Values and Networks – Steps Toward Exploring their Relationships

Carsten Orwat
Karlsruhe Institute of Technology (KIT)
Institute for Technology Assessment and Systems Analysis (ITAS), Germany
orwat@kit.edu

Roland Bless
Karlsruhe Institute of Technology (KIT)
Institute of Telematics (TM)
Germany
bless@kit.edu

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

Many technical systems of the Information and Communication Technology (ICT) sector enable, structure and/or constrain social interactions. Thereby, they influence or implement certain values, including human rights, and affect or raise conflicts among values. The ongoing developments toward an "Internet of everything" is likely to lead to further value conflicts. This trend illustrates that a better understanding of the relationships between social values and networks is urgently needed because it is largely unknown what values lie behind protocols, design principles, or technical and organizational options of the Internet. This paper focuses on the complex steps of realizing human rights in Internet architectures and protocols as well as in Internet-based products and services. Besides direct implementation of values in Internet protocols, there are several other options that can indirectly contribute to realizing human rights via political processes and market choices. Eventually, a better understanding of what values can be realized by networks in general, what technical measures may affect certain values, and where complementary institutional developments are needed may lead toward a methodology for considering technical and institutional systems together.

Keywords

Values, Human Rights, Network Design, Communication Protocols, Rules, Institutions, Governance

1. INTRODUCTION

Currently, initiatives within the *Internet Research Task Force (IRTF)* or the *Values-in-Design Council on Future Internet Architectures* strive to make the future Internet match social values better. For the Internet as a global communication infrastructure, the relevant catalog of social values are *human rights* [1, 21]. They are the only globally effective catalog of normative criteria of fundamental legal rights and moral values. To a certain extent, the Internet and its protocols have already facilitated the realization of human rights, e.g., the freedom of assembly and expression. In contrast, measures of censorship and pervasive surveillance violate fundamental human rights [31, 32].

One of our research objectives is to investigate and reveal the relationships between design principles used in communication networks and human rights (we also note that not every human right is applicable to networks). If we better understand these relationships, the development of technical standards and protocols for the future Internet can probably take designs into account that enforce human rights or certain values and may even inhibit their violation. From a technical perspective, new technologies may imply new design options and also different implications for values. For instance, the current Internet architecture has different implications on privacy than alternative designs like Named Data Networks [45].

The following considerations are based on the assumption that many *technical systems* of the Information and Communication Technology (ICT) sector *enable, structure and/or constrain social interactions*. Thus, ICT systems typically embed and influence numerous values, including human rights. By now, this assumption is intensively discussed in the literature describing and analyzing the regulative or governing features of ICT systems, Internet architectures, protocols, and other Internet-based technologies and services [30, 24, 2, 10, 21, 28]. The terms used in different disciplines to analyze this phenomenon range from *lex informatica*, *code as law*, *regulating code*, *techno-regulation*, *governing algorithm*, *algorithmic governance*, *electronic institutions* to *software institutions*.

The current trend of connecting everything to the Internet leads to a growing dependency of the society and individuals on networks, and new or continued value conflicts can be expected. Despite several efforts in the past, there is still a lack of systematic approaches or methodologies for value-aware communication architectures and value-oriented network design, many research questions have not yet be sufficiently answered. We believe that more interdisciplinary research is urgently needed and that purely technical solutions may often be not sufficient to ensure the implementation of values.

2. VALUES, NORMS AND INSTITUTIONS

Values are "lasting convictions or matters that people feel should be strived for in general and not just for themselves to be able to lead a good life or to realize a just society" [43]. Social values are not individual preferences. They usually provide a mean for orientation, justification, and evaluation of decisions on actions and preferences. To a certain degree, they have intersubjective validity [43, 23].

At least when used for specific purposes, ICT systems intentionally or unintentionally *embed certain values* and have indirect effects on other values [12, 26]. In most cases, the values directly addressed in engineering are technical and economic values like system security or economic efficiency. Approaches of *values in design*, *value-sensitive design* or *constructive technology assessment* aim to broaden the range of values that are considered in research and development of technologies, including ICT systems.

Social values, which are normally abstract or global ideas or objectives, are often incorporated into *norms* to provide more concrete orientation in decision-making. In a broad understanding, norms are "rules that prescribe what concrete actions are required, permitted or forbidden" [43]. Norms prescribe how people should treat each other, and by this they make clear in everyday life how we should act to achieve certain values [43, 23].

For the following considerations, we understand norms as a type of institution. *Institutions* are established *systems of rules* that *enable, structure* and *constrain* social interactions, including the means to enforce them like incentives or sanctions [15, 27] (see also Fig. 2). The relation between values and institutions is that institutions realize certain social values due to their socially binding character. In this sense, institutions are established and enforced systems of intersubjective values.

When institutions and their values are implemented in and/or enforced by software systems we can speak of *"software institutions"*.[1] Following this, software institutions are systems of rules incorporated in and enforced by software that enable, structure and constrain social interactions by digital means. They especially include Internet *protocols* that define formats and rules according to which interactions (e.g., data exchange) between communicating parties take place. It will be shown below that software institutions are, however, just one of many elements in institutional frameworks that address interactions on the Internet.

2.1 Values of Human Rights

The main source of the values of human rights is the *International Bill of Human Rights* that is composed of the *Universal Declaration of Human Rights* (UDHR) [33] along with the *International Covenant on Civil and Political Rights* (ICCPR) [34] and the *International Covenant on Economic, Social and Cultural Rights* (ICESCR) [35]. In the light of several cases of Internet censorship, the Human Rights Council Resolution 20/8 was adopted in 2012, affirming "...that the same rights that people have offline must also be protected online..." [36]. In 2015, the *Charter of Human Rights and Principles for the Internet* [17] was developed and released [18]. According to these documents, some examples of human rights relevant for ICT systems are *human dignity* (Art. 1 UDHR), *non-discrimination* (Art. 2), *rights to life, liberty and security* (Art. 3), *freedom of opinion and expression* (Art. 19), *freedom of assembly and association* (Art. 20), *rights to equal protection, legal remedy, fair trial, due process, presumed innocent* (Art. 7–11), *appropriate social and international order* (Art. 28), *participation in public affairs* (Art. 21), *participation in cultural life, protection of intellectual property* (Art. 27), and *privacy* (Art. 12).

[1]The term "software institution" is used to indicate that such software systems not only govern or regulate but also enable new forms of social interactions. It also indicates that the features of software are seen as distinctive ones. Here, software includes not only algorithms, but also standards, interfaces, settings, defaults, and so on.

2.2 Value Conflicts

Even these fundamental societal values are frequently in conflict with each other, i.e., value conflicts are not the exception but the rule. Many conflicts are handled at national level, but this is not always possible in the context of the Internet as a global infrastructure.

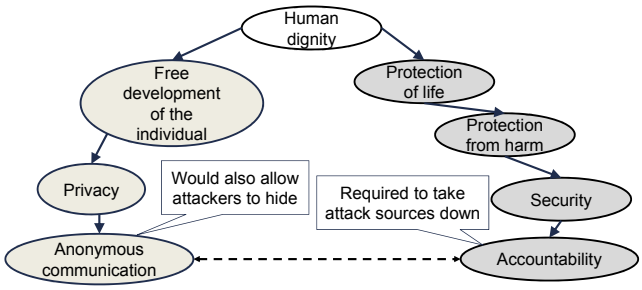


Figure 1: Example of value relations and the resulting value conflicts

Figure 1 shows an example of conflicting values. Protecting *human dignity* (Art. 1 UDHR) provides the moral basis for interpreting other human rights and deriving their meaning [14]. One derivation can lead from *protection of life* via *protection from harm* and *security* (Art. 3 UDHR) to *accountability*. That is, on the one hand, attackers on the Internet trying to disturb the proper functioning of the network (e.g., by launching distributed denial-of-service attacks) should be held accountable for their attacks. On the other hand, a right of the *free development of the individual* involves *privacy* (Art. 12 UDHR) and to use means for *anonymous communication*. But the latter makes it difficult to achieve accountability in order to take attack sources down and thus to protect the proper functioning of the network. Naylor et al. [25] suggested a solution aimed at achieving both goals. However, such a solution would require fundamental changes in the design of the core network protocol in the Internet.

With ongoing developments toward an *"Internet of everything"* further value conflicts can be expected since humans will be interacting with an increasing amount of devices (e.g., sensors and actuators), more areas of life are included and more actors with specific interests are involved. Among such *value conflicts* are those concerning (a) freedom of expression vs. right to privacy and reputation, (b) right to privacy and freedom of expression vs. surveillance for homeland security, (c) use of personally identifiable data vs. right to privacy, (d) platform strategies by Internet companies vs. freedom of choice through competition, (e) platform strategies vs. openness for innovation, (f) differentiation of services and prices vs. non-discrimination, (g) due process and fairness in trials vs. opaque software processes and decision-making, or (h) law enforcement by private companies vs. rule of law and independence of private actors.

Some questions about value conflicts and options of solving them have already been addressed earlier by other researchers, e.g., the seminal "Tussle in Cyberspace" paper by Clark et al. [7] and various approaches in the context of

Future Internet initiatives have been presented in the last years [1, 13, 20]. In spite of these initiatives a *methodology* for implementing values into the Internet protocols and architectures is still missing. A recent initiative within the IETF community led to the formation of a research group of the IRTF (Internet Research Task Force), called Human Rights Protocol Considerations Research Group [16]. The group's current objective is to expose the relation between protocols and human rights, with a focus on the rights to privacy, to freedom of expression and freedom of assembly. Moreover, the group aims to propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development.

In the following, we therefore attempt to shed some light on different options, necessities, and problems encountered in realizing values in networks.

3. TOWARD REALIZING VALUES IN NETWORKS

Handling value conflicts and realizing certain configurations of values on the Internet encompasses interrelated ways:

- *Specification and operationalization* of values, i.e., the transfer of abstract formulations of social values into technological options as well as into specifications and design requirements (cf. Section 3.1). Here, *engineering* provides technical solutions for conflicting requirements as well as basic options for choice, markets, and policy.

- *Institutionalization* of values, i.e., establishing or adjusting the institutional frameworks and governance structures of incentives and constraints so that certain values are more likely to be realized. In the case under consideration, two paths are possible: (a) by *policy and governance* – policy tries to balance interests, i.e., societal decision-making by legislation, court decisions and regulation (cf. Section 3.2.1); (b) by *choice and markets* – institutional frameworks for markets offer choice between different products according to different personal needs for social values (cf. Section 3.2.2).

Because of the specific feature of software institutions, i.e., being a functional part of the overall institutional framework, the above-mentioned ways have to be considered in their interrelations. This is outlined in the following.

3.1 Specification and operationalization of values

Value conflicts would ideally be addressed by applying procedures of measurements, that allow to compare quantified benefits and disadvantages of different alternatives and to choose the most beneficial one. However, unlike physical measurements the theoretical knowledge required for establishing valid quantified measurements of moral values in general [22] and values of human rights in particular does not exist. We do not have a commonly agreed-upon method for transferring values of human rights into measurable attributes. Instead, it seems feasible to specify values by using commonly agreed standards and norms [22, 42].

Human rights are formulated in an abstract way. This has the advantage that they can be applied to different contexts and times, but *requires interpretations* to get more concrete decisions and guidance for technical implementations.[2] More specific rules are given in the ICCPR [34] and ICESCR [35] and in comments and decisions by human rights bodies, as well as to a certain extend in ethical considerations. For instance, the *right to privacy* requires measures to be taken by governing actors, which are spelled out in UN documents: exceptions must be based on law, they should not be arbitrary, must be necessary to achieve a legitimate aim, proportionate to the aim pursued and the least intrusive option available [38]. The UN explicitly recommends to promote encryption and anonymity to exercise the right to freedom of opinion and expression and other rights like privacy [39].

The right to privacy could be implemented by using alternative network protocols other than the Internet Protocol since both versions (*IPv4 / IPv6*) do not offer a high degree of privacy. Sometimes IP addresses can be easily attributed to an individual and thus can be viewed as being personal data that can be tracked. Usually, both the sender and receiver addresses reveal information about communication relationships. The Tor [11] overlay network tries to achieve better privacy properties on top of IP, but suffers from performance problems and also inherits all disadvantages of IP. APIP [25] shows that an alternative design of an Internet Protocol could have led to better privacy properties in the Internet. Hornet [6] is an alternative design that achieves higher performance than Tor and offers stronger privacy protection than APIP, since it can provide both sender and receiver anonymity. However, measures in the network layer may get thwarted by addressing within the link layer, using globally unique IEEE MAC addresses that never change. Moreover, other paradigms like Named Data Networks [45] imply different privacy properties than IP [5].

Every of those alternatives are different approaches to instantiate privacy, but leave some uncertainty as to whether they actually comply with human right provisions or entail unintended consequences. It is necessary to conduct *interdisciplinary research* to enhance the understanding of the underlying purposes, rationales and principles of human rights to get guidance for the transfer to and implementation of human rights in future Internet technologies.[3] Additionally, there is a need for systematic analysis of the implications of technical alternatives for all relevant human rights and for possibilities to handle the few cases of permissible exceptions. These analyses should focus on consequences and side-effects on human rights and make potential tradeoffs that are inherent in decisions on technical developments more transparent. The approach used for implementing social values in technologies is often a context-dependent one, i.e., related to specific products, services or research projects [22]. However, in the case of generic Internet tech-

[2]In most member states of the United Nations, human rights are embedded in constitutional laws, which are sometimes more explicit. They are also interpreted by rulings of (supreme) courts. Although this does not directly result in internationally uniform specifications, it can support the interpretation by providing exemplifying cases of human rights implementations. For instance, the "Census Act" decision of the German Federal Constitutional Court, establishing the fundamental right of informational self-determination (BVerfGE 65, 1), gives an interpretation for the understanding of the right to privacy (Art. 12 UDHR).

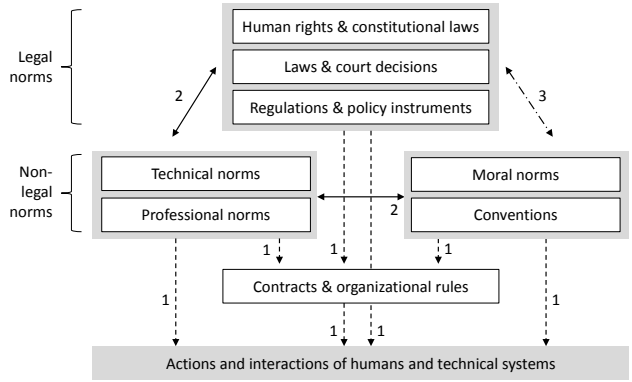
[3]For the rights to freedom of expression and association see the approach in [44].

nologies with an immense amount of possible Internet-based applications, services or products, further methodologies are needed.

3.2 Institutionalizing values

Institutions are one of the principal means to realize certain values and to handle value conflicts in society. In democratic societies, one of the ways how values become institutions is via political and legislative processes. There, value conflicts are articulated and argumentatively negotiated and values and limitations of value realizations are prioritized against other values. The results are legislation, regulations and policy instruments (Fig. 2). These include the institutional framework of markets that have an impact on the choice options and affect decisions of market actors and, indirectly, market outcomes and their implications for values (similarly [24, 9]). Institutional frameworks, ultimately, enable, structure and constrain the actions and interactions of humans and technical systems (between and among each other). This means, specific combinations of interacting types of institutions impact the actual realization of certain values. Thus, we suggest thinking in entire *institutional frameworks*, in which software institutions play a crucial but not the only role. This requires taking into account interactions, complementary or conflicting relations, supporting or replacing effects of software institutions and other types of institutions (similar in [24, 8]).

Without appropriate institutionalization, values of human rights transferred into Internet technologies are at risk of being not applied or being applied differently or even contrary to the original intention.



Legend: (Relation 1) enable, structure and constrain; (2) frame, substantiate and specify; (3) interpret and support

Figure 2: Types of institutions and their relations

As sketched in Figure 2, different types of institutions have *complex relationships* with each other [19]. Legal institutions, including human rights, enable and constrain the institutions of markets, including contracts and organizational rules. They also frame the establishment of technical norms, like in the case at hand, where human rights provisions should frame the development of Internet standards. Legal systems also depend on complementary moral norms that channel individual behavior toward legal provisions, since enforcement of law is most often incomplete. In some cases, legal provisions refer to moral norms like to "good manner" or to technical norms like the technological "state of the art" defined by standards organizations. For instance, the planned European General Data Protection Regulation (GDPR) refers to the use of "data protection by design" and "data protection by default". Non-legal norms include technical norms such as technical standards (e.g., IETF or W3C standards), professional norms such as codes of conduct, as well as moral norms and conventions. Moral norms are often influenced by law, but they are also often reflected in and transferred to law. Briefly, if provisions and enforcement of different institutions conflict with each other this can cause social tensions, including "tussles" in cyberspace [7], and lead to institutional change.

Many of the above-mentioned types of institutions can be implemented and enforced by software systems, even laws and moral norms. Today, private contracts and organizational rules are most often implemented in software institutions (digital rights management systems, social network services, search engines, etc.). This has led to critique, especially pointing to conflicts with legal provisions [24]. In general, when using software institutions to implement social values it is important to consider their *disadvantages and limitations*: (a) they can have negative (unintended) consequences on the realization of other social values and (b) conflicting relations to other institutions; (c) the effective realization of values is uncertain, especially when applied in combined and complex systems; (d) they may not adequately take exceptions of rules into account; (e) the legitimacy can be questionable, (f) they can be (prohibitively) costly, or (g) they can shift costs or other burdens to parties not involved in decision-making.

3.2.1 Policy and governance structures

In democratic societies, human rights are normally enshrined in the constitutional parts of the institutional frameworks and are interpreted and transferred more or less coherently in the corpus of legislation, regulation and administration. Political and juridical actors include values of human rights in political processes and make judgments about the realization of human rights and permissible limitations. The processes include decision- and rule-making, judicial procedures, regulation and oversight, as well as "checks and balances" among institutional actors. The outcomes are legislation, judicial decisions, and normative standards, i.e., the institutional framework that enables and constrains human behavior, including activities and rules on markets in form of contracts and organizational rules.

In the global context of the Internet, such a constitutional part in the institutional framework does not exist in this form. The *de facto* governance of the Internet, here understood in a broad sense [3], is a complex mix of rule systems, procedures and institutional actors at different governance levels, ranging from an international level (e.g., IETF, ICANN, ITU, W3C, IGF, etc.), to supra-national (e.g., EU), national or even regional levels. While there are ongoing discussions about the legitimacy, coherence or effectivity of the governance structures, which cannot be dealt with in this paper, we would like to shed some light on the *responsibilities for realizing human rights*.

Human rights are mainly directed to the relationships between governments and citizens with obligations for governments both to respect the rights of citizens in their own dealings and to protect the rights of citizens from violation by others. Governments should provide effective laws that

protect people from violation of their rights and means to enforce them like independent oversight bodies [37, 38, 32].

Although the juridical legitimacy of the IETF to enforce human rights by technical means might be questionable [4], rationales for responsibility of the IETF may stem from Art. 28 UDHR providing the right to an international order in which human rights can be realized. This claim is directed to global institutional actors [29]. In governance areas where governments are absent or play a minor role, this claim affects the de facto governing actors, i.e., the IETF and other actors of Internet governance.

In addition, private corporations have responsibility to respect human rights [40, 38]. "It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights." [41]. Private actors supply and maintain nearly the entire Internet infrastructure, the applications, products and services running on it, and also play a central role in enabling, providing, enforcing, and developing the institutional framework that governs the Internet [3]. Thus, it strongly depends on the behavior of private actors, be it private corporations or nonprofit standards organizations, how human rights are implemented, but also constrained or violated [32]. For example, it is unclear how Internet protocols and architectures, if solely developed by private companies, impact on human rights. Therefore, institutional frameworks of markets and private actors are also crucial for the actual realization of human rights (cf. Section 3.2.2).

Governments increasingly use private companies as proxies in activities affecting human rights, in particular for Internet surveillance and law enforcement ranging from copyright enforcement, to political censorship or combating Internet crime. From a human rights perspective, this is criticized for being contrary to the rule of law. Moreover, private companies are not subject to the same principles of accountability as governments. This practice is also coupled with an additional burden of monitoring companies by human rights defenders in the system of checks and balances [32].

Furthermore, institutional frameworks also comprise the *rules and conditions of the political processes* of deliberation, decision-making and solutions to value conflicts themselves. Such rules are required to limit or avoid regulatory capture by partial interests or unjustified dominance of state interests, e.g., surveillance of citizens vs. freedom of the individual. With software institutions, the political processes of institutionalization of social values is changed and (should be) shifted toward software development and deployment or the legislative framing or regulation of applications, if the latter is possible at all.[4] The rules for political processes, which should be reconsidered in light of software institutions, include access to necessary information, access to the arenas and processes of deliberation and decision-making, and providing capabilities and resources to participate, fairness criteria and procedural justice [9, 21, 28].

Research in and development of Internet technologies can (a) support the capabilities of individuals and their representatives to exercise human rights in all Internet contexts, and to prevent or correct imbalances in the relationships between and within states, individuals, private companies and other actors, where human rights are concerned. For instance, this can be means for end-users to (indirectly) monitor, audit and assess the actual working of software institutions and for detecting and proving biases in software institutions such as in judicial procedures. Such means can also support representatives of end-users or specialized authorities to ensure effective administrative, judicial and parliamentary oversight and ensuring accountability (as called for in [38]). (b) Research should also address the problem that orienting toward social values may result in context-specific or local solutions, because specific legal provisions have to be taken into account, but may also entail an Internet fragmentation.

3.2.2 Institutional framework for choices and markets

For this path of institutionalization of values, we assume that entrepreneurs and engineers develop products and services that realize certain values and, hence, provide *choice*. Consumers demand, select and use such products and services according to their expectations on fulfilling certain values.[5] By providing choice, the value judgments are "quasi" decentralized and transferred to the demand side. Examples of possible outcomes are privacy-preserving alternatives of search engines or social networks services, devices for monitoring data streams, or network access services guaranteeing certain quality standards.

However, this approach requires many *preconditions* to be fulfilled. Consumers have to be aware of what their values of human rights are in those contexts and how certain products or services affect them. Private companies often have insufficient incentives to include specific social values. For instance, designing privacy-friendly solutions for customers is not in the immediate interest of most companies when it does not provide any additional profit or is even counter-productive from their point of view. Additionally, in many cases only a few dominant companies provide a certain service with strategies to bind suppliers and end-users to their *"platforms"*, so that actual choice is very limited. Furthermore, private Internet companies are one of the main controllers of personal information, derived from the vast amount of online interactions. This can lead to market behavior violating the human right to privacy. Overall, several market failures are possible caused by network effects, tendencies toward monopolies, asymmetric information, externalities, etc.

Therefore, *institutional frameworks*, in the form of market law, consumer protection, privacy regulation, competition policy, and so on *are needed* in order to establish or stimulate

[4]The embedding of social rules in software, often shielded against reverse engineering by technical measures and additionally by law (protection of copyright and business secrets), makes it difficult or even impossible for "outsiders", who are affected by such rules, to directly comprehend, criticize, or even oppose them. This has also implications for the human rights to fair trial, legal remedy, and due process, as enshrined in Articles 8–11 UDHR.

[5]This is also relevant for many Internet-based products and services which end-users do not recognize as commercial goods since they seem to have no market price (e.g., search requests at search engine websites), but they are also private contractual agreements on exchanges (e.g., ordering of the relevance of knowledge in exchange of personal data) end-users often accept with a mouse click.

markets, mitigate market failures or constrain abusive market behavior. Here, the institutional frameworks have functions to enhance the efficiency of markets for products and services that contribute to the realization of human rights or which do not violate human rights during production and consumption. They should also prevent Internet protocols and architectural concepts from being misused or used in other contexts than originally intended.

Research in and development of Internet technologies can support market conditions in favor of realizing human rights, such as research (a) on open standards and other means that allow end-users to transfer products and data to other platforms, and, thereby, ensure actual options of choice, and that allow new commercial actors to participate with innovative products and services. Furthermore, research could be (b) on how increased flexibility in network infrastructures, e.g., by applying virtualization and software-defined networking concepts, can contribute to a flexible (re-) combination of network resources according to individual demands for social values, and (c) on means to enhance the assessment of the actual value-oriented quality of Internet products and services and possible side-effects from the perspective of end-users.

4. CONCLUSIONS

If networks and software systems influence the realization of certain values, their features can also be used to realize the values of human rights. Directly instantiating human rights in Internet protocols and architectures, e.g. through end-to-end encryption of Internet communication, is one option. This approach urgently requires a better understanding of how values and networks are related. What values lie behind protocols, design principles, technical and organizational options is largely unclear. Which values should be enforced by technical measures, at which layers by which design principles? How can technical implementations be assessed in view of values of human rights? Where is a complete implementation unfavorable, when are "hybrids" of ICT systems and conventional institutions more advantageous, and when should we refrain from using technical means for such purposes?

Developing Internet standards for protocols and engineering (e.g., by organizations like IETF and W3C) is probably only one part of a solution to the implementation of values. A coherent and socially acceptable institutional framework would require adequate incentives for engineering, institutional frameworks for markets and private actors as well as global arenas for policy and governance of the Internet. Research and development on Internet technologies could also support these approaches toward realizing human rights, by providing new and more options to choose from.

In conclusion, further research should focus on specifying and operationalizing values as well as the *interaction* of Internet protocols, architectures and software systems as functional parts of the overall institutional frameworks and governance structure. This requires methods that allow simultaneous considerations of technical and institutional solutions.

Acknowledgments

Several people contributed with fruitful and intense discussions on this subject. In particular, we would like to thank Oliver Raabe, Kay Mitusch, and many other colleagues from a proposed research initiative at KIT. Knud Böhle, René König, Reinhard Heil, Patrick Sumpf, Anika Hügle, Christina Merz also provided helpful comments, and Sylke Wintzer improved the language. All remaining errors are ours.

5. REFERENCES

[1] I. Brown, D. D. Clark, and D. Trossen. Should Specific Values Be Embedded In The Internet Architecture? In *ACM ReArch 2010*, 2010. http://dx.doi.org/10.1145/1921233.1921246.

[2] I. Brown and C. T. Marsden. *Regulating Code. Good Governance and Better Regulation in the Information Age*. MIT Press, Cambridge, MA, 2013.

[3] L. A. Bygrave. *Internet Governance by Contract*. Oxford University Press, Oxford, 2015.

[4] C. J. Cath. A Case Study of Coding Rights: Should Freedom of Speech Be Instantiated in the Protocols and Standards Designed by the Internet Engineering Task Force? Master's thesis, Oxford Internet Institute, 2015.

[5] A. Chaabane, E. De Cristofaro, M. A. Kaafar, and E. Uzun. Privacy in Content-oriented Networking: Threats and Countermeasures. *SIGCOMM Comput. Commun. Rev.*, 43(3):25–33, July 2013.

[6] C. Chen, D. E. Asoni, D. Barrera, G. Danezis, and A. Perrig. HORNET: High-speed onion routing at the network layer. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 1441–1454, Oct. 2015.

[7] D. D. Clark, J. Wroclawski, K. R. Sollins, and R. Braden. Tussle in Cyberspace: Defining Tomorrow's Internet. *IEEE/ACM Trans. Netw.*, 13(3):462–475, June 2005.

[8] J. E. Cohen. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press, New Haven, London, 2012.

[9] A. Correljé, J. Groenewegen, R. Künneke, and D. Scholten. Design for Values in Economics. In J. van den Hoven, P. E. Vermaas, and I. van de Poel, editors, *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains*, pages 639–666. Springer, Dordrecht et al., 2015.

[10] L. DeNardis. Hidden Levers of Internet Control – An infrastructure-based theory of Internet governance. *Information, Communication & Society*, 15(5):720–738, 2012.

[11] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *13th USENIX Security Symposium*, pages 303–320. Usenix, 2004.

[12] B. Friedman and H. Nissenbaum. Bias in computer systems. *ACM T Inform Syst*, 14(3):330–347, 1996.

[13] Future Internet Architecture (FIArch) Group. Future Internet Design Principles. `http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf`, Jan. 2012. last access: 2015-11-13.

[14] J. Habermas. The Concept of Human Dignity and the Realistic Utopia of Human Rights. *Metaphilosophy*, 41(4):464–480, 2010.

[15] G. Hodgson. What Are Institutions? *J Econ Issues*, 40(1):1–25, 2006.

[16] Internet Research Task Force IRTF. Human Rights Protocol Considerations Research Group (hrpc). `https://irtf.org/hrpc`, Feb. 2016. last access: 2016-02-22.

[17] IRPC. *The Charter of Human Rights and Principles for the Internet*. Internet Rights and Principles Coalition (IRPC), United Nations Internet Governance Forum, 2015.

[18] R. F. Jørgensen. An Internet Bill of Rights? In I. Brown, editor, *Research Handbook on Governance of the Internet*, pages 353–372. Edward Elgar, Cheltenham, Northampton, 2013.

[19] W. Kasper and M. E. Streit. *Institutional Economics. Social Order and Public Policy*. Edward Elgar, Cheltenham, Northampton, 1998.

[20] C. Knobel and G. C. Bowker. Values in Design. *Communications of the ACM*, 54(7):26–28, 2011.

[21] B.-J. Koops. Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values. In R. Brownsword and K. Yeung, editors, *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*, pages 157–174. Hart, Oxford and Portland, 2008.

[22] P. Kroes and I. van de Poel. Design for Value and the Definition, Specification, and Operationalization of Values. In J. van den Hoven, P. E. Vermaas, and I. van de Poel, editors, *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains*, pages 151–178. Springer, Dordrecht et al., 2015.

[23] H. Lenk, F. Rapp, and G. Ropohl. Wertgrundlagen der Technikbewertung. In R. v. Westphalen, editor, *Technikfolgenabschätzung als politische Aufgabe*, pages 115–136. Oldenbourg, München, Wien, 3 edition, 1997.

[24] L. Lessig. *Code Version 2.0*. Basic Books, New York, 2006.

[25] D. Naylor, M. K. Mukerjee, and P. Steenkiste. Balancing Accountability and Privacy in the Network. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, pages 75–86, New York, NY, USA, 2014. ACM.

[26] H. Nissenbaum. Values in Technical Design. In C. Mitcham, editor, *Encyclopedia of Science, Technology and Ethics*, pages Ixvi–Ixx. Macmillian, New York, 2005.

[27] D. C. North. *Institutions, Institutional Change, and Economic Performance*. Cambridge University Press, Cambridge, New York, 1990.

[28] C. Orwat, O. Raabe, E. Buchmann, et al. Software als Institution und ihre Gestaltbarkeit. *Informatik-Spektrum*, 33(6):626–633, 2010.

[29] T. Pogge. Menschenrechte als moralische Ansprüche an globale Institutionen. In S. Gosepath and G. Lohmann, editors, *Philosophie der Menschenrechte*, pages 378–400. Suhrkamp, Frankfurt am Main, 1998.

[30] J. R. Reidenberg. Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*, 76(3):553–584, 1998.

[31] M. Rundle and C. Conley. *Ethical Implications of Emerging Technologies: A Survey*. United Nations Educational, Scientific and Cultural Organization (UNESCO), 2007.

[32] D. Souter. *Human Rights and the Internet: a Review of Perceptions in Human Rights Organisations*. Association for Progressive Communication (APC), 2012.

[33] UN. *The Universal Declaration of Human Rights*. United Nations (UN), 1948.

[34] UN. *International Covenant on Civil and Political Rights*. United Nations (UN), 1966.

[35] UN. *International Covenant on Economic, Social and Cultural Rights*. United Nations (UN), 1966.

[36] UN HRC. *The promotion, protection and enjoyment of human rights on the Internet. Resolution 20/8*. United Nations, Human Rights Council (UN HRC), 2012.

[37] UN HRC. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40)*. United Nations, Human Rights Council (UN HRC), 2013.

[38] UN HRC. *The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37). Advanced Edited Version*. United Nations, Human Rights Council (UN HRC), 2014.

[39] UN HRC. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32), Advanced Edited Version*. United Nation, Human Rights Council (UN HRC), 2015.

[40] UN OHCHR. *Guidelines for the Regulation of Computerized Personal Data Files. Adapted by General Assembly resolution 45/95 of 14 Dezember 1990*. United Nations, Office of the High Commissioner for Human Rights (UN OHCHR), 1990.

[41] UN OHCHR. *Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework*. United Nations, Office of the High Commissioner for Human Rights (UN OHCHR), 2011.

[42] I. van de Poel. Translating Values into Design Requirements. In D. P. Michelfelder, N. McCarthy, and D. E. Goldberg, editors, *Philosophy and Engineering: Reflections on Practice, Principles and Process*, pages 253–266. Springer, Dordrecht et al., 2013.

[43] I. van de Poel and L. M. M. Royakkers. *Ethics, Technology, and Engineering. An Introduction*. Wiley-Blackwell, Malden, Mass., 2011.

[44] J. Varon, N. ten Oever, C. Guarnieri, W. Scott, and C. Cath. Human Rights Protocol Considerations Methodology, 2016. Internet Draft draft-varon-hrpc-methodology-04, work in progress.

[45] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang. Named Data Networking. *SIGCOMM Comput. Commun. Rev.*, 44(3):66–73, July 2014.