Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security

van de Poel, Ibo

DOI
10.1007/978-3-030-29053-5_3

Publication date
2020

Document Version
Final published version

Published in
International Library of Ethics, Law and Technology

Citation (APA)
van de Poel, I. (2020). Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security. In M. Christen, B. Gordijn, & M. Loi (Eds.), *International Library of Ethics, Law and Technology* (pp. 45-71). (International Library of Ethics, Law and Technology; Vol. 21). Springer. https://doi.org/10.1007/978-3-030-29053-5_3

Chapter 3
Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security

Ibo van de Poel

Abstract This chapter analyses some of the main values, and values conflicts, in relation to cybersecurity by distinguishing four important value clusters that should be considered when deciding on cybersecurity measures. These clusters are security, privacy, fairness and accountability. Each cluster consists of a range of further values, which can be viewed as articulating specific moral reasons relevant when devising cybersecurity measures. In addition to the four value clusters, domain-specific values that are served by computer systems, such as health, are important. Following a detailed discussion of the four relevant value clusters, potential value conflicts and value tensions are considered. The relationships of five pairs of values (privacy-security, privacy-fairness, privacy-accountability, security-accountability and security-fairness) are analysed in terms of whether they are largely supportive or conflicting. In addition, possible methods for addressing these potential value conflicts are discussed. It is concluded that values, and value conflicts, in cybersecurity should be considered in context, also taking into account the specific computer systems at play, to enable the use of nuanced and fine-grained methods for addressing the relevant value conflicts.

Keywords Accountability · Fairness · Privacy · Security · Value conflict · Values

3.1 Introduction

Moral dilemmas in cybersecurity are often framed in terms of privacy versus security. If we want to avoid illegal access to ICT (Information and Communication Technology) systems through hacks, cybercrime or cyberwarfare, we need to be willing to accept the monitoring of Internet traffic and hence give up (some) privacy, so the suggestion goes. Although we may indeed sometimes be confronted with

I. van de Poel (✉)
Department Values, Technology and Innovation, School of Technology, Policy and Management, TU Delft, Delft, The Netherlands
e-mail: i.r.vandepoel@tudelft.nl

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_3

such dilemmas, the privacy versus security tension, as a general framing of moral issues in cybersecurity, is too simplistic. Privacy and security are not always in conflict but are sometimes mutually reinforcing. Whether privacy and security are conflicting or supportive depends on the specific context or application being considered. Moreover, it depends on technical and design choices that can also be made differently so that the conflict can sometimes be designed out. The privacy versus security framing is also too simplistic in that it ignores the fact that a range of other values are at stake in cybersecurity.

The aim of the chapter is twofold. First, it sets out to develop a coherent and comprehensive account of the main values relevant to cybersecurity. This concerns both the values at stake when cybersecurity is somehow compromised as well as those values that should be considered when devising (technical or institutional) measures to maintain or increase cybersecurity. Second, the chapter aims to shed more light on value conflicts in cybersecurity and the possible methods for addressing such conflicts.

The chapter begins with a philosophical clarification of the notion of value. Values are understood as evaluative dimensions that can be used to evaluate the goodness of certain state-of-affairs. Different values thus correspond to different varieties of goodness. In addition, values are conceived as arising in response to certain morally problematic situations, or certain moral concerns. Therefore, they correspond to certain moral reasons (for or against certain actions). This understanding of values allows several value clusters to be discerned in relation to cybersecurity. A value cluster is here understood as a number of values which are a response to similar types of moral concerns and express similar moral reasons. It is argued that, in relation to cybersecurity, four values cluster can be discerned: security, privacy, fairness and accountability.

After addressing these value clusters in more detail, the chapter discusses value conflicts. A value conflict is understood as a situation in which it is not possible to fully realise or respect a range of relevant values simultaneously. Value conflicts are thus practical conflicts, as opposed to values contradicting each other at a general or abstract level. Identifying value conflicts requires a consideration of the specific application or context. Moreover, whether values conflict depends on what is technically possible and what design choices have been made. I discuss some of the main value conflicts in cybersecurity and possible methods to address them.

3.2 Values and Value Clusters

3.2.1 What Are Values?

Although the notion of ‘value’ is generally used in philosophy and the social sciences, there does not seem to be a generally accepted definition of what values are. In general, values are associated with what is *good* and *desirable,* and they are often

believed to provide people with a certain orientation for how to behave. Within this general characterisation, additional conceptions of values are possible.

In the social sciences, values are often associated with attitudes, preferences and interests, and are usually seen as subjective (Williams Jr. 1968; Rokeach 1973; Schwartz and Bilsky 1987). Here, I employ a more philosophical understanding of values, in which values are associated with what is *good*. So conceived, the notion of value can refer to what is good (ontology), or what we belief (epistemology) or express (semantics) to be good (Hirose and Olson 2015). Values help to evaluate certain state-of-affairs in terms of goodness, and different values can therefore be understood as varieties of goodness (von Wright 1963). For example, computer systems may be evaluated in terms of the values of privacy and cybersecurity, by which each constitute a different variety of the goodness of such systems.

Values belong to the evaluative domain of the normative, whereas norms and reasons belong to the deontic domain of the normative (Stocker 1990; Dancy 1993; Raz 1999). The evaluative refers to the normative evaluations we make of state-of-affairs or persons (in terms of goodness). Conversely, the deontic refers to the reasons we have for doing certain things (or refraining from doing them) or to what we should do. The deontic is concerned with rightness (of actions) whereas the evaluative is concerned with goodness (of state-of-affairs).

Since values are evaluative, they are not directly action guiding. Nevertheless, it is often believed that there is a correspondence between values and reasons (for action) of the following kind (cf. Scanlon 1998; Raz 1999):

> *V: If x is a value (or a valuable object) then one has reasons (of a certain kind) for a positive response (a pro-attitude or a pro-behaviour) towards x*

For example, if cybersecurity is a value, we might have reason to increase it through technical and institutional measures; and if privacy is also a value, we might have reason to respect the privacy of computer users in devising such cybersecurity measures. Increasing and respecting are both positive responses.

Statement V is intended to be neutral with respect to the question of whether values ground reasons (as consequentialists typically believe) or reasons ground values (as deontologists typically hold) or that neither can be reduced to the other. As Dancy (2005) notes, whatever position one takes in this debate, something like statement V seems to be true.

It should be stressed that the above account of values does not assume consequentialist ethics. Deontologists may also employ the notion of value, although values may have a different epistemological and ontological status for them than for consequentialists; for the former, values typically follow from reasons (and other deontic concepts such as norms) rather than the other way around (cf. Anderson 1993).

In this respect, it is also important to stress that the positive response mentioned in statement V can take another form than just increasing or maximising the value x. Consequentialists often believe not only that the goodness of the outcomes (consequences) of actions determine the rightness of actions but also that right actions increase or even maximise the 'amount' of value or goodness. Although increasing or maximising a value can be termed a positive response (or a pro-behaviour), it is

certainly not the only possible positive response. Values can, for example, also be *respected;* and a valuable object can be *admired.* Respect and admiration are also positive responses, but they do not have the consequentialist overtone that increasing or maximising value has.

What the appropriate positive response to a value (or a valuable object) is depends both on the value at stake as well on the specific context. For example, in some contexts, we might have reason to maximise privacy, whereas in other contexts it may be sufficient to respect a certain minimal amount of privacy. The proper response to a value in a specific context is often not prima facie obvious; it may require judgment and deliberation.

3.2.2 Value Clusters

If values are varieties of goodness, it seems natural to assume that there exists a plurality of values. Some philosophers have, nevertheless, maintained that there is one overarching value, such as human happiness or human dignity, to which all other values can be related or even reduced; a doctrine known as value monism. Here, I assume that the opposite thesis of value pluralism is true; i.e. there exists a variety of values which cannot be reduced to each other (Mason 2018).

A next question that arises is whether there is a limit to the number of values we can discern or whether it is in principle always possible to discern additional values. One reason to think that there is no limit to the number of values we can discern is that we can almost always make values more specific. For example, starting from the very general and abstract value of security, we can distinguish between individual and collective security. Next, individual security can be further divided between, for example, physical and psychological individual security. This process can go on for quite a while. We might even want to argue that the value of security of person X is not exactly the same value as the security of person Y. In other words, if we zoom in on specific values, and on the specific contexts in which we use value terms, it seems we could almost endlessly discern more specific values.

My aim in this contribution is to discern and analyse the core values in cybersecurity. This is, by its nature, an exercise on a rather general and abstract level. The goal is to come to a set of general values that may require further specification when applying them in specific contexts but that nevertheless provide some insight into the moral concerns and problems that might arise in relation to cybersecurity. However, even at this general level, we might distinguish a large number of different values. For example, in the literature study we conducted for the CANVAS project[1] we found a large number of value terms in the domains of health, business and national security in relation to cybersecurity (Yaghmaei et al. 2017).

[1] See https://canvas-project.eu/canvas/

To create more order in this multiplicity of relevant values, I propose introducing the notion of 'value cluster'. A value cluster is a range of values that express somewhat similar moral concerns. In line with the above-proposed characterisation of values, values in a value cluster correspond to similar moral reasons for action, or to similar norms. Moreover, the values that are part of one value cluster are typically articulated in response to somewhat similar morally problematic situations. It should be stressed that I use the notion of value cluster here relative to a particular domain or societal activity. In this case, the domain is cybersecurity and the value clusters I distinguish are defined in relation to cybersecurity.

3.3 Value Clusters in Cybersecurity

A first value cluster in relation to cybersecurity is that of *security*. Security can be understood in a number of more specific ways, pinpointing different more specific values that are part of this cluster, such as individual security or national security. In this cluster, I also locate the value of cybersecurity and a range of values closely related, or instrumental, to cybersecurity such as information security, and the confidentiality, integrity and availability of (computer) data. The main reasons to which this value cluster corresponds are the protection of humans and other valuable entities against all kinds of harm. The values in this cluster may be seen as a response to morally problematic situations in which harm is (potentially) done, ranging from data breaches and loss of data integrity to cybercrime and cyberwarfare.

A second relevant value cluster is *privacy*. This cluster contains, in addition to privacy, such values as moral autonomy, human dignity, identity, personhood, liberty, anonymity and confidentiality. Values in this cluster correspond to reasons (and norms), for example we should treat others with dignity, we should respect people's moral autonomy, we should not store or share personal data without people's informed consent, and we should not use people (or data about them) as a means to an end. Typically morally problematic situations to which these values are a response include the secret collection of large amounts of personal data for cybersecurity purposes or the unauthorised transfer of personal data to a third party.

A third cluster is *fairness*. This consists of values such as justice, fairness, equality, accessibility, freedom from bias, non-discrimination, democracy and the protection of civil liberties. This cluster of values is a response to the fact that cybersecurity threats, or measures to avoid such threats, do not affect everyone equally, which may sometimes be morally unfair. Another type of moral problem is: These values are a response to the fact that cybersecurity threats, or measures to increase cybersecurity, may sometimes undermine democracy, or civil rights and liberties. Important moral reasons that correspond to this value cluster are that people should be treated fairly and equally, and that democratic and civil rights should be upheld.

The fourth and final value cluster I distinguish is that of *accountability*. Values in this cluster include transparency, openness and explainability. This value cluster is relevant because cybersecurity measures taken by, for example, governments can

potentially harm others, such as citizens, which requires accountability. Accountability, as a more procedural value, is particularly relevant because cybersecurity measures often require the weighing of a range of conflicting substantive values (such as security, privacy and fairness). Typical reasons to which the value of accountability is related include the obligation to account for one's actions but also being blamed for unjustified behaviour or paying damages, or a fine, for the harm that arises from unjustified behaviour.

In addition to the four value clusters, there are values connected to specific applications for which cybersecurity is an issue. These values are *domain-specific*. Examples are values such as health (in the medical domain) or national security. Although these values are different from domain to domain, and sometimes even from application to application, they are connected to a range of more instrumental or technical values related to the proper functioning of applications. I include here more specific values such as efficiency, ease of use, understandability, data availability, reliability, compatibility and connectivity. These technical values are nevertheless often morally relevant as they are frequently instrumental, if not essential, for achieving specific moral values.

3.3.1 Security

The first value cluster is that of security. Below, I propose a general conceptualisation of the value of security that indicates how cybersecurity can be seen as a specific kind of security, roughly understood as the state of computer systems being free from cyber threats. There are, however, many varieties of security, some of which are also directly relevant for the discussion about cybersecurity. These include, for example, personal or individual security but also national security, or the security of certain businesses (cf. Kleinig et al. 2011). It is important to realise that these different, more specific types of security often correspond to distinct values that may conflict with each other on occasion. Nevertheless, the various security values may be said to belong to one value cluster. This is the case not only because they all fit the same general conceptualisation of security, but also because they are all responses to similar morally problematic situations, i.e. situations in which something valuable is threatened by an external danger. Moreover, they also all correspond to similar moral reasons, i.e. moral reasons for protecting what is of value against an external threat or danger.

In very general terms, security may be understood as follows:

> *Security is the state of being free from danger or threat*

Often we speak about the security of a certain entity X from a specific type or kind of danger Y. In such cases, the following general characterisation seems to apply:

> *The security of X from Y is the state of an entity X being free from danger or threat of kind Y*

Here, X can refer to an individual agent, a person, but also to collective social entities such as an organization, a business or a state. X may also refer to a technical system, such as a computer system. Depending on X, we can thus distinguish more specific types of security such as personal security, national security and computer security.

Y can refer to specific types of danger or threat. For example, when we talk about personal physical security, Y refers to physical dangers or threats (to individuals). In the case of national security, Y may refer to, for example, terrorist attacks or an invasion by a foreign country, but nowadays also to (foreign) cyberattacks.

Two further remarks are necessary regarding this general characterisation. First, sometimes a distinction is made between the values of safety and security along the following lines: safety is protection against accidental or unintentional danger (e.g. a collapsing bridge or an earthquake), whereas security is protection against intended harm (e.g. theft or a terrorist attack) (Hansson 2009). The above characterisation does not follow this distinction but rather subsumes it under one general concept of security. This follows the conventional manner of discussing cybersecurity. For example, according to the 2016 EU scoping paper, "Cybersecurity refers to the protection of networks and information systems against human mistakes, natural disasters, technical failures or malicious attacks" (Scientific Advice Mechanism High Level Group 2016: 2). This includes, obviously, unintentional as well as intentional harm.

Second, this characterisation stresses the absence of danger or threat. We might argue that this is only part of the story as security—in particular personal or individual security—may also be understood as a certain peace of mind and the presence of preconditions in which people can live a meaningful and happy life (cf. Kleinig et al. 2011; Waldron 2011). Following the well-known distinction between negative and positive freedom (Berlin 1958), a similar distinction could perhaps be made between negative and positive security here.[2] For the current purpose, I adhere to the negative ("absence of") characterisation of security, as that seems most important when it comes to cybersecurity. Nevertheless, the positive aspect seems important for understanding the moral importance of the value of security in certain contexts, as we will see.

Now that we have a general characterisation of the value of security, we may inquire into the moral importance of this value. Philosophers often make a distinction between instrumental and intrinsic values (e.g. Frankena 1973). Instrumental values are merely valuable because they contribute to something that is valuable, whereas intrinsic values are believed to be good in themselves.[3] In the literature

[2] The positive connotation is, for example, also present in a notion such as food security, which does not primarily refer to the absence of danger or threat (famine) but rather to the availability of (enough) food. Similarly, we might understand cybersecurity as the presence of reliable computer and network infrastructure, although most current definitions stress the absence of, or protection against, certain dangers and threats.

[3] Intrinsic values are also sometimes called final or terminal values, while instrumental values are also sometimes called extrinsic. The different terminologies may not always trace the same distinction (cf. Korsgaard 1983).

review conducted for the CANVAS project, cybersecurity was in most cases described as an instrumental value (Yaghmaei et al. 2017). The reason for this seems quite obvious. Computer systems are not valuable in themselves but because of the functions they fulfil in society, or for individuals and groups, and because of the economic value they represent. Computer systems may also be used for bad purposes, and, in such cases, cybersecurity may even be deemed undesirable.

A value that is closely related to cybersecurity is information security. This value is often understood in terms of the confidentiality, integrity and availability of information. For example, according to the Information Systems Audit and Control Association (ISACA), information security "[e]nsures that … information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity), and non-access when required (availability)" (ISACA 2016). Confidentiality can be understood as being instrumental to privacy, as it prevents unauthorised access to information, which is often essential in maintaining privacy. The integrity and availability of information are instrumental for the (original) purpose of the information system by ensuring that required information is reliably available and accurate. This seems to suggest that information security is merely an instrumental value. Whereas cybersecurity may be more encompassing than information security—it may, for example, also relate to security from unauthorised access to cyberphysical systems (such as the energy grid or a water barrier)—the above seems to support the thesis that cybersecurity is mainly an instrumental value.

However, even if cybersecurity is an instrumental value, we should be careful in drawing too strong conclusions about its moral importance. If we consider, for example, cybersecurity threats to heart monitoring devices in hospitals or aviation systems then in both cases, a lack of cybersecurity may lead to a loss of human lives. In similar ways, cybersecurity is important for the protection of a large number of human and moral values. What these values are depends on the specific technical application and context. However, for some contexts, it would be a misunderstanding to think that cybersecurity is devoid of moral importance just because it is an instrumental value, as in those contexts cybersecurity may be a *sine qua non* for upholding other values with great moral importance, including values of personal security and health. As Dewey (1922) already highlighted in his criticism of the distinction between instrumental and intrinsic values, such distinctions tend to uncritically reify the gap between means and ends; what is a means in one context may well be an end in another (and vice versa).

Whereas cybersecurity is usually seen as instrumental value, several authors have argued that personal (or individual) security is an intrinsic value (e.g. Himma 2016). The main argument for this seems to be that without some degree of personal security, individual people do not have a life at all, let alone a meaningful and happy one. This appears to show that some degree of security is required for individuals to live a good life. However, it is not obvious that this is enough to make security an intrinsic value. We might also argue that it is merely an enabling value (Raz 2003); i.e. a value that is necessary for people to have a meaningful life and to acquire other values. The reason why security understood as the mere absence of threat may not be an intrinsic value is that a life that merely consists of the absence of threat seems

hardly worth living; it is only when people start to do other valuable things that such a life becomes worthwhile.

Whereas there are good reasons to think of personal security as an intrinsic or at least an enabling value, this is less clear from more collectivist notions of security such as national security or business and organisational security. These would seem to be instrumental values, as their moral importance is derived from how they help support other values such as personal security.[4] Moreover, discussions of national security may create a slippery slope, as it allows certain political groups the possibility to claim the moral importance of certain restrictive measures that in practice restrict individual values, including personal security, rather than support them. At the same time, it is clear that some degree of national security is required to ensure personal security. Nevertheless, collectivist notions of security such as national security seem to derive their moral importance from how they eventually impact the security, but also other values such as privacy or liberty, of individuals rather than being intrinsically valuable (cf. Waldron 2011).

3.3.2 Privacy

Privacy is generally seen as an important value in relation to cybersecurity. There is, however, no agreement on how exactly to understand and conceptualise the value of privacy (Moore 2003). Proposed understandings include such notions as "the right to be let alone" (Warren and Brandeis 1890), "informational control" (Westin 1967), an extension of personality and personhood (Pound 1915) and an act of self-care (Allen 2016). Privacy also has several dimensions. Koops et al. (2017) distinguish between bodily, intellectual, spatial, decisional, communicational, associational, proprietary and behavioural privacy and view informational privacy as crosscutting through these categories.

Where cybersecurity is concerned, privacy is usually understood in informational terms. Such informational privacy is about what information about a person is (not) known to, or shared with, others. A further distinction is between notions of privacy stressing the *confidentiality* or *secrecy* of data (and information) and those stressing *control* over what data (or information) is shared with whom. If the first understanding is adhered to, it might be best not to collect and store personal data in the first place to enhance privacy (Warnier et al. 2015). Obviously, that will often be neither possible nor desirable (for other reasons). According to the control conception of privacy, the collecting, storing and sharing of data is not always problematic, rather privacy is about giving people control over the collection, storage and sharing of their own personal data. Here, the notion of 'informed consent' is important. Informed consent means that the collecting, storing and sharing of personal data

[4] A similar stance has been taken by the approach to national and international security known as 'human security'; see e.g. Gregoratti (2013).

require the deliberate and informed consent of the data subject. People may thus also deliberately decide to share information about themselves with others. For both the confidentiality and the control notion, privacy breaches may result from unauthorised access to data and, in this sense, cybersecurity is instrumental, if not crucial, to protecting privacy.

What information is appropriate to share with whom may not only be dependent on the autonomous choices of individuals (as the control notion of privacy stresses) but also be different for various social spheres. The question of what is appropriate to share with an employer is different from what information can appropriately be shared with a physician or spouse. This idea is captured in the notion of privacy as contextual integrity (Nissenbaum 2004).

Some authors have argued that privacy is an intrinsic value, whereas others see it primarily as an instrumental one (e.g. Kleinig et al. 2011; Himma 2016). Those who tend to see it as an intrinsic value may point out that some degree of privacy is indispensable for (moral) autonomy. If one's thoughts and actions are continuously known to others, it will undermine one's capacity to decide and act in a morally autonomous way. Since moral autonomy is crucial for human agency and human dignity, some minimal degree of privacy is required to live a good life. Those who conceive of privacy as an instrumental value may object that what is valued here is not so much privacy in itself but rather what it allows or enables. The relationship between privacy and the ability to live a morally worthwhile life may in this respect not be so different from that between personal security and a good life, as discussed before. We might therefore conceive of privacy as an enabling value, i.e. as a value that is necessary as a precondition for a good life, but one that is not necessarily itself intrinsically valuable; however it is also not a mere instrumental value in the sense that it cannot be replaced by others means and is indispensable for living a worthwhile life.

A somewhat related debate is the one between authors who adhere to reductionist accounts of privacy and those who provide non-reductionist accounts (Katell and Moore 2016). According to reductionist accounts, the moral importance of privacy is based on other values such as autonomy, human dignity and liberty. In the final analysis, there is nothing that the value of privacy adds to the relevant moral considerations and reasons that cannot already be derived from those others values. Privacy, in other words, is merely a placeholder for moral concerns that can already be derived from other values. Van den Hoven, for example, has argued that privacy derives its moral importance from four types of moral considerations: (1) prevention of information-based harm, (2) prevention of informational inequality, (3) prevention of informational injustice, and (4) respect for moral autonomy (Van den Hoven 1998; Van den Hoven and Vermaas 2007). Conversely, non-reductionists do not need to deny that privacy is related to a range of other values and part of a broader value cluster as I have called it, but they at least maintain that the value of privacy articulates moral considerations and corresponds to moral reasons that cannot, or at least cannot fully, be expressed by other values.

As Katell and Moore (2016) stress, even if reductionism about privacy were true, in many practical contexts it would still be useful to use the notion of privacy. After

all, many of the social and political debates about ICT technologies, including those on cybersecurity, are framed in terms of privacy. Nevertheless, it is often helpful to unpack the other values and reasons that are implied when the value of privacy is articulated in concrete situations and debates. This is so because it is frequently the case that what is at stake in such situations is not just the threat of unauthorised access to personal data but rather a range of broader moral concerns related to such values as autonomy, identity and liberty. This is one of the reasons why it is useful to think in terms of value clusters rather than individual values. As indicated before, the value cluster of privacy also contains such values as moral autonomy, human dignity, identity, personhood, liberty, anonymity and confidentiality. Some of the values have a more justificatory relationship to privacy, i.e. they articulate why privacy is morally important (such as moral autonomy, human dignity, identity, personhood and liberty), whereas others (such as anonymity, confidentiality and control) seem more instrumental for preserving privacy.

There is a mutual relationship between how privacy is exactly understood and conceptualised and what other values are (more closely) related to it. For example, Whitman (2004) argues that in the US context, privacy is merely understood (and laid down in laws) in relation to liberty and in particular to moral concerns about government infringements in the personal life sphere of citizens. Such conceptions of privacy tend to stress liberty and the protection of citizens against state actors. He contrasts this with the European, primarily French and German, tradition in which privacy is more closely linked to human dignity and that stresses the relationship between people, so that privacy is also a concern between individuals, or between individuals and companies, rather than between citizens and the state. Arguably, in the current age of information systems and big data, both conceptions are important when it comes to privacy concerns.

3.3.3 Fairness

The third value cluster relevant to cybersecurity is that of fairness. This is a relevant value because both cybersecurity threats and measures to increase cybersecurity impact people differently, which may raise fairness issues. This is connected to a range of other values such as equality, justice, non-discrimination and freedom from bias. In addition, democracy is a relevant value because some cybersecurity measures may be so consequential and invasive that they require democratic legitimation rather than being the authority of private actors such as companies.

In political and moral philosophy, many different notions and theories of both democracy and fairness have been developed. I refrain from delving here into all the subtleties but rather restrict myself to highlighting how these values are affected by cybersecurity concerns and how they are relevant for the institutional and technical design of cybersecurity measures.

Justice and fairness are important values because cybersecurity measures typically come with costs and benefits that may be unequally distributed across the vari-

ous actors involved. Parts of these costs and benefits are financial and economic in nature, and a first question that will therefore arise is whether a certain proposed cybersecurity measure is worth the cost. Strictly speaking, this is more a question about efficiency (i.e. the ratio between benefits and costs) than a question of justice and fairness (i.e. the distribution of costs and benefits). It should be noted, however, that if certain cybersecurity measures are not taken for efficiency reasons (i.e. because the benefits are not considered worth the costs), there will likely be distributional effects. This is the case because, if and when cybersecurity breaches materialise, the costs and harms caused by such breaches will likely not be equally distributed. Indeed, if people are victim to cybersecurity breaches, questions may arise about a right to compensation or the need for insurance.

The fact that costs and benefits are usually not equally distributed implies that even if from a societal point of view it is efficient or cost-effective to take certain cybersecurity measures, it is possible that for none of the actors involved are such measures also individually cost-effective. This may be particularly problematic if the distribution of costs and benefits is somehow unfair. An example is a company that offers services that are sensitive to cyber-attacks. As long as the costs (and other harm) due to the cyberattacks can be externalised (for example to the users of their services), it may not be cost-effective for the company to take certain cybersecurity measures. However, such externalisation of costs may be considered unfair, which in turn may lead to the introduction of a legal obligation (by the government) for the company to compensate its customers for damages due to avoidable cybersecurity breaches. This new distribution of costs and benefits may make certain cybersecurity measures cost-effective that were not so before. In this sense, questions about the cost-effectiveness of cybersecurity measures cannot be completely separated from questions about the fair or just distribution of costs and benefits.

Fairness and justice considerations do not only accrue to distributional effects but may also imply that people have a right to some minimal level of information access (Van den Hoven and Rooksby 2008) or even access to ICT services.[5] Given the crucial importance of information, and also of certain ICT services, in today's society, we may question whether access to such goods and services should not become a basic right. Perhaps, now or in the future, we should grant everybody the right to affordable, secure and accessible ICT services. If such rights were introduced, it would also have implications for the minimal level of cybersecurity that should be guaranteed for everybody. Of course, many questions can be asked regarding whether it is desirable to introduce such rights and about who bears the duties that correspond to such rights. Nevertheless, what these deliberations reveal is that questions about what constitutes a desirable level of cybersecurity do not just

[5] A report by special rapporteur Frank La Rue to the UN in 2011 stated: "Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy (…) to make the Internet widely available, accessible and affordable to all segments of population" (Rue 2011: 22). This was interpreted by some as a plea for Internet access as a human right.

concern efficiency and cost-effectiveness but also fairness, justice and perhaps even human rights.

Fairness and justice may require impartiality but they would not seem to require that people are always or necessarily treated equally (Miller 2017). In most theories of fairness or justice, it is allowed, and sometimes even required, to treat people differently if they somehow deserve different treatment. What factors are relevant in justifying (or requiring) different treatments may be different for different theories and accounts. Nevertheless, some factors are almost universally seen as constituting improper ground for different treatments. This includes such factors as race, gender and sexual preferences. Here, the value of non-discrimination is relevant.[6]

Non-discrimination may be a particularly important value for cybersecurity because it is known that ICT technologies may be vulnerable to bias, i.e. they may unjustifiably treat people differently on the basis of, for example, gender, race or marital status. Such bias may be intentional, but it is often the unintended result of how such systems are designed and used. Friedman and Nissenbaum (1996) discuss three sources of such bias, namely pre-existing bias in human practices, institutions, and attitudes that is reified in computer systems; technical bias (resulting from technical requirements and constraints); and emergent bias that emerges from the use of the system (e.g. use in another context than originally foreseen). The increased use of big data and of self-learning algorithms has further increased the problem of bias (Barocas and Selbst 2016; O'Neil 2016; Ferguson 2017). Algorithmic bias may, in particular, result when algorithms are trained with biased data sets, or on a limited group of people or cases. Large-scale data collection for cybersecurity, therefore, is likely to also be vulnerable to bias if non-discrimination is not from the start considered in the design, training and use of relevant algorithms.

The value of democracy is relevant to cybersecurity in a number of ways. Cyberattacks may undermine the democratic process, as suggested by the 2016 US president elections, which witnessed the hacking of the Democratic Party, trolling and the spread of fake news (see also Chap. 11). It has also been suggested that cybersecurity measures, such as end-to-end-encryption, may protect democratic liberties such as freedom of speech (cf. Christen et al. 2017). However, cybersecurity measures may occasionally also undermine democracy. A particular concern is the strategic use of cybersecurity by national governments for national security aims (see also Chap. 12). Although such use may be justified, it raises a number of concerns (Kleinig et al. 2011; Newell 2016; Rubel 2016; Strossen 2016). One is that it may undermine the civil liberties of citizens. Second, because such use is by its nature often secretive, there may be a lack of democratic legitimacy. A further concern is that government agencies that find cybersecurity weaknesses may strategically keep these secret in order to use them against other countries (or even against their own population). This is not only problematic because such use usually lacks democratic legitimation but also because it increases cybersecurity risks for citizens

[6] However, positive discrimination would seem warranted in some cases, as justice may require advantaging underprivileged groups in specific circumstances.

and companies. It thus leads to fairness concerns because these societal actors have to bear the burden of the costs of cybersecurity threats that have not been revealed by government agencies.

3.3.4 Accountability

The value of accountability (and related values such as transparency, openness and explainability) is particularly relevant to cybersecurity in two types of situations. One are situations in which someone (allegedly) harms someone else, or infringes on the rights of that person. In such situations, we typically hold the (alleged) perpetrator accountable. The other are situations in which there is a power imbalance between two agents and in which the more powerful is in the position to introduce rules or measures that may harm the less powerful ones. For example, governments and companies may be accountable to citizens and consumers for what cybersecurity measures they take even if there is not (yet) a suspicion of undue harm.

In the first type of situation, accountability is closely related to responsibility and its different meanings, such as blameworthiness, liability and obligation-responsibility (Van de Poel et al. 2015). An agent may be said to be accountable if there is a reasonable suspicion that that agent did something wrong or caused undue harm. Accountability here implies an obligation to account for one's actions and their consequences. Such an account may show that the agent is not blameworthy (despite the reasonable suspicion), but if the account is unsatisfactory, the agent may be blameworthy or liable to correct his or her wrong or to pay damages. Accountability is also related to responsibility-as-obligation; in particular, an agent may be accountable if there is a reasonable suspicion that it did not fill its obligation-responsibilities.

What sets the second type of situation apart from the first is that there is not (yet) a reasonable suspicion of wrongdoing. Rather, the need for accountability is based on power imbalances. Although such power imbalances exist in any society, they seem to be aggravated in today's information society by the unequal access to large amounts of data and information. Moreover, citizens and consumers seem increasingly dependent on government and large commercial organisations for the secure storage of (personal) data. This would seem to imply that such powerful organisations are accountable for what cybersecurity measures they take. Such accountability would imply some degree of transparency about what cybersecurity measures are taken. In addition to such transparency, it would also imply a willingness and ability to account for the decisions on which such measures are based. This is particularly important because cybersecurity involves a range of values that are potentially conflicting. There might not be one best way to reconcile these values or to strike a balance between them, which makes it even more important that powerful actors account for how they make such decisions. Accountability here implies a certain traceability of how decisions are made but also the articulation of the reasons and motivations underlying such decisions.

3.4 Value Conflicts in Cybersecurity

It is often said that some of the values relevant to cybersecurity are in conflict with each other. The most frequently mentioned conflict is that between security and privacy, but this is certainly not the only possible value conflict in the domain of cybersecurity. Moreover, as already indicated in the introduction, it is not the case that (cyber)security and privacy are always in conflict.

3.4.1 What Are Value Conflicts?

What does it mean to say that two values are conflicting? If values are varieties of goodness and are used for (moral) evaluation, then one interpretation of a value conflict is that two (or more) values are conflicting if (and only if) they provide opposite or contradictory evaluations of the same state-of-affairs (or object or policy). Therefore, if something is evaluated as good on the basis of one of the values it should, by definition, be bad on the basis of the other value. In cybersecurity, the values of transparency (or openness) versus confidentiality may provide an example. What is transparent is not confidential, and vice versa.

Such value conflicts that seem to derive from oppositions at the semantic level of values are, however, relatively rare. More often, value conflicts seem to derive from the practical implications of values. Under this interpretation, values conflict if they express or correspond to contradictory norms or reasons for actions. For example, if a value such as privacy would require that a certain piece of information is kept confidential, whereas transparency would require that same piece of information to be made public, then the values of privacy and transparency are conflicting.

It should be noted that the question of to which reasons a value corresponds is one of interpretation and judgment, and depends both on the value at stake and the specific context (see Sect. 3.2.1). More specifically, it depends on how the values at stake are conceptualised and specified. Conceptualisation is "the providing of a definition, analysis or description of a value that clarifies its meaning and often its applicability" (Van de Poel 2013: 261). For example, privacy may be conceptualised in terms of *confidentiality* as well as in terms of *control* over information. On the second conceptualisation, it would seem less likely that privacy conflicts with transparency, although it is certainly not impossible.

Moreover, whether values conflict will also depend on their specification. Specification may be understood as the translation of values into more specific norms and requirements (Van de Poel 2013). If privacy is conceptualised in terms of confidentiality, a specification would further specify what (personal) information should exactly stay confidential, and to whom. This means that on some specifications of privacy as confidentiality, privacy and transparency would conflict whereas on other specifications, the values would not conflict. Of course, there are limits to how a value can be specified. In general, a specification may be considered adequate

if meeting the more specific norms and requirements would count as a proper response to the value at stake (cf. the earlier discussion about values in Sect. 3.2.1).

With the above in mind, we can now more precisely define value conflicts. One possible definition is the following:

> *Values are conflicting for a particular X, in context C, if it is practically impossible to respond properly to all values that are relevant to X in context C simultaneously*

Here X can be a state-of-affairs but also (and more relevant to the current discussion) a certain (technical or institutional) cybersecurity measure. This definition would also allow value conflicts if there is only one value, because it may also be practically impossible to respond properly to that one value for that particular X. For example, for a particular cybersecurity policy it may turn out to be impossible to respect (which is a proper response) the value of privacy.

If X is a cybersecurity policy (or measure), the natural response to such value conflicts may be to look for another policy, or measure, that does properly respond to all relevant values. Van den Hoven, Lokhorst, and Van de Poel (2012) argue that in such situations of value conflict (or a moral dilemma), there is a second-order obligation to look for options that help to avoid the value conflict, now or in the future. This may be done through technical or institutional innovation or design, as such innovation or design may extend what is feasible and so allow options that overcome the initial value conflict (Van den Hoven 2013; Van de Poel 2017).

Nevertheless, sometimes it may turn out to be impossible to find options that allow all relevant values to be responded to in an appropriate way. This bring us to the final definition of value conflicts. This definition takes as a starting point the situation in which we need to choose between different options (such as different cybersecurity measures or policies) and in which none of the options seem best in light of all the values at stake. This results in the following definition of value conflict (Van de Poel and Royakkers 2011):

1. *A choice has to be made between at least two options for which at least two values are relevant as choice criteria.*
2. *At least two different values select at least two different options as best.*
3. *There is no single value that trumps all others as choice criterion. If one value trumps another, any (small) amount of the first value is worth more than any (large) amount of the second value.*

It is this type of value conflict that I focus on in the remainder.

3.4.2 Value Conflicts in Cybersecurity

I now examine a number of more specific value conflicts in cybersecurity. Since value conflicts are usually practical conflicts, whether two values are conflicting will depend on the specific context. Nevertheless, it is possible to distinguish a num-

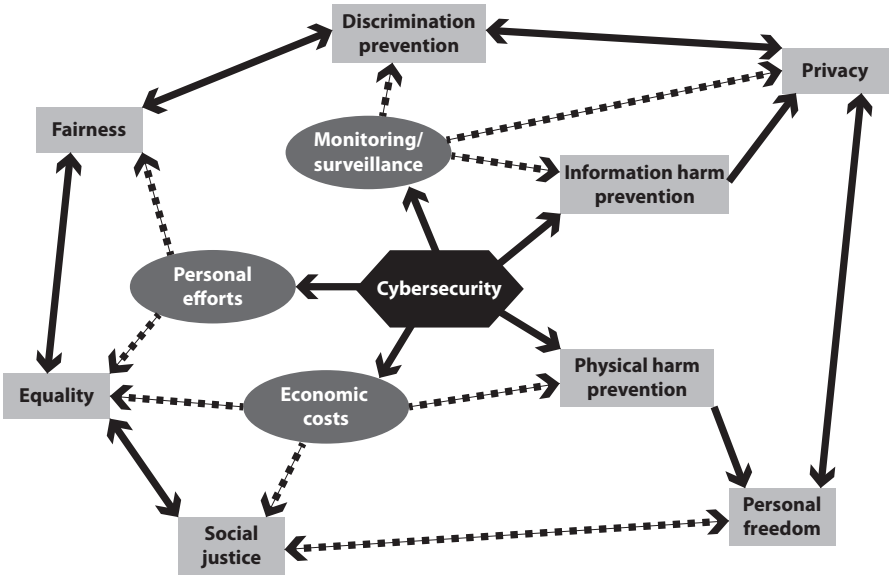

Fig. 3.1 Value tensions in cybersecurity. (Reproduced from Christen et al. 2017)

ber of more general value tensions in cybersecurity. Christen et al. (2017) present the following figure as a graphical representation of potential value conflicts in cybersecurity.

The grey rectangles in Fig. 3.1 represent values. The values of 'information harm prevention' and 'physical harm prevention' belong to the cluster of security I previously discussed; privacy and personal freedom belong do the privacy cluster; and discrimination prevention, fairness, equality and social justice belong to the fairness cluster. Accountability is not mentioned in the figure, which may be explained by the fact that this is more of a procedural value.

Full arrows represent a supporting or reinforcing relation, while dotted arrows represent potential tensions. As shown, cybersecurity is directly instrumental for harm prevention (and so for personal security). It may, however, also involve monitoring and surveillance, which may in turn negatively affect a number of values. Similarly, it involves personal efforts as well as economic costs that may also negatively affect a number of values.

Below, I discuss relations between value clusters, taking the four earlier distinguished value clusters as a starting point. For each relation between value clusters, I discuss whether it is largely supportive or conflicting (or can be both), and if there are conflicts, I discuss ways in which these conflicts may be approached.

3.4.2.1 Privacy Versus Security

The most frequently mentioned conflict in cybersecurity is most likely that between privacy and security. However, closer examination shows that the relationship between security and privacy is much more complex. Consider the following cases[7]:

1. Sometimes security is attained at the cost of privacy. An example is full cable monitoring which contributes to (cyber)security but would seem (in most cases) an unjustified privacy intrusion.
2. Sometimes security helps to achieve privacy. For example, limited or targeted monitoring may help to detect security incidents, which in turn may prevent data leaks, so that the confidentiality of personal information is maintained and, hence, privacy is served.
3. In computer systems, privacy requires some degree of cybersecurity. Privacy sets limits on who has access to what (personal) information. Without some degree of cybersecurity, these limits cannot be maintained, and personal information is subject to unauthorised access.
4. Sometimes, privacy is attained at the cost of security. For example, complete anonymity and secrecy of communications can be exploited by malicious agents.
5. Sometimes, privacy contributes to security. For example, if certain information about users of a system is kept confidential, spear phishing attacks can no longer leverage excessive available user information to choose attack targets.

As these examples demonstrate, security and privacy are not necessarily conflicting but also can support each other. Some degree of cybersecurity is, moreover, required to guarantee privacy. Nevertheless, the question can be asked how we are to deal with those situations in which privacy and security are conflicting.

In the philosophical literature, some authors have argued that security trumps privacy, while others have held that privacy trumps security. Himma (2016), for example, argues the former. His argument is based on the assumption that (personal) security is much more indispensable for a worthwhile life (including values such as autonomy and freedom) than privacy, because without some degree of security, we may not have a life at all. He admits, however, that this does not mean that any amount of security increase (however small) can justify any amount of privacy loss (however large).[8]

Conversely, Moore (2016) argues that privacy and accountability trump privacy. He does so by debunking four often-used arguments for sacrificing some privacy (or accountability) for security. These (fallacious) arguments are (1) "just trust us", i.e. give the benefit of the doubt to those in power and assume that officials will not override individual rights without just cause, (2) the nothing to hide argument, (3)

[7] These examples are based on a presentation by Josep Domingo-Ferrer on the 26th of April 2018 in Brussels concerning the CANVAS white paper on Technological challenges to cybersecurity (Domingo-Ferrer et al. 2017). See also Chap. 13.

[8] On this basis, one might wonder whether the point he makes is really about trumping values, or more about the centrality of certain values for a good or worthwhile life.

The "security trumps" view, and (4) the consent argument, i.e. people voluntarily offer (private) information all the time. While his debunking of the four arguments is convincing, it is questionable whether it follows that privacy (and accountability) trump security, in the sense that no amount of privacy or accountability should be given up to achieve more security.

The problem with trumping arguments is that they discuss value conflicts at a too general level. What values require in a specific situation, and whether values are conflicting, always requires judgement in the specific context (see also Chap. 7). Moreover, it seems very unlikely that either security trumps privacy or privacy trumps security in all possible situations one can imagine (or cannot yet imagine for that matter). Trumping accounts, then, are not able to do justice to how the value of privacy and security play out in specific situations and, therefore, offer an inadequate response to cases of value conflict.

The question, then, remains: how are we to deal with those situations in which the conflict between privacy and security is real? Although this may always require context-specific judgments, the earlier presented examples suggest a somewhat more general approach to the conflict between privacy and security. What we see from these examples is that conflicts in particular arise in two types of situations:

1. All data are gathered or monitored (as in the case of full cable monitoring) so that security is achieved at the cost of privacy
2. No data is gathered or monitored (as in the case of complete anonymity or secrecy) so that privacy is achieved at the cost of security

This suggests that, at least in a practical sense, the conflict boils down to conflicting requirements that follow from the values of security and privacy regarding what data should be collected, stored and shared, and for what purpose. This means that in looking for potential solutions to the value conflict, we should put centre stage questions such as:

– How much data and what data need to be gathered?
– What data should be accessible to whom?
– For how long should these data be stored?

It should also be noted that on a control account of privacy, it is entirely conceivable that individuals consent to the monitoring (and temporary storage) of their data for cybersecurity ends. After all, individuals will value their personal security and this will require some degree of cybersecurity. Therefore, if privacy is understood in control terms rather than confidentiality terms, it may be easier to solve the conflict between privacy and cybersecurity. Another notion that may be important in answering the mentioned questions is contextual integrity. The information that can be properly monitored and gathered in the light of privacy concerns will be different for different spheres in society such as business, health care, insurance, personal life and politics.

One of the implications of this is that to properly deal with the potential conflict between privacy and (cyber)security, we need fine-grained technical and institutional infrastructure that enables the fine-tuning of the data that are monitored, gath-

ered, stored, and shared to the different public spheres and the informed consent of individuals. This allows a sophisticated attuning of privacy and security concerns to the specific context, considering all the relevant value considerations.

3.4.2.2 Privacy Versus Fairness

The relationship between privacy and fairness is often seen as supportive. There are at least two general arguments for why privacy supports fairness. One is that privacy limits what data can be collected about individuals, which can prevent unfair treatment. If, for example, no data about race are collected, it limits the possibilities for discrimination or algorithmic bias based on race.[9] Secondly, it may be argued that some degree of privacy for office holders and political representatives is required in a well-functioning democracy (cf. Lever 2016; Mokrosinska 2016). One reason for this is that otherwise, some private circumstances may be held against political representatives or office holders that endanger their proper and independent functioning, which is required in a democracy. They may, for example, be blackmailed, which may introduce conflicts of interest and forms of secrecy that undermine the democratic process.

Conversely, democracy is supportive of privacy because privacy is often considered a civil liberty or basic right in democratic societies (see also Chaps. 4 and 5). Most democratic countries have laws that protect the privacy of their citizens.

Nevertheless, on occasion, fairness and democracy may also conflict with privacy. Fairness, for example, may require the sharing of some information with the government, in particular in those cases where fairness requires that people are not treated exactly the same. For example, fair taxation may require information about people's income, information that some people may consider private. Conflicts may also occur in cases where democracy seems to require a certain transparency or openness regarding how governmental decisions are made and what the government does (e.g. in terms of surveillance) (cf. Mathiesen 2016). Such transparency or openness may be in conflict (at least at first sight) with the confidentiality requirements that follow from privacy concerns. Since the call for transparency and openness of government operations is often based on considerations of accountability, I first discuss the relationship between privacy and accountability before discussing potential methods for addressing this value conflict.

[9] It does not make it entirely impossible, however. The reason is that discrimination or bias may also be based on proxies. For example, discrimination based on postal codes may in effect be a form of discrimination based on race or income (due to geographical segregation).

3.4.2.3 Privacy Versus Accountability

Privacy and accountability, at first sight, seem to be at tension with each other. Accountability requires the ability and willingness to account for one's actions, in particular for how and why certain decisions were made. This require a certain transparency, and the revelation of information that may be privacy-sensitive.

It should be noted that this tension does not just occur if privacy is understood in terms of confidentiality. In addition, regarding the control notion of privacy, an agent may prefer not to share certain information that is required for proper accountability. An agent may even strategically choose not to reveal certain information to evade accountability under the guise of privacy concerns. Under such circumstances, privacy may even become a means for offenders or criminals (including cyber criminals or cyber attackers) to avoid accountability and responsibility (and hence punishment).

This suggests that control conceptualisations of privacy that give full and unlimited control to individuals regarding what data and information they share with whom are problematic in terms of accountability. One way to address this may be to build in restrictions on what information individuals can reasonably decide not to share with others. It could be argued that a control notion of privacy should be grounded not in absolute liberty but in moral autonomy (and human dignity). Moral autonomy not only implies a certain freedom in shaping one's life but also the willingness to take responsibility for one's actions, and to account to others where that is warranted. If privacy as control is understood in such a way, the conflict with accountability is softened (although, perhaps, not completely avoided).

More generally, dealing with the potential conflict between privacy and accountability would require focusing on what information should be shared (or not be shared) with whom. Accountability does not require the disclosure of all information but rather those pieces of information that are crucial in the light of accountability. Moreover, accountability may require the disclosure of some information to some people but not to others. These requirements need not be in conflict with privacy, as privacy also typically does not require that all (personal) information remains confidential.

For example, political accountability may require that it becomes known who made what decision based on what information and which considerations went into a decision, but it does typically not require disclosure of other personal information. In some situations, it may even be irrelevant who exactly decided what for political accountability, and it may be enough to disclose how a decision was made in terms that are more general. Moreover, as we have seen before, political accountability may be served by some degree of privacy, because this avoids office holders or political representatives being held accountable for things that are private and not politically relevant.

The above does not rule out the fact that privacy and accountability may, on occasion, correspond to conflicting requirements about what information to disclose (or keep confidential) to whom. Such conflicts can, of course, occur. Nevertheless, it brings the discussion to where it should be, namely regarding what information

should be shared and what should be kept confidential to whom in the light of privacy and accountability concerns, and indeed other values such as democracy, fairness and security.

3.4.2.4 Security Versus Accountability

I have argued before that (cyber)security measures, or the lack thereof, require some form of accountability. This is the case because a lack of appropriate cybersecurity measures may create undue harm. However, in as far as accountability requires a revelation of what cybersecurity measures are exactly taken, it may be in conflict with cybersecurity itself. The reason for this is that cybersecurity threats often arise not just from unintentional harm but from the actions of malicious agents or adversaries. These agents will typically strategically adapt their adversary strategies to what cybersecurity measures are taken (or the lack thereof). In this sense, cybersecurity is akin to an arms race, meaning that too much public accountability may undermine the effectiveness of cybersecurity measures.

A similar conflict may occur in those cases where cybersecurity weaknesses are exploited for national security ends. Here again, the revelation of these security strategies, or even of the cybersecurity weaknesses on which they are based, may undermine the effectiveness of those strategies and hence decrease security. Therefore, there seems to be a very real tension between accountability and security.

While this tension may require some form of balancing or trade-off, there are also institutional mechanisms that may help to alleviate the tension. One such institutional mechanism is to create fora for accountability that do not require the full public disclosure of (cyber)security measures, for example, parliamentary committees, cybersecurity committees or councils to which governments, or companies, are accountable for the cybersecurity measures they take (or fail to take). Such institutions may work under certain confidentiality requirements in the sense that they cannot disclose certain cybersecurity measures (or the lack thereof) if that is likely to help cyber attackers or criminals.

These types of institutional mechanisms may still imply a trade-off between accountability and security as they are likely to neither attain full accountability nor full security. The main point, nevertheless, is that the tension between accountability and security should be an incentive to look for new institutional arrangements that allow both values to be better served simultaneously than current institutions. In as far as trade-offs are still inevitable, they should not only be considered in terms of security versus accountability but also in terms of the other values at stake, including the values of privacy and fairness and the values served by the computer systems that are the possible target of cyberattacks.

3.4.2.5 Security Versus Fairness (and Democracy)

Security may conflict with fairness and democracy, in particular when cybersecurity is used for national security aims, for example large state surveillance programmes or cyberattacks on other countries by government agencies. Such activities may put at risk civil liberties and the privacy of citizens (e.g. Rubel 2016; Strossen 2016). This may sometimes be justified but would then require at least some form of democratic legitimacy and accountability. However, the fact that these activities are often secretive makes democratic legitimation and accountability frequently more difficult to achieve.

It is important here to distinguish between different kinds of security, in particular national versus personal security (Kleinig et al. 2011; Waldron 2011). National security should not be seen as an intrinsic value but rather as a value that derives its moral importance from other values such as personal security. It is important to be aware that some measures to increase national security, such as the secretive large-scale surveillance of citizens, may not only serve personal security (through increasing national security) but also endanger it. In particular, if such programmes, in effect, diminish civil liberties without clear democratic legitimacy and a lack of accountability, the loss in personal security may occasionally be bigger than the net gain through increased national security.

This is not to deny that national security is a legitimate concern; arguably, it may require more attention than in the past in the light of an increase in the number of terrorist attacks (at least in Western countries) and an increase in foreign cyberattacks by state agencies (and others). The point is that in addressing conflicts of security versus fairness and democracy, we should not just examine national security but primarily examine the effect on personal security (of citizens).

One particular issue here is that national security measures, and also other types of cybersecurity measures, may well increase the personal security of some while diminishing the personal security (and civil liberties and privacy) of others (Waldron 2011). In other words, such measures have distributive effects that raise questions of fairness. As argued before, it can often be difficult to neatly separate such fairness questions from questions about the right level of (cyber)security that is still worth the costs involved (financial and otherwise).

It might be thought that fairness requires equal treatment and therefore translates into an equal distribution of the costs and benefits of cybersecurity. However, this is far less obvious than may appear. People are not to the same degree vulnerable to cyber threats so that benefits of cybersecurity measures are likely to be unequally distributed. Moreover, it seems just (or fair) that people or organisations that (deliberately) exploit weaknesses in cybersecurity at the cost of others should also bear a larger burden of the costs, if only to compensate for the harm they have done. Another consideration is that in order to increase the total level of (cyber)security we should sometimes be willing to accept some inequalities.

Therefore, although unequal distributions of the costs and benefits of cybersecurity, or national security, are not necessarily or always unfair (or unacceptable), fairness requires that some minimal level of basic rights, including a certain right to

personal security, civil liberties and privacy protection, is guaranteed for all (Rawls 1999 [1971]). This again underlines the fact that in considering value tensions between security and other values (privacy, accountability, democracy), we should always and primarily keep in mind the effect of different choices on personal security rather than simply focusing on national security and cybersecurity (which are largely instrumental values). Moreover, to guarantee some minimal degree of personal security for all, we must also pay attention to privacy, civil liberties and democratic rights.

3.5 Conclusions: Beyond Security Versus Privacy

I began this chapter by stating that the framing of ethical and value issues in cybersecurity in terms of security versus privacy is unsatisfactory. In concluding, I wish to highlight three ways in which we should go beyond this framing if the approach in this chapter is on the right track.

First, we should consider a broader range of values. In particular, I have pointed out that in addition to the value clusters of security and privacy, there are two other values clusters particularly important for cybersecurity, namely fairness and accountability. Moreover, there are those values that are related to cybersecurity in more specific domains (or applications), such as the business domain (Chap. 6), the health domain (Chap. 7) or the national security domain (Chap. 8). These values are also indispensable in understanding value issues and value tensions in relation to cybersecurity. By considering all these values, we gain a much richer picture of both the value issues and conflicts in cybersecurity.

Second, I have argued for a contextual approach when it comes to identifying and addressing value conflicts. This is in line with my general understanding of values as varieties of goodness that require an appropriate response and correspond to certain types of moral considerations and reasons. The question of what constitutes a proper response to a certain value is context-specific and always requires judgement. A value analysis of cybersecurity, therefore, requires contextual judgements. Moreover, values are usually not conflicting in the abstract, but in a specific context. Privacy and security, for example, conflict in some contexts and applications but not in others. Without a proper analysis of context, we are in danger of understanding value conflicts in cybersecurity in too general terms, for example as a conflict between privacy and security, which may hinder rather than help in better addressing such value conflicts.

To better address value conflicts in cybersecurity, then, requires a superior understanding of what is at stake in those conflicts. This not only requires an understanding of what specific values require in a specific situation but also an understanding of why and how values may conflict or support each other. I have discussed this in more general terms for a number of potential value conflicts in cybersecurity. It became apparent that a crucial issue in several of these potential conflicts is what data or information should be monitored, collected, stored and shared for what

purposes, and who is entitled to access such data. Attaining more precision about this type of question would be, at the very least, a step towards alleviating conflicts between, in particular, security, privacy and accountability. In other words, we should zoom in on what the various relevant values require in a specific situation and how these requirements can be reconciled, for example through technical and institutional solutions rather than very general philosophical arguments about why security trumps privacy or vice versa.

Acknowledgements This chapter was written as part of the CANVAS project, which received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 700540. Part of the research for this chapter was also done for the project ValueChange, which has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 788321.

References

Allen AL (2016) The duty to protect your own privacy. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 19–18

Anderson E (1993) Value in ethics and economics. Harvard University Press, Cambridge, MA

Barocas S, Selbst AD (2016) Big data's disparate impact. Calif Law Rev 104:671–732

Berlin I (1958) Two concepts of liberty. Clarendon Press, Oxford

Christen M, Gordijn B, Weber K et al (2017) A review of value-conflicts in cybersecurity. ORBIT J 1. https://doi.org/10.29297/orbit.v1i1.28

Dancy J (1993) Moral reasons. Blackwell Publishers, Oxford

Dancy J (2005) Should we pass the buck? In: Rønnow-Rasmussen T, Zimmerman MJ (eds) Recent work on intrinsic value. Springer, Dordrecht, pp 33–44

Dewey J (1922) Human nature and conduct; an introduction to social psychology. Holt, New York

Ferguson AG (2017) The rise of big data policing: surveillance, race, and the future of law enforcement. New York University Press, New York

Frankena WK (1973) Ethics, 2nd edn. Prentice Hall, Englewood Cliffs

Friedman B, Nissenbaum H (1996) Bias in computer systems. ACM Trans Inf Syst 14:330–347

Gregoratti C (2013) Human security. In*:* Encyclopædia Britannica. https://www.britannica.com/topic/human-security. Last access 7 July 2019

Hansson SO (2009) Risk and safety in technology. In: Meijers A (ed) Handbook of the philosophy of science. Volume 9: Philosophy of technology and engineering sciences. Elsevier, Oxford, pp 1069–1102

Himma KE (2016) Why security trumps privacy. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 145–170

Hirose I, Olson J (2015) The Oxford handbook of value theory. Oxford University Press, New York

ISACA (2016) Cybersecurity fundamentals glossary 2016. https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf. Last access 7 July 2019

Domingo-Ferrer D-F, Blanco A, Arnau JP et al (2017) Canvas White Paper 4 – technological challenges in cybersecurity. SSRN. https://doi.org/10.2139/ssrn.3091942

Katell M, Moore AD (2016) Introduction: the value of privacy, security and accountability. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 1–17
Kleinig J, Mameli P, Miller S et al (2011) Security and privacy: global standards for ethical identity management in contemporary liberal democratic states. ANU Press, Canberra
Koops B-J, Newell BC, Timan T et al (2017) A typology of privacy. Univ Penn J Nat Law 38:483–575
Korsgaard CM (1983) Two distinctions in goodness. Philos Rev 92:169–195
Lever A (2016) Democracy, privacy and security. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 105–124
Mason E (2018) Value pluralism. In: Zalta EN (ed) The Stanford encyclopedia of philosophy, Spring 2018 edn. https://plato.stanford.edu/archives/spr2018/entries/value-pluralism/. Last access 7 July 2019
Mathiesen K (2016) Transparancy for democracy: the case of open governmnet data. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 125–144
Miller D (2017) Justice. In: Zalta EN (ed) The Stanford encyclopedia of philosophy, Fall 2017 edn. https://plato.stanford.edu/archives/fall2017/entries/justice/. Last access 7 July 2019
Mokrosinska D (2016) Privacy, freedom of speech and the sexual lives of office holders. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 89–104
Moore AD (2003) Privacy: its meaning and value. Am Philos Q 40:215–227
Moore AD (2016) Why privacy and acountability trump security. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 171–182
Newell BC (2016) Mass surveillance, privacy and freedom: a case for public access to government surveillance information. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 203–222
Nissenbaum H (2004) Privacy as contextual integrity. Wash Law Rev 79:119–157
O'Neil C (2016) Weapons of math destruction: how big data increases inequality and threatens democracy, 1st edn. Crown, New York
Pound R (1915) Interests of personality. Harv Law Rev 28:343–365
Rawls J (1971) A theory of justice, Rev edn. (1999) The Belknap Press of Harvard University Press, Cambridge, MA
Raz J (1999) Engaging reason. On the theory of value and action. Oxford University Press, Oxford
Raz J (2003) The practice of value (with commentaries by Christine Korsgaard, Robert Pippin, & Bernard Williams; edited and introduced by R. Jay Wallace). Oxford University Press, Oxford
Rokeach M (1973) The nature of human values. The Free Press, New York
Rubel A (2016) Privacy, transpararency and accountablity in the NSA's bulk metadata program. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London, pp 183–202
Rue FL (2011) VI. Conclusions and recommendations. Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Last access 7 July 2019
Scanlon TM (1998) What we owe to each other. Harvard University Press, Cambridge, MA
Schwartz SH, Bilsky W (1987) Toward a universal psychological structure of human values. J Pers Soc Pyschol 53:550–562
Scientific Advice Mechanism High Level Group (2016) Scientific advice mechanism scoping paper. European Commission, Cybersecurity
Stocker M (1990) Plural and conflicting values. Clarendon Press, Oxford
Strossen N (2016) Post-9/11 government surveillance, supression and secrecy. In: Moore AD (ed) Privacy, security, and accountability: ethics, law and, policy. Rowman & Littlefield International, London/New York, pp 223–246

Van de Poel I (2013) Translating values into design requirements. In: Mitchfelder D, McCarty N, Goldberg DE (eds) Philosophy and engineering: Reflections on practice, principles and process. Dordrecht: Springer, 253–266.
Van de Poel I (2017) Dealing with moral dilemmas through design. In: van den Hoven J, Miller S, Pogge T (eds) Designing in ethics. Cambridge University Press, Cambridge, pp 57–77
Van de Poel I, Royakkers L (2011) Ethics, technology and engineering. Wiley-Blackwell, Oxford
Van de Poel I, Royakkers L, Zwart SD (2015) Moral responsibility and the problem of many hands. Routledge, New York
Van den Hoven J (1998) Privacy and the varieties of informational wrongdoing. Aus J Prof App Ethics 1:30–43
Van den Hoven J (2013) Value sensitive design and responsible innovation. In: Owen R, Bessant J, Heintz M (eds) Responsible innovation. Wiley, Chichester, pp 75–84
Van den Hoven J, Rooksby E (2008) Distributive justice and the value of information: a (broadly) Rawlsian approach. In: van den Joven MJ, Weckert J (eds) Information technology and moral philosophy. Cambridge University Press, Cambridge
Van den Hoven J, Vermaas PE (2007) Nano-technology and privacy: on continuous surveillance outside the panopticon. J Med Philos 32:283–297
Van den Hoven J, Lokhorst G-J, Van de Poel I (2012) Engineering and the problem of moral overload. Sci Eng Ethics 18:143–155
Von Wright GH (1963) The varieties of goodness. Routledge & Kegan Paul, London
Waldron JJ (2011) Safety and security. Neb Law Rev 85:454–507
Warnier M, Dechesne F, Brazier F (2015) Design for the value of privacy. In: van den Hoven J, Vermaas EP, van de Poel I (eds) Handbook of ethics, values, and technological design: sources, theory, values and application domains. Springer, Dordrecht, pp 431–445
Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4:193–220
Westin AF (1967) Privacy and freedom. Atheneum, New York
Whitman JK (2004) The two western cultures of privacy: dignity versus liberty. Yale Law J 113:1151–1221
Williams RM Jr (1968) The concept of values. In: Sills DS (ed) The concept of values. Macmillan Free Press, New York
Yaghmaei E, van de Poel I, Christen M et al (2017) Canvas White Paper 1 – cybersecurity and ethics. SSRN. https://doi.org/10.2139/ssrn.3091909