relevant normative considerations in order to strike a good balance between competing values.

Cybersecurity value conflicts in health: Conflicts with regard to cybersecurity in health are often related to privacy and data protection, i.e. securing health data against unauthorized access. However, there are other types of conflicts. For instance, reaching a high level of cybersecurity might be very costly and therefore, only a small amount of people might be able to afford strong cybersecurity. Cybersecurity also might contradict usability and accessibility.
These problems can be demonstrated with the paradigmatic example of the German eHealth Card (eHC): "As part of the German health-care reform, the current health insurance card is being upgraded to an electronic health card. On it, data on patient investigations, drug regulations, vaccinations and emergency data are stored. The aim is among other things to improve medical care and the prevention of drug incompatibilities and duplication of investigations" (Jürjens & Rumm, 2008). Initially, it was planned to disseminate the eHC to every person insured through the German health insurance system. However, due to strong opposition from various stakeholders, only at least 10 per cent of insured person should receive an eHC (Fox, 2010). Furthermore, due to security considerations concerning data protection some of the functions (electronic prescription and electronic health record; the latter can be used on a voluntary basis) of the eHC were not realized. Particularly German physicians are quite skeptical with regard to the eHC, since it is feared that its deployment will cause huge costs and will increase the workload of physicians and health care personnel. At the same time, the benefits, e.g. in terms of security, are less clear: "The efficiency of the system is considered as critical by the physicians, particularly in terms of data security and potential misuse of data. The primary concern of the physicians is the unauthorized access of a third party to stored data." In addition, "[r]egarding the introduction of the eHC to date, most physicians have criticized the very opaque communication and poor instruction on the subject" (Wirtz, Mory, & Ullrich, 2012). From the point of view of at least some stakeholders, it seems not to be satisfactory to only claim, for instance by state authorities, that cybersecurity and efficiency can be increased—more information is requested. Given the existing literature regarding security issues of the German eHC, many of the concerns that were mentioned by physicians seem to be correct (Sunyaev, Leimeister, & Krcmar, 2010; Winandy, 2010).

The deployment of the German eHC and similar ICT infrastructures in other countries might also be accompanied with potential discrimination. Due to security considerations, e.g. to protect medical data against misuse and unauthorized access, such infrastructures employ encryption and password protection of sensitive data. Laur mentions "[w]hile some people have already difficulty remembering a PIN (especially elderly and disabled people), having many more passwords that are intended to protect them could put them at risk of disclosure, loss or stealing" (Laur, 2015). Although Laur refers to electronic health records in general, the problem also applies to the German eHC in particular. The security measures employed in the case of the eHC are not designed in a way the idea of universal design and general accessibility is demanding. This raises questions regarding social justice and equality. It is quite likely that the affected stakeholders will create their own

work-arounds, for example by writing passwords or PINs on the eHC or by disclosing them to health care personnel, which certainly will reduce their level of data protection, privacy and security with regard to their medical record. In other words, cybersecurity measures that shall protect medical information of citizens but are ill constructed from a usability point of view, force at least some parts of the population to act in a way that reduces their security.

To sum up, at least the example of the German electronic health card and probably other instances of such cards or electronic health records show that cybersecurity can be in conflict with other values than privacy. In the above-mentioned cases, we see conflicts with regard to usability and accessibility, social justice and equality. Moreover, increasing cybersecurity almost always causes economic burdens which might not be fairly distributed.

Cybersecurity value conflicts in national security: Value conflicts with respect to cyber security in the political domain are regularly phrased in terms of security versus privacy, but at closer inspection they are often more complicated. Take for example the discussion about end-to-end encryption in *WhatsApp*. Governments and security agencies have argued that they need to be able to access such encrypted communication for security reasons, e.g. to be able to early detect possible terrorist attacks. Opponents of such access by governments and security agencies do not only point at privacy considerations, but also at the fact that encrypted communication that cannot be accessed by governments and their agencies might be important for the democratic process, and that it enables opposition movements in countries with totalitarian or suppressive regimes.

A similar issue has arisen in relation to the *Tor* network. "Tor is free software and an open network that helps … defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy."[13] The networks operates as "a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet."[14] In the aftermath of the hacking of the Democratic Party during the US elections, it turned out that a Dutch private *Tor* server had probably been used in the hacking.[15] The Tor server was owned by Rejo Zenger, A Dutch *Bits of Freedom* employee. *Bits of Freedom* describes itself as "the leading Dutch digital rights organization, focusing on privacy and communications freedom in the digital age".[16] While Zenger recognized that *Tor* servers can be misused by hackers, and are in that sense a threat to cybersecurity, he believes that this is a price worth paying, not only for reasons of privacy but also because these servers may be crucial for whistle blowers to

13 See: https://www.torproject.org/ - Accessed 28/01/2017.

14 See: https://www.torproject.org/about/overview.html.en - Accessed 28/01/2017.

15 See: http://nos.nl/artikel/2151234-tor-helpt-hackers-maar-ook-klokkenluider-stoppen-heeft-geen-zin.html - Accessed 28/01/2017.

16 https://www.bof.nl/home/english-bits-of-freedom/ - Accessed 29/01/2017.

reveal abuses. Again, the value that is at stake here is not just privacy but also a range of civil liberties that are seen as crucial for democracy and the democratic process.

Another example is profiling. In this case, values like non-discrimination and absence of bias are at stake and are potentially conflicting with security. In profiling, people are approached, judged or treated in a certain way because these have characteristics that fit a certain profile and that are associated with certain other traits (i.e. traits other than by which they are identified as belonging to the profile). Profiling is used for a wide range of purposes. It may be used by the police or security agencies to find criminals or terrorists; by airports to decide who to check more carefully, by (internet) companies to target certain consumers, by banks in deciding who to give a loan (and against what percentage). As these examples already suggest sometimes profiling serves security objectives. At the same time, profiling may inflict all kinds of undeserved harm on people, from nuisance to false accusations to even, in extreme cases, imprisonment of innocent people. Although profiling may involve privacy violations, because personal information is gathered to fit somebody into a profile, the main issue at stake is not privacy. Rather the issue is that a generalization is made based on limited information about a person. This generalization is based on statistical information about a group to which a person belongs while, due to its probabilistic nature, this information may say nothing about that particular person. Profiling may lead to stereotyping and discrimination. For example, the use of facial recognition technologies by the police and security officers has led to such concerns. Some studies suggest that facial recognition cognition algorithms are less accurate for certain social groups or races (Klare, Burge, Klontz, Vorder Bruegge, & Jain, 2012), which may lead to racial bias in their use (Garvie, Bedoya, & Frankle, 2016; Introna & Wood, 2004).

Another value issue that might arise due to the collection of data by certain organizations for security reasons and that is not completely covered by privacy is the creation of power imbalances. Economic monopolies or oligarchies are often considered undesirable, and in democracies, balancing the (political) power between citizens and their government is an important concern. Maintaining certain power balances is therefore considered important by many for a healthy economy and for democratic politics. What seems to be less recognized is that in the information age, the possession of information about others and their behavior is increasingly a source of power. This also means that organizations that collect or possess large amounts of (personal) data may have increasingly power over other actors, which may lead to the disruption of existing power balances and the creation of new power imbalances. This applies to companies like *Google* or *Facebook* that collect large amounts of data about users and consumers, but also to governments and security agencies that may collect large amounts of data about citizens—and to providers of cybersecurity technologies as well, as they activities may involve the access to highly sensitive data. It should be noted that the accumulation of large amounts of data in the hands of a few may lead to new power imbalances and may be problematic even if such data is anonymized, or if people have given their informed consent for the collection, storage and use of their data. This means that even if privacy concerns are properly addressed, the accumulation of large amounts of data in the hands of a few may be considered problematic for economic as well as political reasons.

Value conflicts in cybersecurity design processes: Cybersecurity field offers opportunities for security service providers to be responsive to secure digital ecosystem but it must also challenge them to ensure that such opportunities are taken to reflect the need of embedding fundamental values in innovative security services and products. This mainly happens under Research and Development (R&D) initiatives of these companies to address real-world cyber-security threats and scenarios in addition ensure trust and confidence among their clients. Hence, security service providers must continue to build and protect their clients, their user machines, engage different stakeholders including businesses and customers to reflect their technical, political, social and ethical values and concerns, and respect functional values upon which our society was built on e.g. autonomy, equality, fairness, freedom and responsibility (Van den Hoven, 2008). They should then not only focus on the security vs. privacy dichotomy, but also highlight any other linkages between the core value of security in cybersecurity to other social and ethical values in order to understand the ethical problems of cybersecurity. To fulfill so, they need to address pro-actively future threats that come with the emergence of the next generations of technologies and services (e.g. IoT, 5G, etc.). But how can we make sure the R&D of security service providers today will meet the needs and requirements of tomorrow? How can we make sure relevant social and ethical values will be incorporated into the security service providers' R&D? The discussed issues are solved when security service providers understand their security initiatives consequences.

Some security service providers may detect an intrusion attempt through their independent security labs. The question is how aggressively they should block and stop an intrusion attempt. In most cases, a trade-off is seen as they could block a bit or aggressively in contrast. From a customer point of view, the rate of detection over the collection of files could be against the positive rate. Security vendors have then two choices: either apply for high intrusion detection rate or apply high positive rate. Choosing either of those choices has economic implications for customers, and has an impact on their fairness levels. In addition, cybersecurity operators (such as ICT security software providers) have considerable access power to the computer systems of their customers, which involves privacy risks, including the possibility of wrongly accusing an employer of the customer to be responsible for a certain cyber threat. The right split between the rate of detection and the positive rate is absolutely a subjective issue and depends on the specific context. For instance, a military environment comparing a health sector environment might ask a higher positive rate instead of only detecting data, and as this request fulfills by security service providers, one can argue different fairness level within different cyber space environments.

Another example is, when security vendors collect data from user machines, where they need to have user consent for different activities. In fact, security service providers ask their clients to fill out the consent forms and clients literally accept relevant consent forms. The question here is to what extent security service providers need to give their clients access to systems. Here is a value conflict between security measures and their impacts on customer' access. More control from customers cause less control by security service providers, in turn revealing more sensitive information. Hence, the level of

customer' access to user machines and digital infrastructure, which can involve discrimination (Custers, Calders, Schermer, & Zarsky, 2013), is twined to the security level. Hence, this value conflict between security and discrimination also must be taken into account within security service providers' R&D.

Accordingly, security service providers' R&D must also address social and ethical values rather only security while they take appropriate security measures. This is essential for the maintenance of critical societal or economic activities in different sectors (e.g., energy, transport, banking, financial services, health, and digital infrastructure).

Mapping and evaluating value conflicts in cybersecurity

However, how can cybersecurity service providers get a reasonable understating on the values involved in cybersecurity problems? Our suggestion is to provide a map on how key aspects of cybersecurity activities positively or negatively affects those values. Figure 4 shows a first draft of such a map based on values discussed in the previous sections. The map shows that cybersecurity is directly related to harm prevention values —both information harm (e.g., caused through disclosure of personal information) or physical harm (e.g., preventing damage on the critical infrastructure). Harm-prevention is supporting for a set of other important values such as privacy or personal freedom. However, cybersecurity measures usually involve some degree of monitoring, cause economic costs and require personal efforts. Those elements usually have negative impact on a whole set of values: Economic costs raise problems of resource allocation that can be in conflict with notions of social justice of equality. Personal efforts needed is confronted with the problem that individuals differ with respect on possessing the necessary (e.g., cognitive) resources. Surveillance not only increases the risk of discrimination and privacy violation; false negative results also can directly impact a core value cybersecurity usually upholds, namely preventing information harm (e.g., because the accused employee loses reputation). The problem is further complicated by the possibility that some values may be in a conflicting relation as well. Personal freedom can counteract social justice, requiring some kind of balancing—exemplified by John Stuart Mills famous quite in *On Liberty*: "The only freedom which deserves the name, is that of pursuing our own good in our own way, so long as we do not attempt to deprive others of theirs, or impede their efforts to obtain it."

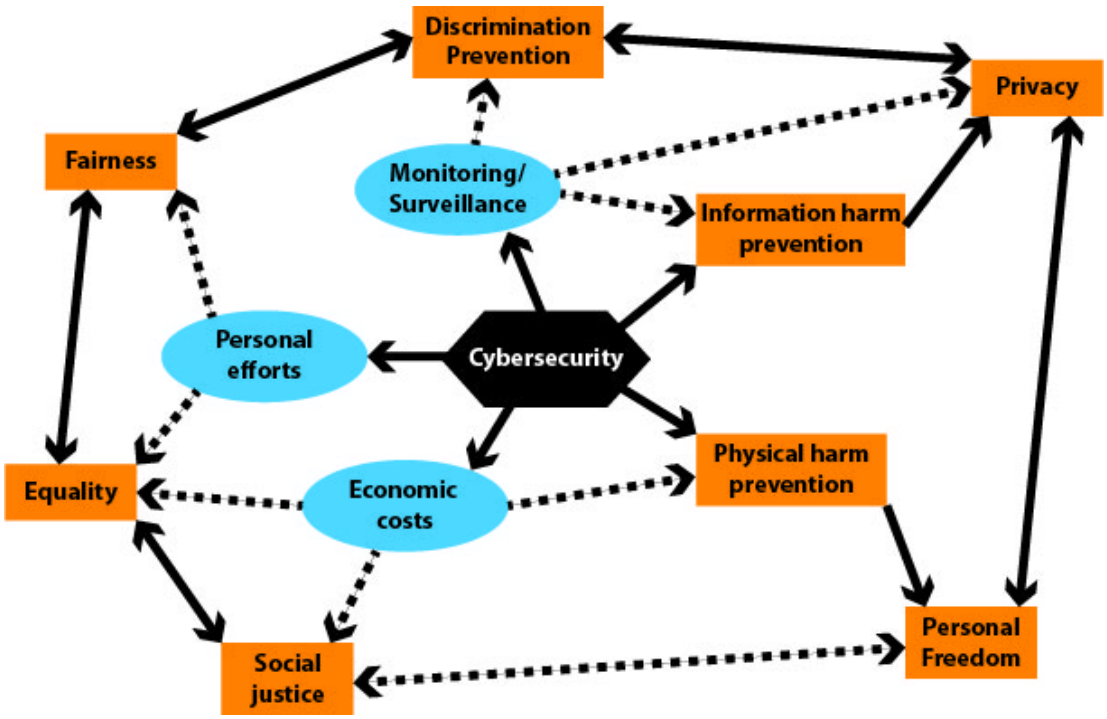

Figure 4: Outlining a first draft of a map on value conflicts in cybersecurity. Arrows with continuous lines show positive (i.e., supporting) relations, whereas arrows with dotted lines show conflicting relations (the map does not show all possible relations). Orange squares refer to values.

So, how can a map help to mitigate these conflicts? For doing this, it is important to recognize that the context strongly influences the framing of those value conflicts. By "context", we do not refer to the details of each single case, but to the notion of "contextual integrity", that emphasizes the importance of distinct social spheres and context sensitive norms in data flows (Nissenbaum, 2004). Contextual integrity forms a main moral reason for data protection (Van den Hoven, 2008); it is legally expressed in terms of purpose specification, use limitation, and data minimization. Contextual integrity refers to the fact that the human environment is structured in social spheres that provide important reference points for human beings. Humans expect to be treated differently in a family context compared to, for example, in a governmental organization. They accept inequality in treatment in the economic sphere that they would not accept in the health, legal or education sphere. Thus, the interpretation of moral values such as justice or autonomy, and the rules related to these values—for example in the case of justice different allocation rules such as "an equal share for everyone" compared to "sharing ac-cording to needs"—differ along these social spheres. The analysis of value conflicts in cybersecurity will have to consider such context effects.

The following example might be useful for explaining the role of contextual integrity. Let us assume that a cybersecurity service provider has considerable access to a computer network of a customer for allowing intrusion detection. In performing its monitoring task, the cybersecurity provider detects suspicious activities within the company computer network that might indicate that some employees of the company are actually involved in offensive cyberattacks against some other target, i.e., the company is not a victim of an

external intrusion, but acts as an attacker towards third parties. What is the status of this information with respect to contextual integrity? At first sight, we are in a business context with a contractual obligation between the customer and the provider. Disclosing this information towards the customer is thus an obligation. The fact that employees of the companies themselves act as attackers, however, have implications that go beyond the business domain. One possibility is that the employer acts on behalf of the company in order to disturb the activities of a foreign company that practices industrial espionage. This "hacking back" would follow the conception of "self-defense" that might also morally justify offensive actions, but its legality is questionable (Lin, Allhoff, & Abney, 2014). The other possibility is that the employee acts on his own, e.g. he tries to hack into a governmental website of an oppressive state as a form of hacktivism. This is surely illegal with respect to the internal rules of the company, but let us assume that the person emigrated from this oppressive country and that some of his family still lives there. If the information about this hacking activity leaves the business context, the ethical problems aggravate. In the first case, by approaching jurisdiction, the case likely becomes public—and a company that has a reputation of hacking back is likely to become an even more likely target, thus increasing the cybersecurity problem[17]. In the second case, a risk of actual physical harm to third parties (the family of the offender) is risked. Thus, in either case, the ethical solution might be that this sensible information does not leave the business context. In the first case, the company could be informed by the security provider about the substantial risks "hacking back" actually involves, whereas in the second case, the employee could be internally sanctioned for his behavior without disclosing the reason. This example illustrates that getting an understanding on how the changing context influences the ethical valence of information is important to understand value conflicts in cybersecurity.

Conclusion

In this contribution, we first demonstrated an (expected) growing importance of cybersecurity in general (measured by the number of publications) and an escalation in terms of describing the severity of the incidences (as increasingly war-like nowadays). We also found that the terminology of privacy still is the dominating ethical term in the debate, although there are indications that this is changing. By referring to exemplar cases, we found that—although cybersecurity has an ethical justification in terms of harm prevention—cybersecurity activities can induce conflicts with other values, some even counteracting the ethical legitimation of cybersecurity as such.

This work, however, should be seen as a preliminary result. First, because the quantitative analysis has pointed to some conflicting results that need further investigations—which is not easy given that the literature body is huge. Second, because the examples provided deserve a deeper normative analysis as done so far. Our draft of a value map requires more refinement. Furthermore, it should include a more intuitive way of visualizing the contextual aspects of possible conflicts. For doing this, we consider the framework of

17 See: https://business.kaspersky.com/hacking-back-ii/4556/ - Accessed 02/02/2014

contextual integrity as fruitful. However, more work is needed in order to explore this approach.

Acknowledgement
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 700540 and the Swiss State Secretariat for Education, Research and Innovation under contract number 16.0052-1.

References

Brey, P. (2007). Ethical Aspects of Information Security and Privacy. In M. J. Carey & S. Ceri (Eds.), *Security, Privacy and Trust in Modern Data Management* (pp. 21–36). Heidel-berg: Springer.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons*, *34*(14), 39–48.

CSIS - Center for Strategic and International Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. Retrieved January 31, 2017, from http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf

Custers, H. M., Calders, T., Schermer, B. W., & Zarsky, T. Z. (2013). Discrimination and Privacy in the Information Society Berlin/London: Springer. In *Studies in Applied Philosophy, Epistemology and Rational Ethics* (Vol. 3). Berlin/London: Springer.

Egelman, S., Herley, C., & van Oorschot, P. C. (2013). Markets for zero-day exploits: ethics and implications (pp. 41–46). ACM Press. https://doi.org/10.1145/2535813.2535818

Elkington, J. (1997). *Cannibals with Forks. The Triple Bottom Line of 21st Century Business*. Mankato: Capston Publishing Ltd.

Fox, D. (2010). Elektronische Gesundheitskarte. *Datenschutz Und Datensicherheit – DuD*, *34*(12), 844.

Freeman, R. E. (1984). *Stakeholder management: A stakeholder approach*. Boston: Pitman.

Friedman, M. (1970). The social responsibility of business is to increase its profits. *The New York Times Magazine*, *13*, 122–126.

Friedman, M. (1982). *Capitalism and Freedom.* Chicago: The University of Chicago Press.

Garvie, C., Bedoya, A. M., & Frankle, J. (2016). *The perpetual line-up. Unregulated police face recognition in America.* Georgetown Law Center on Privacy & Technology.

Introna, L., & Wood, D. (2004). Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance and Society*, *2*(2/3), 177–198.

International Telecommunications Union. (2008). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity. Retrieved January 31, 2017, from https://www.itu.int/rec/T-REC-X.1205-200804-I

Jürjens, J., & Rumm, R. (2008). Model-based Security Analysis of the German Health Card Architecture. *Methods of Information in Medicine*, *47*(5), 409–421.

Klare, B. F., Burge, M. J., Klontz, J. C., Vorder Bruegge, R. W., & Jain, A. K. (2012). Face Recognition Performance: Role of Demographic Information. *IEEE Transactions on In-Formation Forensics and Security*, *7*(6), 1789–1801.

Klimburg, A. (Ed.). (2012). *National cyber security framework manual.* NATO CCD COE Publications.

Laur, A. (2015). Fear of e-Health Records implementation? *Medico-Legal Journal*, *83*(1), 34–39.

Lin, P., Allhoff, F., & Abney, K. (2014). Is Warfare the Right Frame for the Cyber Debate? In L. Floridi & M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 39–59). Berlin: Springer.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*, 119–157.

Pike, R. E. (2013). The "Ethics" of Teaching Ethical Hacking. *Journal of International Technology and Information Management*, *22*(4), 1–7.

Rowe, N. C. (2008). Ethics of Cyber War Attacks. In L. Janczewski & A. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 384–394). Hersey: Information Science Reference.

Sunyaev, A., Leimeister, J. M., & Krcmar, H. (2010). Open Security Issues in German Healthcare Telematics (pp. 87–194). Presented at the Proceedings of the Third International Conference on Health Informatics (HealthInf 2010), Valencia/Spain.

Van den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. In J. van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 301–321). Cambridge, New York: Cambridge University Press.

Winandy, M. (2010). A Note on the Security in the Card Management System of the German E-Health Card. In *Electronic Healthcare—Third International Conference* (pp. 193–203). Casablanca/Morocco.

Wirtz, B. W., Mory, L., & Ullrich, S. (2012). eHealth in the public sector: An empirical anal-ysis of the acceptance of Germany's electronic health card. *Public Administration*, *90*(3), 642–663.

World Commission. (1987). Report of the World Commission on Environment and Development: Our Common Future, Chapter 2: Towards Sustainable Development. Retrieved from http://www.un-documents.net/our-common-future.pdf