opinion Art. 19 (1)), Art. 19 (2) is considered 'indispensable' for self-development, 'essential for any society', and '*the* foundation stone for every free and democratic society.'[194] Frank la Rue rightly mentions freedom of expression as an "enabler" of many other rights enjoyed under the ICCPR.[195] For the right to freedom of expression and information, the protected matter is characterized by mutual dependencies: information is the basis for expression, but expression will also produce and disseminate information.[196] Restrictions on the right to freedom of expression are only permitted under the conditions of Article 19, paragraph 3. Restrictions shall be provided for by law and they shall be necessary (a) for the respect of the rights or reputations of others or (b) for the protection of national security or of public order or of public health or morals. A further possibility for restriction is set out in Art. 20 ICCPR,[197] In the context of limitations on cryptography, restrictions will most often be based on Article 19 (3)(b), i.e. risks for national security and public order. This raises the complex issue of the relation, and distinction, between security of the individual, e.g. from interference with personal electronic communications, and national security. The two are not necessarily the same thing, they often are not. There is a danger that governments emphasize national security at the expense of technical definitions of computer security and/or human security.[198]

Article 19 of the ICCPR applies to all forms of audio-visual, as well as electronic and Internet-based modes of expression.[199] The text of the norm is thus clearly open to accommodate socio-technical developments. Article 19 also protects communication practices on the Internet and the different types of intermediary services, not only the services that disseminate information but also those enabling communication.[200] The Internet holds unprecedented potential for multidirectional communicative activity, also because of its relatively low entry barriers, and affordance to Internet-based actors that help determine the shape of freedom of expression and information.[201] The important roles of main

190 Art. 19 ICCPR; Art. 32 ACHR (Arab Charter on Human Rights); Art. 13 ACHR (American Convention on Human Rights); Art. 9 ACHPR (African Charter on Human and Peoples' Rights); Art. 23 AHRD (ASEAN Human Rights Declaration).

191 Sarah Joseph and Melissa Castan, *The International Convention on Civil and Political Rights*, third Edition, Oxford, 2013, p. 590.

192 Dominic McGoldrick, *The Human Rights Committee*, Clarendon Press, 1994, p. 460.

193 General Comment 34/11.

194 CCPR/G/GC/34, § 2 with reference to Marques de Morais v. Angola, 1128/2002; Benhadj v. Algeria, No. 1173/2003; Tae-Hoon Park v. Republic of Korea, No. 628/1995.

195 A/HRC/17/27, § 23. Cf. Michael O'Flaherty. op cit. pp 58 et seq.

196 Tarlach McGonagle. in: McGonagle and Donders. *The United Nations and Freedom of Expression and Information*. chapter 1, p. 3.

197 Manfred Nowak, CCPR Commentary, 2nd edition, p. 477. Cf. Michael O'Flaherty. International Covenant on Civil and Political Rights: interpreting freedom of expression and information standards for the present and the future. in: McGonagle and Donders. *The United Nations and Freedom of Expression and Information*. chapter 2, p. 69 et seq.

198 For a discussion, see Nissenbaum 2005.

199 CCPR/C/GC/34, § 12.

200 Josef and Castan. op cit. p. 599.

201 Tarlach McGonagle. ibid. p. 5.

moderator in public debates or main gatekeeper are therefore no longer primarily assigned to the traditional media, although traditional media is still the primary source of journalistic content and sets the agenda more broadly.[202]

Due to their structural importance for freedom of expression, the whole process of the protection of journalistic content against undue interference is covered by Article 19. Furthermore, this also means that limitations are only lawful when specific and imminent risks for important public or private interests can be demonstrated by the respective state. Based on that assessment, intermediaries may also enjoy freedom of expression protection because of their structural importance for others communicating, even if they are not making 'statements' by themselves. This will be elaborated below, specifically with respect to their role for access to encryption.

The right to privacy[203] protects against 'arbitrary or unlawful interference' with one's privacy, one's family, one's home and one's correspondence. Additionally, Article 17(1) of the ICCPR protects against 'unlawful attacks' against one's honour and reputation. The scope of Article 17 is broad. Privacy can be understood as the right to control information about one's self.[204] The possibility to live one's life as one sees fit, within the boundaries set by the law, effectively depends on the information which others have about us and use to inform their behavior towards us. That is part of the core justification for protecting privacy as a human right.

The provision on the right to privacy allows for new manifestations of the scope of protection.[205] Indeed, the rise of networked communications was not envisioned when the provision was drafted. However, the concept of 'correspondence' in Article 17(1) logically covers the integrity and confidentiality of new forms of private electronic communications, such as e-mails and direct messages on platforms like Twitter.[206] Insofar as electronic communications facilitate the freedom to seek, access and impart information and ideas, there is a close interrelationship between privacy and freedom of expression. Similarly, when cryptographic methods are used to ensure protection of confidentiality or integrity of information, thereby strengthening the protection of the right to privacy, it follows that the protection can be extended to these new forms of secure communication.[207] Only then, one can speak of actual freedom from unwarranted and unreasonable intrusions.[208]

The protection of Article 17 ICCPR also facilitates the freedom of thought, association and religion (even though they are also protected as separate rights). As such, privacy has the widely recognized quality of enabling the enjoyment of other rights – a quality it shares with the right to freedom of expression. From a scholarly perspective it has been claimed by Volio that 'all human rights are aspects of the right to privacy',[209] a notion reiterated by Regan.[210]

---

202 See Tarlach McGonagle. ibid.
203 Art. 17 ICCPR; Art. 21 ACHR (Arab); Art. 11 ACHR (America); Art. 21 AHRD.
204 See Charles Fried. Privacy. (1968) 77 *Yale Law Journal* pp. 475, 483.
205 F. Volio. Legal Personality, Privacy and the Family, p. 197, in: L. Henkin, '*The International Bill of Rights*', New York: Columbia University Press 1981. This is equally true of Art. 8 of the European Convention of Human Rights, see e.g. ECtHR 4 dec. 2008, Appl. No 30562/04, §66, for an overview of protected realms including ECtHR jurisprudence.
206 General Comment 16/32, §8. Manfred Nowak. op cit. p. 401.
207 See also Wagner 2012.
208 Cf. the definition of SE Wilborn. Georgia Law Review 32 (1998), pp. 825, 833.
209 F. Volio. op cit. p. 193.
210 See Regan 1995.

In addition to the duty to not infringe these rights, States have a positive obligation to effectively ensure the enjoyment of freedom of expression and privacy of every individual under their jurisdiction.[211] Section 2, Article 17 ICCPR on the right to privacy explicitly orders states to protect citizens against interferences through legislation and other measures.[212] The right has to be guaranteed against interferences and attacks whether they emanate from State authorities or from natural or legal persons.[213] Importantly, the confidentiality and integrity of communications is to be protected both de jure and de facto,[214] while effective measures need to be in place to ensure that data processing by both public authorities and private bodies adheres to the Covenant.[215]

When considering the protection of a particular form of encryption under these relevant human rights, it is worth making the distinction between the technical application of encryption on the one hand, and the human-facing properties of communications, information and computation on the other hand. As discussed before, these properties include confidentiality, privacy, authenticity, availability, integrity, and anonymity. It is this set of properties of communication and information storage or processing tools, which deserves protection against interferences, because these properties effectuate the protection of the rights protected under international human rights law. Consequently, the Committee of Ministers of the Council of Europe has identified prohibition or weakening of encryption as indicating steps contrary to Internet freedom.[216]

Freedom of expression and opinion and the right to private life (including the right to private communications) can be in conflict in specific situations. Immediately at the outset, it was recognized that the positive obligations under Article 17, Section 2 must not lead to the authorization of censorship and the fact that the right to privacy and the right to freedom of expression are interdependent.[217] Freedom of expression can interfere with but has to respect the protection of the right to privacy, when expression relates to or affects a natural person. There is an additional link. The basic human need in communication contexts is to communicate and receive information and to develop one's personality. To be meaningful in that respect, the process of communication has to fulfill certain normative requirements that extend to both the rights in question.

As mentioned above for the example of freedom of expression, these rights may conflict with other rights and interests, such as dignity, equality or life and security of an individual or legitimate public interests. In these cases, the integrity of each right or value must be maintained to the maximum extent, and any limitations required for balancing have to be in law, necessary and proportionate (especially least restrictive) in view of a legitimate aim (such as the rights of others, public morals and national security).

---

211 CCPR/G/GC/34, § 11.

212 General Comment 16/1.

213 General Comment 16/1.

214 Nowak further notes that this protection of the secrecy of correspondence and telecommunications under article 17 ICCPR extends to cases in which information dissemination systems are operated by private firms. Cf. M. Nowak, p. 401.

215 General Comment 16/32, § 8 - § 10.

216 Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom. 13th April 2016. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa, points 4.1.7. and 4.2.5.

217 M.J. Bossuyt, 'Guide to the "travaux préparatoires" of the International Covenant on Civil and Political Rights', Dordrecht: Nijhof 1987, p. 346, referring to the Commission of Human Rights, 9th session, E/CN.4/SR.374, p. 12-15.

Guaranteeing "uninhibited communications"

Building on Frank La Rue's assessment of the structural importance of freedom of expression, it is important to identify essential characteristics of legal and factual preconditions that make the process of communications effectively "free". One of these essential requirements that is strongly fostered by the availability of encryption, is what one can call the requirement of "uninhibited communications". Encryption supports this mode of communication by allowing people to protect the integrity, availability and confidentiality of their communications. The requirement of uninhibited communications is an important precondition for freedom of communication, which is acknowledged by constitutional courts like the US Supreme Court[218]and the German Bundesverfassungsgericht[219] as well as the ECtHR[220].

More specifically, meaningful communication requires people's ability to freely choose the pieces of information and develop their ideas, the style of language and select the medium of communication according to their personal needs.[221] The imposition of censorship instruments and its effects on the free exercise of freedom of expression is an example of adverse effects on these important aspects and features of the right. Providing falsified content through interference with the security of dissemination channels distorts what an expressing actor had wished to convey. The knowledge of third parties monitoring communications is capable of changing the mode of communication.[222] Citizens might choose to change their way of expression, to trick a censor or to even refrain entirely from communicating on specific issues through self-censoring. The latter demonstrates that the "chilling effect" can be seen as a possible distortion of communication, in case the conditions for uninhibited communication no longer exist.

Uninhibited communication is also a precondition for autonomous personal development. Human beings grow their personality by communicating with others.[223] According to the UN's first Special Rapporteur on Privacy, professor Joe Cannataci, privacy is not just an enabling right as opposed to being an end in itself, but also an essential right which enables the achievement of an over-arching fundamental right to the free, unhindered development of one's personality.[224] In case such communication is inhibited, the interaction is biased because a statement does not only reflect the speaker's true (innermost) personal views but can be unduly influenced by considerations that should not shape communication in the first place. Therefore, the process of forming one's personality through social interaction is disrupted.

These restrictive effects of such disruption, directly affect the free expression of information and ideas of a person. Moreover, when the conditions for uninhibited communications no longer exist, this may influence the communicative and expressive climate in a society as a whole. Thus, the lack of "uninhibited communications" may result in the general numbness or freezing of intellectual life.[225] This more general effect makes any state action that hampers

218 See for example New York Times Co. v. Sullivan, 376 U.S. 254 (1964) and Dombrowski v. Pfister, 380 U.S. 479 (1965).
219 See BVerfG NJW 1995, 3303 (3304) and BVerfG NJW 2006, 207 (209).
220 Cumhuryiet Vafki and others v. Turkey, ECHR 10.08.2013 - 28255/07; Ricci v. Italy, ECHR 10.08.2013 - 30210/06.
221 Cf. General Comment 16/8.
222 As General Comment 34 emphasizes, there is an interrelationship between privacy and freedom of expression. Cf. from an american perspective Canes-Wrone/Dorf, NYU Law Review 90 (2015), 1095 et seq.
223 Tarlach McGonagle. The United Nations and Freedom of Expression and Information. chapter 1, p. 3.
224 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/31/64.
225 Cf. Sylvie Coudray. The United Nations and Freedom of Expression and Information. chapter 7, p. 258.

the possibility of "uninhibited communications" per se a grave restriction of the freedom of expression. Furthermore, it supports the views that the use of encryption technology falls within the scope of the right to the freedom of expression ("right to encryption"). The example of the German Constitutional Court's ruling on the "IT basic right"[226] supports and illustrates the viability of extending basic rights in view of technological change in similar ways: The German constitutional court recognizes – metaphorically speaking – that parts of one's personality move into IT systems and therefore the applied protection has to travel with it.

Since state measures that restrict the use and deployment of encryption tend to have the effect of restricting "uninhibited communications", one can make a strong argument that a concept of effective human rights protection has to cover the possibility of a citizen to protect his or herself by technology. In a complex society freedom of speech does not become reality when people have the right to speak. A second level of guarantees need to protect the precondition of making use of the right to express oneself. If there is the risk of surveillance the right to protect one freedom of speech by means of encryption has to be considered as one of those second level rights. Thus, restriction of the availability and effectiveness of encryption as such constitutes an interference with the freedom of expression and the right to privacy as it protects private life and correspondence. Therefore, it has to be assessed in terms of legality, necessity and purpose.

Procedural aspects: guaranteeing transparency

Freedom of expression and the right to privacy (including the right to private communications) have a substantive character, i.e. they materially protect a certain behavior or a personal state. It is well established in fundamental rights theory that substantive rights have to be complemented by procedural guaranties to be effective.[227] Those procedural guarantees can be rights such as the right to an effective remedy. However, it is important to acknowledge that those procedural rights must, similar to the substantive rights, be accompanied by specific procedural duties of governments without which the rights would erode.

Civil and political rights in the ICCPR and UDHR are classically at least primarily perceived as freedoms from state interference.[228] They are conceptualized as negative rights. That means they require a state to refrain from certain actions. As discussed earlier, to some extent the rights also require positive action, including to protect against intrusions into rights by non-governmental entities.[229] Of course, the ICCPR treaty binds only the state directly, therefore there has to be a state action or omission to invoke fundamental rights. At the same time, the UN Guiding Principles on Business and Human Rights do call on private actors to respect human rights in their operations.

When looking at state action from this perspective, it is worth noting that in many policy fields we can observe changes in the modes of legal governance. Such legal governance is often not to be characterized as more traditional linear form of regulation between the state and citizens in vertical relation. But it is rather exercised in a network of state and non-state actors and does not build on legal norms alone but also on informal instruments.[230]

226 BVerfG NJW 2008, 822.
227 Cf. Robert Alexy and Julian Rivers. A Theory of Constitutional Rights. pp. 315 et seq.
228 Herdegen. Völkerrecht. § 47 recital 1.
229 Cf. Schiedermair. Der Schutz des Privaten als internationales Grundrecht. p. 74.
230 See e.g. Røiseland. Informal Governance. In: Encyclopedia of Political Science, p. 1018.

This is particularly the case with respect to information and communications technologies and services in the current globalized environment.

These networked governance arrangements, including informal instruments, can be highly effective in achieving regulatory goals. However, from a human rights perspective, they also trigger risks. When governance systems become more and more complex and when state actors informally collaborate with private actors in human rights sensitive areas,[231] there is the risk of a diffusion or obfuscation of responsibility. Citizens do not know, who to hold accountable for certain effects or perceived injustices. Therefore, the substantial rights have to be construed in a way that they also contain the duty to make governance systems transparent, at least to the extent that allows citizens to assess (1) who made a decision and (2) what measures have been taken.

This is highly relevant to government talks with intermediaries and other industry players, in various jurisdictions, as regards encryption. These talks and their outcomes can lead to a system where states do not take formal action but just rely on the cooperation with the industry to hand over data or encryption keys whenever requested, and irrespective of an evaluation of the legality, necessity and legitimate purpose. Since there is then no law or regulation which can be subject to legal scrutiny, the procedural aspect of human rights protection requires transparency (other procedural and substantive safeguards notwithstanding). States have a duty to be transparent about these networked arrangements and the restrictions these impose on the free use and deployment of secure cryptographic methods and technologies. The opposite is achieved when so called "gag orders" are issued. These orders often prevent the industry not only from informing data subjects but also the general public about deliberate interferences with their rights. In this respect a call for transparency is more than general call for bringing things out of the dark and ensure accountability. It is the precondition to know about the dangers for fundamental rights and make use of the respective freedoms.

States, users and service providers: 'security intermediaries'

Since users rely on service providers for the security of their data, it is important to consider the legal framework for these service providers with particular care, also from the perspective of the protection of human rights in the digital domain. Section 2 of this study already illustrated the variety of configurations in which cryptographic methods are potentially deployed in the interests of end-users. From this overview it is clear that, outside of the possibility that users deploy protections themselves, the effectuation of human rights protection requires the impulse and involvement of service providers. Regarding surveillance of users of cloud-based services, in many respects "a user cannot protect himself but depends on the cloud provider for the enjoyment of fundamental rights and the protection against arbitrary national security interferences".[232] These service providers often act as intermediaries facilitating expression and communication of their users of different kinds.[233] Users should be able to rely on their service providers to take the appropriate state of the art measures that ensure the integrity, availability and confidentiality of their information and communication. States should therefore not hamper the ability of media and communication platforms and services to use secure cryptographic methods. Instead,

231 Cf. Tarlach McGonagle. op cit. chapter 1, p. 39.
232 See Arnbak 2016.
233 MacKinnon et al. UNESCO study; Cf. Karol Jakubowicz. Early days: the UN, ICTs and freedom of expression. in: The *United Nations and Freedom of Expression and Information*. chapter 10, pp. 324 et seq.

legal frameworks should provide for obligations on service providers or at least incentivize them to do so, for instance by setting technical minimum standards in their data protection and security acts or establishing data security seals which can signal the implemented degree of protection to the users. In any case measures taken by intermediaries to protect their users' privacy fall within the scope of both Article 19 and Article 17 ICCPR due to their structural importance for the factual protection of those freedoms.

In debates about cryptographic policy, the question of lawful government access – and the conditions under which such access should take place in order to respect human rights – has a vertical and national focus. What is meant here is that the discussion addresses the duties and responsibilities of the state in relation to the members of its own society, and the laws and regulations that should be established accordingly, while respecting human rights. In each separate country, the concern about access thus tends to be centrally about a lack of access of the proper authorities. What sometimes does not get acknowledged sufficiently, is the fact that the services and tools that are being discussed do not stop at borders.[234] The same is true for government and other actors that may seek to gain access to information and communication transnationally. The international dimension and the possibility of transnational access, actually means that foreign actors should be included in threat models for data protection and cybersecurity policies.[235] This is one reason why cryptographic methods can be actively explored to restrict and shape transnational access to data by governments.

These complexities of jurisdiction in lawful government access are significant and present a still unsolved puzzle. In particular, there has been a dramatic shift from traditional lawful government access to digital communications through the targeting of telecommunications providers with strong local connections, to access through targeting over-the-top services with fewer or loose connections to the jurisdictions in which they offer services to users. This raises the question in which cases such internationally operating service providers should (be able to) hand over user data and communications to local authorities. Relevant considerations include the locality of the data, the respective user(s), and the users' nationality, and the jurisdictional specifics of the subject under investigation.

The deployment of encryption by service providers is a further complicating factor in this setting. From the perspective of service providers, it seems likely that cryptographic methods will have to be designed to account for only providing user data on the basis of valid legal process in certain situations. More specifically, cryptographic methods are increasingly amongst the necessary ingredients of measures to limit exposure of user data and communications and reduce the complexity of dealing with government access requests. End-to-end encryption can have the result that no content data is available to hand over in response to a lawful government request, but a shutdown of the service in such cases is clearly disproportionate.

234 Cf. Karol Jakubowicz. Early days: the UN, ICTs and freedom of expression. in: *The United Nations and Freedom of Expression and Information*. chapter 10, pp. 341 et seq.

235 See e.g. Kristina Irion. Government Cloud Computing and National Data Sovereignty. 30th June 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859. See also Joris van Hoboken, Axel Arnbak and Nico Van Eijk. Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad. 9th June 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

In recent years, companies and especially online intermediaries have found themselves increasingly in the focus of the debate on the implementation of human rights.[236] Against this background, it is worth noticing that online intermediaries[237] not only have a role of intermediaries between content providers and users but also one of "Security Intermediaries" in various aspects. Their practices and defaults as regards encryption are highly relevant to the user's access to and effective usage of those technologies. Since a great amount of data is travelling through their routers and is stored in their clouds, they offer ideal points of access for the intelligence community and non-state actors. Thus, they also, perhaps involuntarily, function as an interface between the state and the users in matters of encryption policy. The role has to be reflected in the human rights debate as well, and it calls for a comprehensive integration of security of user information and communication in the emerging Internet governance model of today.

Human rights and encryption: obligations and room for action

The table below shows the specific risks that could be addressed, as well as relevant services' adoption of cryptographic solutions and the minimal requirements and good practices to address these risks effectively. The minimum requirements identified in this study with respect to human rights and cryptographic policy are not exhaustive and are offered to help guide further norm development in practice at various levels.

Risks	Relevant services adoption of cryptographic solutions	Good practices
Technical restrictions on access to content (blocking) Interception Hacking by state and non-state actors Traffic analysis and surveillance Interference with the reliability or authenticity of content	Cloud storage providers Internet connectivity provider Publisher sites Search engines Messenger and communications services Browsers	Secure authenticated access to publicly available content Legal certainty Transparency about interferences Availability of end-to-end secure communications Availability of anonymous access Education, including media and information literacy Standards and innovation

236 Cf. the UN Guiding Principles on Business and Human Rights. 2011. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf and the UNESCO publication Fostering Freedoms Online. The Role of Internet Intermediaries. 2014. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

237 Cf. Karol Jakubowicz. Early days: the UN, ICTs and freedom of expression. in: The United Nations and Freedom of Expression and Information. chapter 10, pp. 324 et seq.

In specific cases of interference with the freedom to use and deploy cryptographic methods, a legal assessment has to take place to take account of the specific legal, societal and technical circumstances with an eye to international human rights standards. The concept of Internet Universality, developed by UNESCO, including its emphasis on openness, accessibility to all, and multi-stakeholder participation, can also be brought to bear. While these minimal requirements and good practices can be based on more abstract legal analysis, these assessments have to be made in specific contexts.

To summarize, with some examples, several remarks can be made. Secure authenticated access to publicly available content, for instance, is a safeguard against many forms of public and private censorship and limits the risk of falsification. It can foster trust in an online public sphere and for online services and e-commerce in general.[238] One of the most prevalent technical standards that enables secure authenticated access is TLS. Closely related to this is the availability of anonymous access to information. It allows users to obtain knowledge of any field of personal or political interest without fearing repercussions or even justifying their interests in front of others. As mentioned previously, TOR is a system that allows the practically anonymous retrieval of information online. Both aspects of access to content directly benefit the freedom of thought and expression.

The principle of legal certainty is vital to every juridical process that concerns cryptographic methods or practices. Legal certainty makes outcomes predictable and allows citizens to shape their actions more consciously. As such, the principle is essential to any forms of interception and surveillance, because it can prevent unreasonable fears of surveillance, such as when the underlying legal norms are drafted precisely. Hence, legal certainty may avert chilling effects by reducing an inhibiting key factor for the exercise of human rights.

Continuous innovation in the field of cryptography and setting and spreading new technical standards is essential as well. Cryptographic standards can expire quickly as computing power increases continuously. Even maintaining a certain level of protection therefore necessitates a continuous modernization of cryptographic techniques and their quick dissemination. Here, education has key role for establishing and spreading these standards, because in almost all cases the encryption of information is an effort that needs to be made by two or more parties. Users themselves need continued media and information literacy to keep abreast of the issues.

The lawfulness of limitations

We have now demonstrated the scope of human rights protection regarding encryption. However, the actual impact of human rights can only be assessed by analyzing the possible limitations that states can set for those freedoms. The national security can without any doubt be a legitimate aim for actions that limit the freedom of speech and the right to privacy. However, the measures have to be necessary and proportional. Whether that is the case can only be assessed on a case by case basis. However, this analysis also provides criteria that can become highly relevant when testing the lawfulness of an interference of a state with the right to encryption as a guarantee enshrined in the freedom of expression and in privacy as demonstrated above. An interference with this right is especially severe if:

- It affects the ability of key service providers in the media and communications landscape to protect their users' information and communication through secure

238 For more in depth discussion, see Section 2.

cryptographic methods and protocols, thereby constituting the requirement of uninhibited communications for users of networked communication services and technologies.

- The state reduces the possibility of vulnerable communities and/or structurally important actors like journalists to get access to encryption;
- Mere theoretical risks and dangers drive restrictions to the relevant fundamental rights under the legal system of a state;
- The mode of state action, e.g. if restrictions on fundamental rights are established through informal and voluntary arrangements, lead to unaccountable circumvention or erosion of the security of deployed cryptographic methods and technologies.

6. Recommendations

General recommendations

There needs to be recognition of cryptographic methods as an essential element of the media and communications landscape. What ultimately matters, from a human rights perspective, is that cryptographic methods empower individuals in their enjoyment of privacy and freedom of expression, as they allow for the protection of human-facing properties of information, communication and computing. These properties include the confidentiality, privacy, authenticity, availability, integrity and anonymity of information and communication.

The protection of encryption in relevant law and policy instruments from a human rights perspective is particularly important because encryption makes it possible to protect information and communication on the otherwise insecure communications platform that is the Internet. Initially, the Internet was itself not designed to provide for the security of information and communications generally. Over the years, cryptographic techniques have become a core component of the Internet, supported by numerous protocols and standards that support their implementation in practice. Encryption makes it possible to help ensure confidentiality, privacy, authenticity, availability, integrity and anonymity in specific settings. This facilitates the protection of human rights of Internet users, and freedom of expression and privacy in particular.

Further recommendations on the structural conditions related to encryption and human rights are listed below:

[1] Encryption policy should be seen in a broader context of Internet Governance and the broader societal functions of and human values implicated by the various uses of the Internet.

[2] The representation of the human rights angle in the debates about encryption policy must be strengthened. While influential, in practice other considerations such as national security and economic competitiveness tend to be dominant drivers. Increasing the representation of the human rights angle entails:

- More robust cognizance of human rights standards and international norm development;

- Development of safeguards against interferences as well as good practices of state and industry actors as well as users;
- The need for protections against non-legal interference with encryption protocols and implementations (including informal 'backdoors', standard setting, etc.), and the building of trust in the media and communications environment;
- Transparency requirements with respect to the informal non-legal interference with security of media and communications;
- The promotion of transparent software code practices and accountability when deploying technologies with privacy and security guarantees;
- Sensitivity to the role of encryption in regards to violation of the rights of women and girls and other vulnerable groups online, including ethic and racial minorities, and LGBT communities;

[3] All relevant stakeholders should be involved. The issue is not only relevant to government and industry but should also include members of civil society, representatives of vulnerable communities including minorities, women and girls, as well media and educational institutions.

[4] It must be recognized that encryption is not a magic bullet for human rights protection: it needs to be embedded in other support and protections for human rights to be effective.

Stakeholder recommendations

The reflections presented in this study lead to some insights that can be useful for various stakeholders. The following recommendations are options for consideration, designed to properly balance the human rights issues involved with legitimate other considerations like public safety and security. The recommendations target different stakeholder groups (users, service providers, technology experts, lawmakers) and the particular role they play in the overall system.

States to consider:

[5] Restraining from imposing general restrictions on the deployment of encryption by users and relevant service providers;

[6] Including human rights considerations into encryption policies across relevant sectors and ensure that encryption policy is gender-sensitive as well as responsive to the specific needs of protected minorities.

[7] Establishing legal certainty – the lack of legal certainty can especially hamper free and open communication since neither the citizens nor industry players can really assess the risks;

[8] Providing for transparency – Especially informal agreements between government and industry actors can trigger risks for human rights in the area of encryption, since this negatively affects the attribution of acts to governments, which is a precondition to apply human rights most effectively;

[9] Ensuring fact-based (rather than fear-based) policy- making on questions of lawful government access and engage all relevant communities on these questions;

[10] Working towards better international coordination on encryption policy issues;

[11] Stimulating the research and the development of cryptographic innovation and standards for deployment in media and communications landscape;

[12] Developing global monitoring and measurement schemes to evaluate the adoption (and lack thereof) of technologies that protect user communications and information;

[13] Giving consideration to UNESCO's concept of 'Internet Universality and Knowledge', including multi-stakeholder processes to discuss how any limitations on encryption will impact on human rights, openness and accessibility to all on the Internet.

Private sector and Internet intermediaries could consider:

[14] Online intermediaries have not only the role of intermediaries between content providers and users but should also be recognized as "security intermediaries" in various aspects;

[15] Continue to deploy all suitable security measures that help to establish and promote the enjoyment of privacy and freedom of expression by users, including end-to-end encryption of communications and the use of authenticated encryption for data at rest;

[16] Engage internationally and across jurisdictions in ways that promote a race to the top, in terms of the protection enjoyed by users, and not a race to the bottom;

[17] Innovate on the deployment of cryptographic methods to protect users' privacy and freedom of expression;

[18] Support open development of privacy enhancing technologies and human rights oriented encryption projects;

[19] Promote secure coding practices and increase efforts to improve confidentiality and anonymity in services;

[20] Increase efforts of coordination and contributions to standardization to address fragmentation challenges in the software ecosystem.[239]

Users, civil society and the technical community could consider:

Surveys in many countries show the relevance that a significant number of users assign to privacy issues. Consequently, they become frustrated and even hostile when they learn that their trust in the privacy of personal and professional online service has been betrayed. However, the large majority of users may not invest in enhancing privacy by using available means of encryption. Research indicates that this may be better understood as a sign of resignation than a sign that users do not attribute value to their privacy.

239 See Berkman Center 2016 ("Software ecosystems tend to be fragmented. In order for encryption to become both widespread and comprehensive, far more coordination and standardization than currently exists would be required").

The noted discrepancy cannot only be observed in relation to cryptographic technology but to others means of privacy protection as well. In view of this, we recommend the following approach:

[21] Privacy protection should not just rest on the users making use of cryptographic technologies. Communicating the risks and spreading knowledge on the technologies should be a part of a national policy, with sufficient sensitivity of raising awareness among all users including various groups with different vulnerabilities such as journalists, women and girls, minorities, etc. States should be encouraged to make encryption literacy part of their communication as well as media and information literacy programs. Even though these measures might be limited in their effect, they remain an important element of any policy that puts the informed user in the centre.

[22] Developing smart technologies that make encryption as convenient as possible would support privacy and freedom of expression, including special protection measures for journalists, media actors and vulnerable users such as women and girls and minorities. Systems that know when you need a higher level of encryption and automatically react to that demand could be helpful. Users might not want to decide again and again about the security of their communication, but might do it once when opting for a device or a software system.

[23] When interests of the consumers are at stake, it might be effective not just to rely on the individual user but to strengthen the agencies that protect consumer interests.

[24] Privacy policy should target the intermediaries that serve the users in their communications and transactions. If there is effective encryption on this level, even users who do not realize the risks are protected.

[25] There is an important role for education and training, and the more general goal that people should have a realistic idea of the risks that they face without being burdened with impossible requirements to protect oneself against unauthorized access to their content and communications. Actions to this effect can build on research about the reasons for not using encryption.[240]

[26] Gender dimensions and vulnerable communities: women and girls, as well as vulnerable communities, such as journalists, media actors and protected minorities, can be more exposed to interferences with human rights and therefore even more in need of encrypted communications and need particular enhancement on their issues.

[27] The human rights debate can greatly benefit from expertise provided by the technical community. Thus the involvement of technology experts should be welcomed. Technology experts should consider the effects of their decisions on privacy and freedom of communication. These considerations should be reflected in professional ethics and training.

[28] Standard setting community processes on a multi-stakeholder basis aimed at the promotion of human rights in technical standards should be supported and further strengthened. Efforts should be prioritized to rapidly improve protocols known to be insecure.

240 E.g. K. Renaud, M. Volkamer, A. Renkema-Padmos.

References

Harold Abelson et al., Keys Under Doormats: mandating insecurity by requiring government access to all data and communications, July 2015, http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf.

Access and PEN American Center, Comment on Encryption/Anonymity, Submission to UN, 2015.

Bhairav Acharya, The Short-lived Adventure of India's Encryption Policy, December 2015, https://www.ocf.berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption-policy/.

ACLU, Stingray Tracking Devices: Who's Got Them?, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last accessed: 29 August 2016).

Ben Adida et al., CALEA II: Risks of Wiretap Modifications to Endpoints, Center for Democracy & Technology, 17 May 2013, available at https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf (last accessed: 14 September 2016).

Marion Albers, Informationelle Selbstbestimmung, Baden-Baden 2005.

Robert Alexy and Julian Rivers, A Theory of Constitutional Rights, Oxford, 2010.

Apuzzo et al., Apple and Other Tech Companies Tangle With U.S. Over Data Access, New York Times, September 7th, 2015.

Axel Arnbak, *Securing Private Communications: Protecting Private Communications Security in E.U. Law: Fundamental Rights, Functional Value Chains and Market Incentives*, Kluwer Law International, 2016.

Kim Arora, Draft National Encryption Policy put up online for public comment, experts worried, The Times of India, Sept 20th, 2015.

Aydin et al., Turkey v. encryption: An attack on freedom of expression, Access, September 3rd, 2015.

Jack Balkin, Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society, NYU Law Review 79 (2004).

Derek Bambauer, Orwell's Armchair, The University of Chicago Law Review 79 (2012), 3, pp. 863-944.

BBC, MI5 boss warns of technology terror risk, BBC UK, September 17th, 2015.

Cory Bennett and Katie Bo Williams, Paris revives battle over government access to encrypted data, The Hill, November 17th, 2015.

Berkeley Information Privacy Law Association Blog, The Short-lived Adventure of India's Encryption Policy.

Berkman Center, Don't Panic: Making Progress on the "Going Dark" Debate, February 1, 2016.

Daniel Bernstein, Tanja Lange and Ruben Niederhagen, Dual EC: A Standardized Back Door. Cryptology ePrint Archive: Report 2015/767.

BITKOM Survey 08/2014 Cybercrime, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2014/August/140827-BITKOM-Charts-PK-Cybercrime-mit-BKA-28-07-14.pdf.

Thomas Böckenförde, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, pp. 925-939.

Markus Böhm, Messenger Telegram: Lieblings-App der IS-Terroristen sperrt Propagandakanäle, 18th November 2015, http://www.spiegel.de/netzwelt/apps/is-auf-telegram-messenger-app-kuendigt-massnahmen-an-a-1063535.html.

Gabriele Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, pp. 411-414.

Bernard Cazeneuve, French Minister of the Interior, Speech at the Joint Press Conference with Thomas de Maizière, German Minister of the Interior, Paris, 23 August 2016, available at http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe (last accessed 14 September 2016).

Citizen Lab (Munk School of Global Affairs, University of Toronto) and Collin Anderson, The Need for Democratization of Digital Security Solutions to Ensure the Right to Freedom of Expression, Joint Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. David Kay, 10th February 2015, http://www.ohchr.org/Documents/Issues/Opinion/Communications/CitizenLab.pdf.

James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" October 2014, Speech at the Brookings Institution, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

CTITF, Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects, Working Group Compendium (May 2011).

Michael Chertoff and Tobby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance Paper Series: No. 6 (Chatham House, February 2015).

CoE Research Devision, National security and European case-law, CoE / European Court of Human Rights, 2013.

CoE Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Rapporteur: Mr Pieter Omtzigt, Report of 18 March 2015 on Mass Surveillance, Doc. 13288.

Joseph Cox, Apple's iMessage Defense Against Spying Has One Flaw, Wired, 8th September 2015, http://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/.

Ryan Calo, Tech companies may be our best hope for resisting government surveillance, Fusion, September 7th, 2015.

Canes-Wrone, Brandice/Dorf, Michael C., Measuring the chilling effect, NYU Law Review 90 (2015), pp. 1095-1114.

Conner-Simons, CSAIL report: Giving government special access to data poses major security risks, MIT News, Jul 7th, 2015.

Data Security Council of India and NASSCOM, Recommendations for Encryption Policy.

Laura DeNardis, Hidden Levers of Internet Control, Information, Communication & Society, pp. 37-41, 2012.

Claudia Diaz, Omer Tene and Seda Gürses, Hero or Villain: The Data Controller in Privacy Law and Technologies, 74 (2013) Ohio State Law Journal, pp. 923-964.

The Economist, The TSA Locked out, Sept 19th 2015.

EFF, Anonymity and Encryption, Comments submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, February 10, 2015.

EFF, EFF's Encrypt the Web Report, November 2014, https://www.eff.org/encrypt-the-web-report.

EFF. Secure Messaging Scorecard, Version on 3rd November 2015, https://www.eff.org/secure-messaging-scorecard.

ENISA and Europol. On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement. 20 May 2016.

Martin Eifert, Informationelle Selbstbestimmung im Internet. Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, pp. 521-523.

EPIC, Use of encryption and anonymity in digital communications, Submission to UN, Feb 10th, 2015.

EPRS, Science and Technology Options Assessment (STOA), Mass Surveillance, Part 1 - Risks and opportunities raised by the current generation of network services and application, 2014.

EPRS, Science and Technology Options Assessment (STOA), Mass Surveillance, Part 2 – Technology foresight, options for longer term security and privacy improvements, 2014.

European Parliament Resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries', 2014/2232(INI) [Marietje Schaake Rapporteur].

Europol, The Internet Organized Crime Threat Assessment (IOCTA) 2015, 30 September 2015, online version available at https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (last accessed: 14 September 2016).

Ed Felten, On Security Backdoors, Freedom to Tinker, 11th September 2013, https://freedom-to-tinker.com/blog/felten/on-security-backdoors/.

Ed Felten, Software backdoors and the White House NSA panel report, Freedom to Tinker, December 2013, https://freedom-to-tinker.com/blog/felten/software-backdoors-and-the-white-house-nsa-panel-report/.

Kristin Finklea, Dark Web, CRS Report, July 7, 2015.

Jim Finkle, Advanced iOS virus targeting Hong Kong protestors -security firm, Boston, September 2014, http://www.reuters.com/article/hongkong-china-cybersecurity-apple-idUSL2N0RV2D320140930.

FOSS, Cryptography is Important to the Public Interest, 2015.

Tom Fox-Brewster, Facebook opens up to anonymous Tor users with .onion address, The Guardian, 31st October 2014, http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion.

Charles Fried, Privacy, Yale Law Journal 77 (1968), pp. 475-493.

Kevin Gallagher, Why aren't more news organizations protecting their e-mail with STARTTLS encryption?, 24th February 2015, https://freedom.press/blog/2015/02/why-arent-more-news-organizations-protecting-e-mail-with-starttls.

Eric Geller, 'A complete guide to the new 'Crypto Wars'', The Daily Dot, 26 April 2016. Available at http://www.dailydot.com/politics/encryption-crypto-wars-backdoors-timeline-security-privacy/.

Julia Gerhards, (Grund-)Recht auf Verschlüsselung?, Baden-Baden 2010.

Samuel Gibbs, Google can unlock some Android devices remotely, district attorney says, The Guardian, 24th November 2015, http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted.

Andy Greenberg, Cops Don't Need a Crypto Backdoor to Get Into Your iPhone,12th October, 2015, http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/.

Graham Greenleaf, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, 133 *Privacy Laws & Business International Report*, February 2015.

GNI, Submission to the UN, 2015.

Peter Gola & Rudolf Schomerus, Bundesdatenschutzgesetz, 12th edition, Munich 2015.

Dan Goodin, Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations, arsTechnica, 28th October 2015, http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/.

Jennifer Granick, Federal Judge shines a spotlight on the "going dark" debate, The Center for Internet and Society, October 2015, http://cyberlaw.stanford.edu/blog/2015/10/federal-judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate.

Apar Gupta, How many bits are enough? the legality of encryption, November 2011, http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

Seda Gürses and Bart Preneel, Cryptology and Privacy, In: Van Der Sloot, Broeders and Schrijvers (eds.), *Exploring the Boundaries of Big Data*, Netherlands Scientific Council for Government Policy, 2016.

Heninger and Halderman, Tales from the Crypto Community: The NSA Hurt Cybersecurity. Now It Should Come Clean, Foreign Affairs, October 23, 2013.

Ryan Henry, Stacie Pettyjohn and Erin York, Portfolio Assessment of Department of State Internet Freedom Program, RAND National Security Research Division, February 2014, http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1035/RAND_WR1035.pdf.

Matthias Herdegen, Völkerrecht, 14th edition, Munich 2014.

Alex Hern, Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim, The Guardian, July 2015, http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

Joris van Hoboken, Axel Arnbak and Nico Van Eijk, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad, 9th June 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

Thomas Hoeren and Ulrich Sieber, Handbuch Multimedia-Recht, Munich 2012.

Wolfgang Hoffmann-Riem, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, JZ 2008, pp. 1009-1022.

Jeanette Hofmann, Constellations of Trust and Distrust in Internet Governance, in: Report of the Expert Group 'Risks of Eroding Trust - Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT)', European Commission, Brussels, 2015.

Gerrit Hornung, Die Krypto-Debatte: Wlederkehr einer Untoten, MMR 2015, pp. 145-146.

Gerrit Hornung, Ein neues Grundrecht, CR 2008, pp. 299-306.

Human Rights Watch & ACLU, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy (2014).

India Law and Technology Blog, How many bits are enough? The legality of encryption, India Law and Technology Blog, November 2011 http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

India Telecom Laws and Regulations Handbook, 2013. Volume 1.

Indian National Telecom Policy of 1999, http://www.dot.gov.in/telecom-polices/new-telecom-policy-1999.

Indian National Telecom Policy of of 2012, http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final.pdf.

Indian Government Draft Policy, September 2015, http://www.scribd.com/doc/282239916/DRAFT-NATIONAL-ENCRYPTION-POLICY.

Kristina Irion, Government Cloud Computing and National Data Sovereignty, 30th June 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859.

Inserra et al. Encryption and Law Enforcement Special Access: The U.S. Should Err on the Side of Stronger Encryption, Heritage Foundation, 2015.

International Journal of Computer Application, Legal Issues Involving Cryptography In India.

Internet Architecture Board (IAB), Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement, August 2015, http://tools.ietf.org/html/rfc7624.

Sarah Joseph and Melissa Castan, The International Convention on Civil and Political Rights, third Edition, Oxford, 2013.

David Kaye, Phone Encryption: Balancing Privacy and Protection, Letter to the Editor, NYTimes, August 21st, 2015.

David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, May 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

Eric King and Matthew Rice, Behind the curve: When will the UK stop pretending IMSI catchers don't exist?, November 2014, https://www.privacyinternational.org/node/454.

Nadim Kobeissi, On Encryption and Terrorists, November 23rd, 2015.

Neal Koblitz and Alfred Menezes, A Riddle wrapped in an Enigma, December 2015, http://eprint.iacr.org/2015/1018.pdf.

Alexander Koch, Grundrecht auf Verschlüsselung?, CR 1997, pp. 106-110.

Eitan Konigsburg, Embracing HTTPS, November 2014, http://open.blogs.nytimes.com/2014/11/13/embracing-https/.

Bert-Jaap Koops, Crypto Law Survey - Overview per country - Version 27.0, February 2013.

Joshua Kopstein, FBI Chief Asks Tech Companies to Stop Offering End-to-End Encryption, 9th December 2015, http://motherboard.vice.com/read/fbi-chief-asks-tech-companies-to-stop-offering-end-to-end-encryption.

Christopher Kuner, 2013.

Christopher Kuner, We actually lost the crypto wars, LSE Media Policy Project, 12th November 2014, http://blogs.lse.ac.uk/mediapolicyproject/2014/11/12/we-actually-lost-the-crypto-wars/.

Micah Lee, Apple still has plenty of your data for the feds, The Intercept, 22nd September 2014, https://theintercept.com/2014/09/22/apple-data/.

Julian von Lucius, GMail ist ein Telekommunikationsdienst im Sinne des TKG, 11th December 2015, http://www.noerr.com/de/presse-publikationen/News/gmail-ist-ein-telekommunikationsdienst-im-sinne-des-tkg.aspx.

Jonathan Mahler, Who Spewed That Abuse? Anonymous Yik Yak App Isn't Telling, N. Y. Times, March 8, 2015.

Rebecca Mackinnon et al., Fostering Freedom Online: The Role of Internet Intermediaries, UNESCO/Internet Society, 2014.

McConnell, Chertoff, et al., Why the fear over ubiquitous data encryption is overblown, Opinion, WaPo, Jul 28th, 2015.

Kieran MacCarthy, Dutch govt says no to backdoors, slides $540k into OpenSSL without breaking eye contact, The Register, January 4, 2016.

Dominic McGoldrick, The Human Rights Committee, Clarendon Press, 1994.

Tarlach McGonagle and Yvonne Donders, The United Nations and Freedom of Expression and Information, Cambridge University Press, 2015.

McSweeney, Worried About Your Data Security? How Encryption Can Help Protect Your Personal Information, Huff Post, September 3, 2015.

Amir Mizroch, Surveillance and Silicon Valley Are 'Destroying' Europe's Privacy Balance. 11th December 2015. http://blogs.wsj.com/digits/2015/12/11/surveillance-silicon-valley-destroying-europes-privacy-balance.

Peter Münch, Technisch-organisatorischer Datenschutz, 4. edition, Frechen 2010.

Ellen Nakashima, FBI chief: Terrorist group turning to encrypted communications, WaPo, July 8th, 2015.

Ellen Nakashima, Obama faces growing momentum to support widespread encryption, WaPo September 16th, 2015.

Michael Nelson, Clinton, clipper and crypto, The Hill, September 10, 2015.

Helen Nissenbaum, 'Where computer security meets national security', *Ethics and Information Technology*, (2005) 7, pp, 61-73.

Manfred Nowak, CCPR Commentary, 2nd edition, 2005.

NSC draft options paper on strategic approaches to encryption, Summer 2015, http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/.

OECD, Cryptography Policy, The Guidelines and the Issues, 1998.

A. Parvathy, Ravi Shankar Choudhary and Vrijendra Singh, Legal Issues Involving Cryptography in India, April 2013, International Journal of Computer Application, Issue 3, Volume 2, http://rspublication.com/ijca/april13/6.pdf.

Andrea Peterson, Washington Post starts to automatically encrypt part of Web site for visitors, WaPo, Jun 30th, 2015.

Andreas Pfitzmann, Datenschutz durch Technik, DuD 1999, pp. 405-408.

Andreas Pfitzmann and Marit Hansen, 'Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology', Version v0.25, December 6th, 2005.

Jörg Pohle, Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens, FlfF-Kommunikation 2/15, pp. 41-44.

Isabelle de Pommereau, In Snowden's wake, crypto-startups take root in Germany, CS Monitor, 3th August 2015, http://www.csmonitor.com/World/Passcode/2015/0803/In-Snowden-s-wake-crypto-startups-take-root-in-Germany.

Privacy International, Article 19 & IHRC, Securing Safe Spaces Online, 2015.

Privacy International, Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications, February 2015.

Public Intelligence, India Draft National Encryption Policy, September 2015.

Nandagopal Rajan, Encryption Policy: WhatsApp, web services out of draft encryption policy after outcry, September 2015, http://indianexpress.com/article/technology/tech-news-technology/draft-national-encryption-policy-you-might-need-to-store-whatsapp-messages-for-90-days/.

OECD, OECD Guidelines for Cryptography Policy, 27 March 1997.

P. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill: University of North Carolina Press, 1995.

Philipp Rogaway, The Moral Character of Cryptographic Work, University of California, December 2015.

Sasha Romanosky, Martin C. Libicki, Zev Winkelman, Olesya Tkacheva, Internet Freedom Software and Illicit Activity, Supporting Human Rights Without Enabling Criminals, Rand Corporation, 2015.

Philipp Roos, Das IT-Sicherheitsgesetz, MMR 2015, pp. 636-645.

Alexander Roßnagel, Das De-Mail-Gesetz, NJW 2011, pp. 1473-1478.

Alexander Roßnagel, Schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Deutscher Bundestag, Innenausschuss, Ausschussdrucksache 18(4)(284)B.

Ira Rubinstein and Joris van Hoboken, Privacy and Security in the Cloud, Maine Law Review 2014, pp. 488-533.

Ira Rubinstein and Michael Hintze, Export Controls on Encryption Software, http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm.

Fabian Scherschel, Keeping Tabs on WhatsApp's Encryption, c't, 30th April 2015, http://m.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html.

Stephanie Schiedermair, Der Schutz des Privaten als internationales Grundrecht, Tübingen, 2012.

Bruce Schneier, How We Sold Our Souls - and More - to the Internet Giants, May 2015, https://www.schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html.

Sebastian Schulz, Privacy by Design, CR 2012, pp. 204-208.

Spiros Simitis, Bundesdatenschutzgesetz, 8th edition, Baden-Baden 2014.

Chris Soghoian, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era. 8 J. on Telecomm. and High Tech. Law 359 (2009).

Oliver Stiemerling and Jürgen Hartung, Datenschutz und Verschlüsselung, CR 2012, pp. 60-68.

Thomas Stögmüller, Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen, CR 2008, pp. 435-439.

Peter Swire, Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy", 8th July 2015.

Peter Swire, Encryption and Globalization, Columbia Science and Technology Law Review, Vol. 23, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602.

Jürgen Taeger and Detlev Gabel, BDSG und Datenschutzvorschriften des TKG und TMG, 2nd edition, Nordstrand 2013.

Paul Taylor, Security that makes spies feel insecure, Financial Times, 2nd August 2010, http://www.ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a.html#axzz3R5nCIW6I.

Telecom Regulatory Authority Of India, Recommendations on Application Services.

Telecom Regulatory Authority Of India, TRAI Consultation paper on Mobile Financial Services.

The Indian Express, Needed clear, robust encryption policy – without a backdoor.

The Internet Association, Statement on Encryption, November 23rd 2013.

The Reserve Bank of India, Report of the Working Group on Electronic Banking.

The Reserve Bank of India, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds.

Thomas et al., May seeks backing for surveillance laws, Sept 16th, 2015, Financial Times.

UCI Law International Justice Clinic, Selected References: Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression, 2015.

UNESCO, Keystones to foster inclusive Knowledge Societies, Paris 2015, http://unesdoc.unesco.org/images/0023/002325/232563E.pdf.

UN Counter-Terrorism Implementation Task Force (CTITF), Countering the Use of the Internet for Terrorist Purposes, CTITF Working Group Report (February 2009).

US Department of Commerce (Bureau of Industry and Society) In, Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility.

Vance et al., When Phone Encryption Blocks Justice, NYTImes, Opion Pages, August 11th, 2015.

Andreas Voßhoff and Peter Büttgen, Verschlüsselung tut Not, ZRP 2014, pp. 232-235.

W3C, EndtoEnd Encryption and the Web, W3C TAG Finding 16 July 2015.

Ben Wagner, After the Arab spring: New paths for human rights and the Internet in European Foreign Policy, European Parliament, Directorate-General for External Policies, Policy Department, 2012.

Jane Wakefield, How does IS communicate securely?, BBC News, Technology, 17 November 2015.

Fabian Warislohner, Tatort: Verschlüsselung. Die Schuldfrage nach Paris, 19th November 2015, https://netzpolitik.org/2015/tatort-verschluesselungstechnik-die-schuldfrage-nach-paris.

Nicholas Weaver, We think encryption allows terrorists to hide. It doesn't, December 2015, https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think-encryption-allows-terrorists-to-hide-it-doesnt.

Daniel Weitzner, 'Encryption solution in wake of Paris should come from Washington not Silicon Valley', Washington Post, November 24th, 2015.

WhatsApp, WhatsApp Encryption Overview, Technical White Paper, April 4th, 2016.

Tom Whitehead, Internet firms to be banned from offering unbreakable encryption under new laws, The Telegraph, November 2nd, 2015.

White House, National Security Council, Review of Strategic Approaches to Encryption, Leaked Draft Memo, September 2015, available through WaPo.

Zack Whittaker, Kazakhstan will force its citizens to install Internet backdoors, ZDNet, December 3, 2015.

SE Wilborn, Revisiting the Public/Private Distinction, Georgia Law Review 32 (1998), pp. 825-858.

Wilson Center Symposium, How Have We Changed? Evolving Views in the U.S. on Security and Liberty. Remarks of Bob Litt, https://www.youtube.com/watch?list=PLzM1iiQhVrdHHZPSZ1z_ztTrUuRPMUtRb&v=PWj8eqKKB64.

Wittes, Thoughts on Encryption and Going Dark: Part I, Lawfare, July 9, 2015.

Wittes, Thoughts on Encryption and Going Dark: Part II, Lawfare, July 12, 2015.

World Wide Web Foundation et al., Freedom of Expression, Encryption, and Anonymity: Civil Society and Private Sector Perceptions, 2015.

Yulong Zou, Xianbin Wang and Lajos Hanzo, A survey on wireless security: technical challenges, recent advances and future trends, Proceedings of the IEEE, May 2015, http://arxiv.org/pdf/1505.07919.pdf.

Appendix 1: UNESCO Connecting the Dots Outcome Document

Outcome document

The "CONNECTing the Dots: Options for Future Action" Conference held at UNESCO Headquarters 3-4 March 2015,

Noted the potential of the Internet to advance human progress towards inclusive Knowledge Societies, and the important role of UNESCO in fostering this development within the wider ecosystem of actors,

Affirmed the human rights principles that underpin UNESCO's approach to Internet-related issues, specifically that the same rights that people have offline must be protected online as per Human Rights Council resolution A/HRC/RES/26/13;

Recalled Resolution 52 of the 37th session of the General Conference, which mandated a consultative multi-stakeholder study with options for consideration of Member States, to be reported to the 38th General Conference within the framework of UNESCO's work on the World Summit on the Information Society,

Further recalled the establishment of principles in guiding documents that include the article 12 and 19 of the Universal Declaration of Human Rights, and article 17 and 19 in the International Covenant on Civil and Political Rights;

And, having *reviewed* the draft of the UNESCO consultative study,

Commend continued work on the related options below, and look forward to UNESCO Member States deliberations on them:

1. Overarching options for UNESCO

   1.1 Considering the Final Statement of the first WSIS+10 conference, endorsed by the 37th General Conference, affirm the on-going value of the World Summit on the Information Society (WSIS) outcomes, including the Internet Governance Forum (IGF), for the post-2015 development agenda, Internet governance issues, and the role and work of UNESCO;

   1.2 Affirm that the fundamental human rights to freedom of opinion and expression, and its corollary of press freedom and the right of access to information, and the right to peaceful assembly, and the right to privacy, are enablers of the post-2015 development agenda;

   1.3 Also affirm that increasing access to information and knowledge across society, assisted by the availability of information and communication

technologies (ICTs), supports sustainable development and improves people's lives;

1.4 Promote the alignment of Internet-related laws, policies and protocols with international human rights law;

1.5 Support the Internet Universality principles (R.O.A.M) that promote a Human Rights-based, Open Internet is Accessible to all and characterized by Multi-stakeholder participation;

1.6 Strengthen the cross-cutting role of the Internet in all of UNESCO programmatic activities, including Priority Africa, Priority Gender Equality, support to Small Islands Developing States and Least Developed Countries, as well as in UNESCO's leadership of the International Decade for the Rapprochement of Cultures.

2. Options for UNESCO related to the field of Access to Information and Knowledge:

2.1 Foster universal, open, affordable and unfettered access to information and knowledge, and narrowing the digital divide, including the gender gap, and encourage open standards, raise awareness and monitor progress;

2.2 Advocate for ICT policies that enhance access guided by governance principles that ensure openness, transparency, accountability, multilingualism, inclusiveness, gender equality, and civil participation including for youth, persons with disabilities, marginalized and vulnerable groups;

2.3 Support innovative approaches to facilitate citizen involvement in the development, implementation and monitoring of the Sustainable Development Goals, as agreed at the UN General Assembly;

2.4 Promote universal access to information and knowledge and ICTs by encouraging the creation of public access facilities, and by supporting users of all types to develop their capabilities to use the Internet as creators and users of information and knowledge;

2.5 Reaffirm the important contribution provided by open access to scholarly, scientific and journalistic information, open government data, and free and open source software, towards the building of open knowledge resources;

2.6 Explore the potential of the Internet for cultural diversity.

3. Options for UNESCO related to the field of Freedom of Expression

3.1 Urge Member States and other actors to protect, promote and implement international human rights law on free expression and the free flow of information and ideas on the Internet;

3.2 Reaffirm that freedom of expression applies, and should be respected, online and offline in accordance with Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) that any limitation on freedom of information must comply with international human rights law as outlined by Article 19(3) of the International Covenant on Civil and Political Rights;

3.3 Support safety for journalists, media workers, and social media producers who generate a significant amount of journalism, and reaffirm the importance of the rule of law to combat impunity in cases of attacks on freedom of expression and journalism on or off the Internet;

3.4 Noting the relevance to the Internet and digital communications of the international Convention on the Rights of Persons with Disabilities (CRPD), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and the work of the Office of the High Commissioner on Human Rights, concerning the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (Rabat Plan of Action 2012), promote educational and social mechanisms for combating online hate speech, without using this to restrict freedom of expression;

3.5 Continue dialogue on the important role that Internet intermediaries have in promoting and protecting freedom of expression;

4. Options for UNESCO related to Privacy

4.1 Support research to assess the impacts on privacy of digital interception, collection, storage and use of data, as well as other emerging trends;

4.2 Reaffirm that the right to privacy applies and should be respected online and offline in accordance with Article 12 of the UDHR and Article 17 of the ICCPR and support as relevant within UNESCO's mandate, the efforts related to UN General Assembly Resolution A/RES/69/166 on the Right to Privacy in the Digital Age;

4.3 Support best practices and efforts made by Member States and other stakeholders to address security and privacy concerns on the Internet in accordance with their international human rights obligations and consider in this respect the key role played by actors in the private sector;

4.4 Recognise the role that anonymity and encryption can play as enablers of privacy protection and freedom of expression, and facilitate dialogue on these issues.

4.5 Share best practices in approaches to collecting personal information that is legitimate, necessary and proportionate, and that minimizes personal identifiers in data;

4.6 Support initiatives that promote peoples' awareness of the right to privacy online and the understanding of the evolving ways in which governments and commercial enterprises collect, use, store and share information, as well as the ways in which digital security tools can be used to protect users' privacy rights;

4.7 Support efforts to protect personal data which provide users with security, respect for their rights, and redress mechanisms, and which strengthen trust in new digital services.

5. Options for UNESCO related to Ethical dimension of the Information Society

    5.1 Promote human rights-based ethical reflection, research and public dialogue on the implications of new and emerging technologies and their potential societal impacts;

    5.2 Incorporate, as a core component in educational content and resources, including life-long learning programmes, that support the understanding and practice of human rights-based ethical reflection and its role in both online and offline life;

    5.3 Enable girls and women take full advantage of the potential of the Internet for gender equality through taking proactive measures to remove barriers, both online and offline, and promoting their equal participation;

    5.4 Support policy makers in enhancing their capacity to address the human right-based ethical aspects of inclusive knowledge societies by providing relevant training and resources;

    5.5 In recognition of the trans-boundary nature of the Internet, promote global citizenship education, regional and international cooperation, capacity-building, research, the exchange of best practices and development of a broad understanding and capabilities to respond to its ethical challenges.

6. Options for UNESCO related to cross-cutting issues:

    6.1 Promote the integration of UNESCO's expertise on Media and Information Literacy (MIL) into formal and informal education systems, in recognition of the important roles that digital literacy and facilitating universal access to information on the Internet, play in the promotion of the right to education, as enumerated in Human Rights Council, Resolution 26/13;

    6.2 Recognize the need for enhanced protection of the confidentiality of sources of journalism in the digital age;

    6.3 Support Member States as requested in the harmonization of relevant domestic laws, policies and practices with international human rights law;

    6.4 Support transparency and public participation in the development and implementation of policies and practices amongst all actors in the information society.

    6.5 Promote research into law, policy, regulatory frameworks and the use of the Internet, including relevant indicators in the key areas of the study.

    6.6 Promote UNESCO's participation in discussions on Network Neutrality as relevant to the fields of access to information and knowledge and freedom of expression.

7. Options related to UNESCO role

    7.1 Reinforce UNESCO's contributions and leadership within the UN system, including continued implementation of the WSIS outcomes, the WSIS+10 review, the IGF and the post-2015 development agenda;

7.2 Engage as relevant with partners outside of the UN system, such as individual governments, civil society, news media, academia, private sector, technical community and individual users; including by providing expert advice, sharing of experience, creating fora for dialogue, and fostering development and empowerment of users to develop their capacities;

7.3 Support Member States in ensuring that Internet policy and regulation involves the participation of all stakeholders, and integrates international human rights and gender equality.

Appendix 2: UNESCO Concept paper on Internet Universality

Internet Universality: A Means Towards Building Knowledge Societies and the Post-2015 Sustainable Development Agenda

2 September 2013

Abstract

UNESCO's Communication and Information Sector is canvassing a new concept of "Internet Universality", which could serve to highlight, holistically, the continued conditions for progress towards the Knowledge Society and the elaboration of the Post-2015 Sustainable Development Agenda. The concept includes, but also goes beyond, universal access to the Internet, mobile and ICTs. The word "Universality" points to four fundamental norms that have been embodied in the broad evolution of the Internet to date, and which provide a comprehensive way to understand how multiple different aspects are part of a wider whole. For the Internet to fulfill its historic potential, it needs to achieve fully-fledged "Universality" based upon the strength and interdependence of the following: (i) the norm that the Internet is Human Rights-based (which in this paper is the substantive meaning of a "free Internet"), (ii) the norm that it is "Open", (iii) the norm that highlights "Accessible to All", and (iv) the norm that it is nurtured by Multi-takeholder Participation. The four norms can be summarized by the mnemonic R – O – A – M (Rights, Openness, Accessibility, Multi-stakeholder). The "Internet Universality" concept has very specific value for UNESCO in particular. By building on UNESCO's existing positions on the Internet, the concept of "Internet Universality" can help frame much of UNESCO's Internet-related work in Education, Culture, Natural and Social Sciences and Communication-Information for the strategic period of 2014-2021. As regards global debates on Internet governance, the "Internet Universality" concept can help UNESCO facilitate international multi-stakeholder cooperation, and it can also help to highlight what the Organization can bring to the Post-2015 Sustainable Development Agenda.

By: Division of Freedom of Expression and Media Development

Communication and Information Sector[241]

* An integral version of this paper in all UN offcial languages is online at:

http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/internet-universality/

241 Incorporating insights from UNESCO Inter-sectoral and external consultations. We also thank Ms Constance Bommelaer for her contribution to the development of the concept.

Summary version (4 pages)

1. Why a concept of "Internet Universality"?

UNESCO has long recognized that the Internet has enormous potential to bring the world closer to peace, sustainable development and the eradication of poverty.[242] As an international intergovernmental organization that operates with a global remit and promotes values that are universal, UNESCO has a logical connection to the Internet's "universality". This "universality" can be understood as the common thread that runs through four key social dimensions pertaining to the Internet, namely the extent to which this facility is based on universal norms of being: (i) Human Rights-based (and therefore free); (ii) Open; (iii) Accessible to All; and (iv) Multi-stakeholder Participation. The four norms can be summarized by the mnemonic R – O – A – M (Rights, Openness, Accessibility, Multi-stakeholder).

Various stakeholders have characterized the Internet according to what they perceive as its essential features, highlighting one or other aspects such as freedom of expression, open architecture, security issues, online ethics, etc.[243] What this range of conceptualisations illustrates is both the diversity of concerns and interests, as well as the multi-faceted character of the Internet itself. In turn, this prompts the question as to the possibility of understanding how the various considerations and dimensions relate to each other and to the wider whole. As a method to conceptualize this bigger picture, UNESCO is now canvassing the concept of "Internet Universality", which could serve as a macro-concept. The purpose is to capture the enduring essentials of the vast, complex and evolving Internet, and which facilitates a comprehensive understanding of where and how different parties, and especially UNESCO, relate to the Internet. The concept could particularly serve as an enabling perspective in the context of the increasing centrality of Internet to societies, and specifically the increasing "Internetization" of education, the sciences, culture and communication-information.

As well as identifying four distinctive norms that have special interest to UNESCO, the concept of "Internet Universality" groups these under a single integrated heading in a way that affords recognition of their mutually reinforcing and interdependent character. Without such a comprehensive intellectual device, it would otherwise be hard to grasp interconnections amongst UNESCO's Internet-related work and how it contributes to Knowledge Societies and the Post-2015 Sustainable Development Agenda.

As regards UNESCO's involvement in global debates, the concept of "Internet Universality" can be considered for its potential as a unifying, consolidated and comprehensive framework. On the one hand, it highlights the freedom and human rights principles as shared by those existing notions such as "Internet freedom"; on the other hand, it also provides an umbrella to address the intertwined issues of access and use, as well as the

242 For example: "Reflection and Analysis by UNESCO on the Internet: UNESCO and the use of Internet in its domains of competence" (2011). http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ED/ICT/pdf/useinternetdomains.pdf.

243 For example, there have been different emphases at the Stockholm Forum, the Freedom Online Coalition on Cyberspace, Wilton Park, and the London and Budapest conferences on Cyberspace. Similarly, the Internet has been analyzed diversely by international organisations. Examples here are: the Council of Europe's "Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet" (2011), the OECD Council Recommendation on Principles for Internet Policy Making (2011), the OSCE Representative on Freedom of the Media Recommendations from the Internet 2013 Conference (2013); the ICC Policy Statement on "The freedom of expression and the free flow of information on the Internet", and the Internet Rights and Principles Coalition's "Internet Rights & Principles Charter" (2010).

matters of technical and economic openness. In addition, the concept also encompasses multi-stakeholder engagement as an integral component. In this inclusive way, the "Internet Universality" concept can therefore be a bridging and foresighted framework for dialogue between North and South and among different stakeholders. As such, it could also make a unique contribution to shaping global Internet governance discourse and the post-2015 Sustainable Development Agenda.

2. Unpacking the concept of "Internet Universality"

The linking of four normative components of the "universality" of the Internet builds closely upon prior UNESCO thinking about the Internet which includes:

- *Recommendation on the Promotion and Use of Multilingualism and Universal Access to Cyberspace* (2003).[244] (This document particularly points to the accessibility norm, as well as the need to balance rights).
- *Reflection and Analysis by UNESCO on the Internet* (2011).[245] (This document highlights normative work in relation to UNESCO's programmes, and multi-stakeholder participation).
- *Final Recommendations of WSIS+10 review event*, and the *Final Statement of the WSIS+10 review event* (2013).[246] (These cover rights, access, openness, and multi-stakeholder issues).
- *UNGIS (UN Group on the Information Society) Joint Statement on the Post-2015 Sustainable Development Agenda* (2013).[247] (This document highlights the importance of the social conditions for Information and Communication Technologies in general, and the Internet in particular, to contribute to inclusive Knowledge Societies).

"Internet Universality" integrates a range of existing UNESCO insights and shows the link between the Internet and what UNESCO has already recognised[248] as the underlying key principles of Knowledge Societies: freedom of expression, quality education for all, universal access to information and knowledge, and respect for cultural and linguistic diversity. In this way, the concept highlights what is needed for the Internet to be a means towards achieving Knowledge Societies. It serves as a heuristic to highlight that the Internet's character and utility entail technical, social, legal, economic and other arrangements which in turn depend on particular norms that underpin the positive potentiality of this facility. Considered in more depth, the R – O – A – M norms constitutive of "Internet Universality" (Rights, Openness, Accessibility, Multi-stakeholder) can be understood as follows:

(i) By identifying the Internet's connection to Human Rights-based norms as constituents of freedom, "Internet Universality" helps to emphasize continued harmony between

244 http://www.unesco.org/new/en/communication-and-information/about-us/how-we-work/strategy-and-programme/promotion-and-use-of-multilingualism-and-universal-access-to-cyberspace/.

245 http://unesdoc.unesco.org/images/0019/001920/192096e.pdf;

246 Documents from the First WSIS+10 Review Event, "Towards Knowledge Societies for Peace and Sustainable Development", Paris 25-27 February, 2013: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_recommendations_en.pdf; http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf

247 http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/ungis_joint_statement_wsis_2013.pdf.

248 *Reflection and Analysis by UNESCO on the Internet,* http://unesdoc.unesco.org/.images/0019/001920/192096e.pdf.

the growth and use of the Internet and human rights. A free Internet in this sense means one that respects and enables the freedom to exercise human rights.[249] In this regard, "Internet Universality" enjoins us to consider the gamut of interdependencies and inter-relationships between different human rights and the Internet – such as freedom of expression, privacy, cultural participation, gender equality, association, security, education, etc.

(ii) "Internet Universality" also highlights the norm of the Internet being Open. This designation recognizes the importance of technological issues such as open standards, as well as standards of open access to knowledge and information. Openness also signals the importance of ease of entry of actors and the absence of closure that might otherwise be imposed through monopolies.

(iii) Accessible to All as a norm for "Internet Universality" raises issues of technical access and availability, as well as digital divides such as based on economic income and urban-rural inequalities. Thus it points to the importance of norms around universal access to minimum levels of connectivity infrastructure. At the same time, "accessibility" requires engaging with social exclusions from the Internet based on factors such as literacy, language, class, gender, and disability. Further, understanding that people access the Internet as producers of content, code and applications, and not just as consumers of information and services, the issue of user competencies is part of the accessibility dimension of "Universality". This highlights UNESCO's notion of Media and Information Literacy which enhances accessibility by empowering Internet users to engage critically, competently and ethically.

(iv) The Internet in this sense cannot only be seen from the "supply side", but needs a complimentary "user-centric" perspective. The Participatory, and specifically the Multi-stakeholder engagement, dimension of "Internet Universality" facilitates sense-making of the roles that different agents (representing different sectors as well as different social and economic status, and not excluding women and girls) have played, and need to continue to play, in developing and governing the Internet on a range of levels. Participation is essential to the value that the facility can have for peace, sustainable development and poverty eradication. In bridging contesting stakeholder interests, participative mechanisms contribute to shared norms that mitigate abuses of the Internet. "Universality" here highlights shared governance of the Internet.

These norms for these four aspects are distinct, but they also reinforce each other. Rights without accessibility would be limited to the few; accessibility without rights would stunt the potential of access. Openness allows for sharing and innovation, and it complements respect for rights and accessibility. Multi-stakeholder participation helps guarantee the other three norms. Overall, an Internet that falls short of respecting human rights, openness, accessibility or multi-stakeholder participation would by definition be far less than universal.

3. How the concept of "Internet Universality" is relevant to UNESCO

UNESCO has a unique role in promoting "Internet Universality". It is the UN agency with a mandate that spans social life at large and, within this, has programs that involve the

249 In this manner, "Internet Universality" accords with the Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and also echoes the first resolution on "promotion, protection and enjoyment of human rights on the Internet" passed by UN Human Rights Council in 2012.

Internet in education, culture, science, social sciences and communication-information. By using "Internet Universality" as an umbrella concept, UNESCO can position more specific concerns such as mobile learning, education for girls, cultural and linguistic diversity, media and information literacy, research into climate change, freedom of expression, universal access to information, bioethics and social inclusion, etc. In this way, "Internet Universality" can also support the priorities of Gender Equality and Africa. It can serve as an over-arching, integrating framework for Internet-related work across UNESCO, establishing a common frame of reference for all. Operationally the concept can elevate a range of work to the status of initiatives that jointly advance "Internet Universality". It can encourage synergies and inter-sectoral co-operation and joint programming. In particular, the concept can enhance understanding of the mid-term strategy of 2014-2021 (37/C4) and the quadrennial program (37/C5).

4. Conclusion

"Internet Universality" accords with the Organization's service to the wider international community in the following respects:

- Laboratory of ideas, including foresight – elaborating the concept is directly relevant to UNESCO's creative and think-tank potential;
- By stimulating global debate, "Internet Universality" illustrates how UNESCO can be a catalyst for international cooperation, with a holistic and inclusive approach.
- Standard-setter – if the concept gained traction broadly, it could inform the development of standards for monitoring progress in "Internet Universality"
- As a normative framework that can inform policies, and draw in public and private, civil society and decision-makers, "Internet Universality" can help UNESCO fulfill its role as a capacity-builder in Member States.

Looking ahead, "Internet Universality" could follow in the footsteps of previous influential intellectual work by UNESCO such as the concepts of "Intangible cultural heritage" and "Knowledge Societies". Because "Internet Universality" represents an updated conceptualization of the era, the concept could become a valuable contribution to the global discussion about this complex and dynamic human creation and serve to enhance Internet's continued contribution to humanity's shared future.

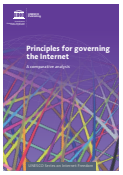
UNESCO Series on Internet Freedom

UNESCO has started in 2009 to commission this flagship series publications of Internet Freedom, aiming to explore the changing legal and policy issues of Internet and provide its Member States and other stakeholders with policy recommendations aiming to foster a conducive environment to freedom of expression on the net.

This is the 8th edition of the series, with previous editions presented as below:

Privacy, free expression and transparency: redefining their new boundaries in the digital age

This study analyzes the interactions between the right to freedom of expression, the right to privacy and the value of transparency in the Internet environment. It covers the legal frameworks and current mechanisms for balancing rights, and presents specific issues, cases and trends. The interplays between multiple players – State actors, Internet users, ICT companies, civil society organizations, the judiciary, security services –are envisaged and recommendations for stakeholders are provided.



Principles for governing the Internet

As the sixth edition in the UNESCO Internet Freedom series, this study encompasses both quantitative and qualitative assessments of more than 50 declarations, guidelines, and frameworks. The issues contained in these documents are assessed in the context of UNESCO's interested areas such as access, freedom of expression, privacy, ethics, Priority Gender Equality, and Priority Africa, and sustainable development, etc.

Countering Online Hate Speech

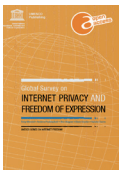
The study provides a global overview of the dynamics characterizing hate speech online and some of the measures that have been adopted to counteract and mitigate it, highlighting good practices that have emerged at the local and global levels. The publication offers a comprehensive analysis of the international, regional and national normative frameworks, with a particular emphasis on social and non-regulatory mechanisms that can help to counter the production, dissemination and impact of hateful messages online.

Building digital safety for journalism: A survey of selected issues

As technologies develop, so do opportunities as well as threats to journalism. This research explains some of the emerging threats to journalism safety in the digital era, and proposes a framework to help build digital safety for journalists. Examining 12 key digital threats to journalism, ranging from hacking of journalistic communications, through to denial-of service attacks on media websites, it assesses preventive, protective and pre-emptive measures to avoid them. It shows too that digital security for journalism encompasses, but also goes beyond, the technical dimension.

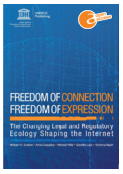
Fostering freedom online: the role of internet intermediaries

With the rise of Internet intermediaries that play a mediating role between authors of content and audiences on the internet, this UNESCO publication provides in-depth case studies and analysis on how internet intermediaries impact on freedom of expression and associated fundamental rights such as privacy. It also offers policy recommendations on how intermediaries and states can improve respect for internet users' right to freedom of expression.



Global survey on internet privacy and freedom of expression

This publication seeks to identify the relationship between freedom of expression and Internet privacy, assessing where they support or compete with each other in different circumstances. The book maps out the issues in the current regulatory landscape of Internet privacy from the viewpoint of freedom of expression. It provides an overview of legal protection, self-regulatory guidelines, normative challenges, and case studies relating to the topic. .



Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet

This report provides a new perspective on the social and political dynamics behind the threats to expression. It develops a conceptual framework on the 'ecology of freedom of expression' for discussing the broad context of policy and practice that should be taken into consideration in discussions of this issue.

All publications can be downloaded at:
http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/

Human Rights and Encryption

This publication follows UNESCO's new approach to Internet issues, as endorsed in November 2015 on the occasion of its 38th General Conference. Our 195 Member States have adopted the CONNECTing the Dots Outcome Document, in which 38 options for future action from UNESCO are set out; and the Internet Universality principles (R.O.A.M.), which advocates for a Human-rights-based, Open and Accessible Internet, governed by Multi-stakeholder participation.

Encryption is a hot topic in the current global discussion on Internet governance. This research delves into the subject, to outline a global overview of the various means of encryption, their availability and their potential applications in the media and communications landscape. The research explains how the deployment of encryption is affected by different areas of law and policy, and it offers detailed case studies of encryption in selected jurisdictions.

It analyzes in-depth the role of encryption in the media and communications landscape, and the impact on different services, entities and end users. Built on this exploration and analysis, the research provides recommendations on encryption policy that are useful for various stakeholders. These include signaling the need to counter the lack of gender sensitivity in the current debate, and also highlighting ideas for enhancing "encryption literacy".

United Nations
Educational, Scientific and
Cultural Organization

Communication and
Information Sector

9 789231 001857