Whose responsibility is it anyway? Dealing with the consequences of new technologies

Vedder, A.H.; Custers, B.H.M.; Sollie P., Düwell M.

Chapter 3
Whose Responsibility Is It Anyway? Dealing with the Consequences of New Technologies

Anton Vedder and Bart Custers

Abstract The infrastructure of our information and communication networks is quickly developing. All over the world, researchers are successfully working on higher capacity data transmission and on connectivity enhancement. Traditional limitations of time, space and quantity are gradually loosing their grip on the availability and accessibility of information and communication. These developments will change the world for the better in many ways. They can, however, have drawbacks as well. These are primarily concerned with the societal impact of the broader use of the technologies after they have been introduced into the market. In this chapter, we ask in which stage of the process of designing, developing, producing and introducing into the market of the technology these consequences should be identified, and by whom this should be done. We also focus on the responsibilities for addressing and solving these drawbacks. In this latter part of the essay, we detach ourselves a little from the practical setting of fast and ubiquitous networks and address a recently often heard claim, i.e., that reflection on the social, moral and legal aspects of technology should primarily take place in the phase of development so that solutions of possible problems can be quasi built into the device. We take a critical stance towards this claim and argue that concern and care for the social, moral and legal aspects should take place during the whole process, by different parties to the extent of their specific capacities and possibilities.

Keywords Ethics of technology · Responsibility · Privacy · Security · Reliability · Equal access to information

3.1 Introduction

The infrastructure of our information and communication networks is quickly developing. All over the world, researchers are successfully working on higher capacity data transmission and on connectivity enhancement. Traditional limitations

A. Vedder (✉)
Tilburg Institute of Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

P. Sollie, M. Düwell (eds.), *Evaluating New Technologies*, The International Library of Ethics, Law and Technology 3, DOI 10.1007/978-90-481-2229-5_3,

of time, space and quantity are gradually loosing their grip on the availability and accessibility of information and communication. These developments will change the world for the better in many ways. They can, however, have drawbacks as well. These have to do with the quality of information, and the privacy, security, and accessibility of information and communication. They are primarily concerned with the societal impact of the broader use of the technologies after they have been introduced into the market. Subsequently, we will ask in which stage of the process of designing, developing, producing and introducing into the market of the technology these consequences should be identified, and by whom this should be done. Finally we will focus on the responsibilities for addressing and solving these drawbacks. In this latter part of the essay, we will detach ourselves a little from the practical setting of fast and ubiquitous networks. We will address a recently often heard claim, i.e., that reflection on the social, moral and legal aspects of technology should primarily take place in the phase of development so that solutions of possible problems can be quasi built into the device. We will take a critical stance towards this claim and argue that concern and care for the social, moral and legal aspects should take place during the whole process, by different parties to the extent of their specific capacities and possibilities.

3.2 Ultrafast Communication

Easy and fast network access is being realized in different ways. One way in which this is done, is by implementing high-capacity optical connections and flexible access to and in home networks. The use of a variety of wireless networks is rapidly growing. Examples are wireless local area networks, bluetooth and mobile telephony. The growth of both of these wireless networks and fibre-to-the-home connections will dramatically increase the need for more capacity in the wired part of the network. During the last decade, a vast amount of optical fibre cable has been installed in communication networks all over the world and even today new cables are laid at an astonishing rate. Especially the increasing number of fibre-to-the-home connections will put enormous pressure on the capacity of the upper hierarchy of long-distance networks. Most of the growth will be due to the expanding internet traffic.

In fact, these technological developments seem to be exponential. According to Moore's Law, the number of transistors on an integrated circuit (a "chip" or "microchip") for minimum component costs doubles every 24 months (Schaller, 1997). This more or less implies that storage capacity doubles every two years or that data storage costs are reduced by fifty percent every two years. This empirical observation by Gordon Moore was made in 1965; by now, this doubling speed is approximately 18 months. Moore's Law deals with storage capacities, but similar observations are made for communication speed and volume. According to Gilder's Law, the total bandwidth availability of US communication systems has tripled every twelve months since the 1980s and will expand at the same rate for the next 30 years to come (Raessens, 2001). Moore's Law is not only about making existing technologies more efficient. It also takes into account the new ideas and inventions in the field of information technology. The latest developments to increase the speed and volume of information transfer on communication networks are focused on changing from electronic communication to optical communication. This is likely to result in a significant increase in the speed and volume of information transfer on communication networks. This new type of communication is referred to as *ultrafast communication* (Miller, 2004).

Ultrafast communication networks are mainly based on optical communication. Without doubt, light has become the dominant medium for transmitting information. In fact, photonics is considered to be the most important key technology of this century, to such an extent that one might refer to the present century as that of the photon, just like last century was that of the electron.

A crucial element in every network is the communication node, a facility in which information packages are received, inspected, buffered, labeled, redistributed and sent out again. They are present in every network, and the demand for higher capacity and throughput will manifest itself first at the higher levels of the network hierarchy. Presently, these nodes are fully electronically operating. This means that incoming optical signals are converted into electronic signals, then electronically processed, i.e. identified, buffered and labeled, and finally converted back into optical signals and transmitted to the user or to a next node. The processing speed of one conventional electronically operating node is generally 1 Gbit/s, i.e. 10^9 data bits per second. This may seem incredibly fast, but one should realize that the transmission capacity of a single ordinary optical fibre transmission cable is generally more than 100 Tbit/s, more than 100,000 times higher capacity than one electronic node. This means that if the fiber links in a telecommunication network are used to their full potential, the communication nodes will become bottlenecks for fast processing and rerouting of the data packages. Congestion of the whole network will unavoidably happen, not to speak of the danger of data packages getting lost forever. The solution to this problem is to develop a sufficiently fast alternative technology for data processing, preferably at teraherz speed, on the basis of which new types of nodes can be constructed. The potential maximum bit rate for a telecommunication link is set by the above-mentioned optical bit transmission capacity of the glass fiber. In order to deal with this enormous capacity in the node and to avoid the previously mentioned congestion problem, it would be very logical to stay in the optical domain all the way and hence make the network nodes optical as well. This means that a basic ultrafast optical device technology should be developed which will make the realization of all types of functionalities possible, such as, buffering of data, header recognition, switching of packages and regeneration of pulses. These devices must allow digital processing functions to be performed on data signals while "on the fly" and never leaving the optical domain (Cotter et al., 1999).

The engineers working on these devices find themselves in a situation comparable to that of the microelectronical challenge for electronic information processing in the1960s. Knowing the basic components needed for realizing the necessary functionalities, the challenge then was to realize microelectronical building blocks that could be integrated onto one single electronic chip device. We all realize now that this development led to a revolution in electronic devices, ultimately bringing fast electronical equipment within reach of the general public; the personal computer being the most remarkable example. The ambition of Photonics is to make all of this much faster, not only in transmission speeds but also in bit manipulations per second. At the same time, the photonic circuits should become less power consuming in order to create opportunities for personal applications in portable versatile communication devices or for personal electronic health care. Thus, light will influence our way of living to an extent we never could have imagined just a few decades ago. Photonics will play a crucial role—often the central role—in our daily life, notably in the ways we communicate and in the tools we use to explore the frontiers of science.

To realize the photonic ambition, one needs to find optical alternatives for each electronic building block, such as flips flops, gates, buffers, memories, shift registers, transistors etc. The information in electronics is normally present in the form of binary units or bits, simply on or off. This is less restrictive in the photonics domain, since here the possibility of different parallel wavelengths in adition to the binary information handling introduces per wavelength channel an enormous flexibility in the way the information is digitized, which introduces a lot more design possibilities.

In short, new technology is developed for all-optical ultrafast signal processing and handling. This will lead to all-optical ultrafast telecommunication nodes that can handle the full potential of the existing optical fiber transmission capacity. All-optical building blocks have been realized in concept and the first integrated device versions will soon be fabricated. This development will make telecommunication networks in general and the Internet in particular orders of magnitude faster.

3.3 Consequences

In this section we will focus on a number of possible drawbacks. We focus on quality and security of information and communication, privacy, public security, accessibility, and exclusivity. We will provide only an overview of these drawbacks here, since detailed discussions are beyond the scope of this contribution.[1]

3.3.1 Quality and Security of Information and Communication

The introduction of the Internet has brought about considerable changes in the ways in which people communicate and disseminate and gather information. Remarkably,

[1] For more detailed discussions we refer to earlier publications, e.g., for more on quality and reliability, see Vedder and Wachbroit (2003) and Vedder and Lenstra (2006). For more on the drawbacks regarding privacy and public security, see Custers (2008) and for more on the drawbacks on exclusivity and the digital divide, see Compaine (2001).

people's ways of assessing reliability of information and safeguarding the security of communication are still, to a high degree, geared to traditional media. (Vedder, 2002) They relate to the—often institutionally embedded—signs of authority of the sources and intermediaries and to the recognisability of the details of the process of the transactions involved. With the growing speed of the information and communication networks two characteristics of the Internet are further enlarged. First, as the number of content providers and the ease of uploading information further increases assessing the true nature of sources and intermediaries of information becomes more difficult. Second, as the technologies involved become more sophisticated and complicated, the processes of interaction become less transparent. All of this diminishes the possibilities of assessing the trustworthiness of partners in communication and of information content providers, and of assessing the validity and reliability of information and of ensuring the security of transactions (Vedder and Lenstra, 2006).

Sometimes, the drawbacks of limited quality or reliability of information may not be obvious. However, some examples may illustrate the consequences of lacking data quality or flawed security. For instance, many people tend to increasingly rely on the use of medical information on the Internet for diagnosing their own medical situation. Since not everyone is a medical expert, this may lead to errors in such diagnosis. As a result, people may start to use the wrong medication or treatment. Obviously, not all medication can be obtained without seeing a health care professional, but the Internet also provides plenty of options of ordering medication abroad. Medication produced in countries with less strict quality assurance may result in even worse consequences.

Another example of how limited reliability and security of information on the Internet may have serious drawbacks concerns financial data. *Phishing* is the process of attempting to acquire personal information, such as passwords and credit card details, from people by pretending to be a trustworthy person or organization. A phishing attempt usually involves an email that asks users to fill out their personal data. Such emails may look reliable to the users, they may even be exact copies of messages from their own bank, in order to convince users to hand over their personal data. Once the data are sent, they can be used by the criminals to make financial transactions for their own benefit.

Reliability in the epistemologically normative sense that is relevant here is a matter of proper justification in terms of "content criteria" and "pedigree criteria" of reliability (Vedder and Wachbroit, 2003; Vedder, 2005). "Content criteria" refer to the conditions or criteria of reliability that are a function of the content of the information itself. Among these are the criteria of evidence that mostly belong to the domain of experts—people familiar with the subject or with a specific educational background or experience. Other examples of content criteria are logical criteria and, arguably, subject-matter criteria. "Pedigree criteria" are the conditions or criteria of reliability that relate to the authority and the established legitimacy and credibility of the source or intermediary of the information. Pedigree criteria are not merely used by non-experts. Experts use them as well. Pedigree criteria are established by credibility-conferring institutions. Here one can think of institutions in a very broad way, ranging from well-organized institutes to broader—sometimes intricate and tangled—networks of cultural and societal arrangements. Earlier research has shown that many problems regarding reliability of online information on the Internet are not problems of information *lacking* reliability, but of receivers misperceiving or not perceiving (un-) reliability.

The very possibility of adequately recognizing pedigree criteria will increasingly diminish where fast networks with enhanced connectivity are concerned. Increasingly often, a content provider will be anonymous or will have merely a virtual identity. Also, the lack of traditional intermediaries (such as libraries, librarians, specialized publishers) has a negative influence on the capabilities of information seekers to assess the reliability of information. These kinds of factors leave the users often without clues or any indication whatsoever about the character, background, and institutional setting of the content provider. As the accessibility to a broader public of information originally intended for experts increases, the absence of intermediaries becomes gradually more problematic. Finally, as the connectivity and the possibility of providing content through networks increase, the opportunities for content providers to present themselves as others than they are—resulting in misinformation and, for instance, phishing—will multiply accordingly. Consequently, there will be a growing need for—not only—the development of new credibility conferring systems, but even for possibilities of identification and authentication of content providers.

3.3.2 Privacy and Public Security

Another issue is the role of ultrafast networks in public security and its implications for the privacy of individuals. Currently, lots of information on communication is collected and processed by judicial authorities and intelligence services themselves and by third parties such as telecom corporations and internet providers to support governments in their fight against crime and terrorism (Vedder et al., 2007) This surveillance can be distinguished in two main types, i.e. tapping and data retention. Tapping, or wire tapping, has been used for a long time and aims at monitoring the contents of any specific communication, such as phone call or an e-mail. In most modern countries there are very strict regulations to comply with before tapping is allowed. Data retention is a more recent form of surveillance. It is not aimed at the contents of any communication, but on the traffic data, i.e., surveillance of the call detail records of telephony and Internet traffic and transaction data. In March 2006 the European Union adopted a directive that requires telecom operators and Internet providers in all member-states to implement data retention systems for both telephone and Internet traffic.[2] Data retention focuses on the storage of call detail

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

records of telephony and Internet traffic and transaction data. Basically this concerns phone calls made and received, emails sent and received and web sites visited. These data provide an idea of who stays in contact with whom, when and how frequent. When possible, further identifying information may be added, as well as location data.

The new generation of ultrafast communication networks is likely to be a combination of optical and wireless. The former is relatively hard to tap; the latter is relatively easy to tap. Particularly for the wireless parts of ultrafast communication it is therefore recommended that cryptography is used to prevent unauthorized tapping. However, the cryptography used should not be too strong to be deciphered in cases in which tapping is allowed. The use of trapdoors and technologies such as key recovery systems, key escrow systems and trusted third-party encryption may be helpful to achieve this. These are systems and technologies in which exceptional access is possible. This enables users with additional information to circumvent the regular access and security procedures. For more detailed information, see Abelson et al. (1998) and Akdeniz (1998).

Whereas tapping concerns the contents of the communication, data retention focuses on storing and analyzing communication data, particularly call detail records regarding phone calls and Internet traffic. Ultrafast networks will require larger capacities for storing and analyzing data. The former is relatively easy, since storage capacity is ever increasing (though the costs involved are subject of a major discussion); the latter is a significant problem. Analyzing vast amounts of data needs to be done in automated ways, such as with the use of data mining. However, most data mining technologies are not yet very sophisticated for large-scale use. Furthermore, a major disadvantage is that the risk profiles resulting from the automated analyses may not be accurate, see Custers (2003). False-positives may result in investigating and even arresting innocent people. False-negatives may result in criminals and terrorists being out of scope. When risk profiles have limited accuracy, they should only be used with the utmost care, in order to prevent investigating and arresting innocent people. It is recommended to keep performing double checks on existing risk profiles and not to merely rely on data in databases, but also perform significant field work. In order to prevent the worst forms of unjustified discrimination and social polarization, it is recommended not to include sensitive personal data, such as religion and ethnic background, in the risk profiles, see Custers (2004).

In sum, tapping and data retention in the age of ultrafast communication networks may be very useful to reveal criminal and terrorist networks and to find first offenders. Both aspects are increasingly needed in the fight against crime and terrorism. However, because of the increasing amounts of data that are communicated over ultrafast networks, it is absolutely necessary to make, from the outset, selections on which data should be collected. Even though all data can be stored, it is not recommendable to do so, because the overview will be lost. A better idea is to make a selection of the data that may be useful. This will be a more targeted and effective approach than storing and analyzing all available data. This will be a lesser infringement of the privacy of those data subjects whose data is involved, particularly of those who are innocent. Obviously, privacy infringements may be allowed in some cases, both from a moral and a legal perspective, particularly when dealing with organized crime and terrorism, but such infringements should be limited to a minimum. According to Etzioni (1999), limitations of privacy should only occur when there is a well-documented and macroscopic threat to the common good at stake. Even then, it should be considered whether the intended measures limiting the privacy are effective and whether the goal cannot be achieved with other measures that are less privacy-invasive. When this is the case and the privacy of individuals or groups of people is actually violated, measures should be considered to treat undesirable side effects.

3.3.3 Accessibility and Exclusivity

In the last decades, it has become clear that people are not only increasingly using information and communication technologies, but are also becoming increasingly dependent on them. As a result, many actions that people used to do in person or on paper are now performed digitally. For instance, many people are no longer booking their flight tickets through a travel agency in town, but use the Internet. In many countries, people request their tax returns via their home computers, no longer using paper files. Instead of going to a shop to buy a CD, many people nowadays download their music from the Internet. The dependency of people on information and communication networks raises questions on the accessibility and exclusivity of these networks. These questions are closely related to the debate on the so-called *digital divide*. For more on this debate, see, for instance, Compaine (2001), Van Dijk (2005), Mossberger et al. (2003).

Ultrafast communication networks are likely to introduce two barriers of access to users: costs and knowledge. These access barriers may result in excluding groups of people from access to these networks. In the early stages of introduction of new technological developments, it is likely that the costs will be kept low in order to get a critical number of users that communication networks usually require. This is a different approach the normally used in non-networked technologies, such as apartments, cars, or books, in which cases profit has to be made from selling the product itself. After a sufficient number of users is connected to the network, profit has to be made to compensate investments that were made, and costs for consumers to buy the products and services offered on the network will increase. These costs may decrease again after the introduction of more competition. Generally spoken, the number of users may depend on the costs involved and even though costs may be kept low, it is likely that there will always be groups (small or big) of people who are excluded.

The same goes for the knowledge that is required from users of sophisticated networks. In general, older people seem to have more trouble adapting to the latest technological developments. New technologies may expect more of users regarding education levels and may require users to be able to adapt to new concepts, such as using a mouse or a touch screen or talking to a computer on the phone. This may also result in excluding some groups of people from access to communication networks.

When larger groups of people are excluded from the networks, this may cause social polarization between those who are included and those who are excluded. Apart from social polarization, another effect of exclusive networks may be the limited number of providers of structure and content, which may lead to manipulation of the information provided.

Because digital services may address most customers and may involve fewer costs, it may ultimately no longer be profitable for companies to have offices in town where people can go to for their products or services. As a result of Internet trade, many music stores, travel agencies and bank offices have already downsized or closed. It is expected that many more will follow in the years to come. This is likely to increase the exclusivity of networks, particularly when, in the next stage of technological developments, ultrafast networks will replace the existing networks. Here we will offer three suggestions that may help to deal with the above-mentioned effects of the exclusivity of ultrafast communication networks. The first and second aim to decrease the exclusivity of the networks by addressing the access barriers, the third addresses alternatives to exclusive networks:

- *Remove the costs barrier*
  The first reason for exclusivity are the costs involved. There may be several ways to remove this barrier. For instance, the costs may be compensated, or free access points, such as in libraries, may be provided.
- *Remove the knowledge barrier*
  The second reason for exclusivity is the knowledge required. There may be several ways to remove this barrier. For instance, by educating these groups and by providing more user-friendly access points.
- *Ensure off-line alternatives for basic needs*
  Some networks will be exclusive, when the barriers above cannot be removed. For most commercial networks this is not necessarily a problem. It may become a problem when there are basic needs involved for the users. Booking a flight ticket is generally not considered a basic need, but buying clothing or completing tax return forms may be considered so. For these applications, it seems reasonable to provide off-line alternatives, even if they may no longer be profitable after some time.

Current communication networks, such as the Internet, do not show large-scale social polarization and manipulation of information. Most basic needs can still be purchased off-line. Although ultrafast communication systems are likely to show at least some of the effects described on a larger scale, the suggestions above may help to minimize or avoid these effects. Exclusivity of networks is not necessarily a negative thing, as long as there remain some choices and alternatives for both those who are included and those who are excluded. However, exclusivity may become a drawback when it causes social polarization and prohibits people from access to basic needs.

3.4 Responsibilities Involved

In the previous sections we expounded the possible benefits and drawbacks of the development and introduction of technologies that can further increase the speed and accessibility of information and communication networks. We mainly concentrated on the broad social impact that these technologies may have in the future. We have not and we will not say much about possible benefits and drawbacks of earlier phases of the development and introduction into the market of these technologies. Of course, it is possible that at some stage of these earlier phases morally questionnable situations arise. It could be possible, for instance, that poisonous materials were used exposing researchers to health risks. Or that materials were used that are rare and extracted under very bad circumstances in developing countries. We did not refer to possible problems such as these (and to our current knowledge would not need to do so) because the expertise needed to identify these problematic issues belongs to the domain of other specialists, e.g. the engineers that perform the research themselves. This brings us to questions regarding the responsibilities for identifying and actually addressing possible positive and negative consequences of technologies.

For this question to be answered, it is important to consider the different phases in developing and introducing new technologies. Here we will distinguish the following phases:

1. Research and development
2. Production
3. Introduction into the market/society

When thinking through the division of responsibilities with regard to the diagnosis of and the response to possible opportunities and risks, it must be taken into account that many of the actors and stakeholders involved in the phases mentioned only have a very restricted insight into the opportunities and risks involved. Moreover, many of them have restricted means to respond. For instance, engineers are involved in the first phases, but have limited influence on the introduction of new technologies into the market/society. End users may have effect on how the new technologies are introduced into society and how the new technologies are actually used. However, end users have restricted means to influence research, development and production of new technologies.

It seems, therefore, appropriate to first distinguish between responsibilities to identify benefits and drawbacks, on the one hand, and responsibilities to act in order to respond to them, on the other. Recognizing advantages and drawbacks requires insight and expertise in the technological developments and also a kind of ability to see what would be socially beneficial or detrimental. This insight and ability need not necessarily be accompanied by the ability and capacity to respond, once advantages or drawbacks have been identified. For example: it may be an engineer's responsibility to identify risks to the environment involved in the production of an artifact, but that does not mean that the solution for this problem is this person's responsibility as well.

Second, a distinction should be made between the responsibilities of the different parties and individuals who are somehow involved, for instance: the researchers, supervisors, organizations funding the research, enterprises, governmental authorities, consumer organizations and other NGOs. The responsibilities with regard to the identification of drawbacks and advantages may vary according to the different expertise in technology and acquaintance with the various needs and preferences in society. The responsibilities for acting can vary with the different capacities and powers of the parties involved. An NGO may have a responsibility to do something about environmental risks caused by the production of an artifact, which an engineer involved in that process may not have, although he or she identified the risk and communicated it to the NGO involved—simply because the NGO is in a much better position and is apt to respond to phenomena like these.

It is by all means undesirable that all responsibilities are assigned to just one group of stakeholders, such as the researchers or engineers themselves. Nonetheless, the currently popular value-sensitive design approach in ethics of technology (Friedman et al., 2006) has a natural focus on the stage of design. This focus may be appropriate in light of the still very dominant view that technology and its design are in themselves morally neutral. Simultaneously, it is apt to draw away the attention from the other stages and from stakeholders other than the directly involved engineers. Coincidence or not, there is a growing tendency to restrict the window of possible interference in the case of flaws in technology to the pre-market phase. This tendency, pervades the plans of the Bush administration to restrict liabilities to risks involved in technology to the risks that were foreseeable at the time of design (Pear, 2004).

The responsibilities should be assigned to the various parties involved because of their different expertise, abilities and powers. They should not be restricted to the stage of research and development, simply because not all possible advantages and drawbacks can be known at that stage. The process of appraisal and critical evaluation should start in that first stage, but it should not also be finished in that stage. This will prevent that those involved in the different stages will push off responsibilities to others. It is still often the case that engineers and technicians suggest that they only build a particular technology that others can use for better or for worse. The end users, however, often suggest that they only use technologies for the purposes for which they were intended or designed. In the case of weapon technology, for instance, manufacturers usually claim end user responsibility, whereas victims of this technology suggest that their harm may have never occurred when the weapons were not manufactured in the first place.

In order both to facilitate the identification and to find creative responses, communication by all the parties involved throughout all stages would be desirable. With regard to possible drawbacks, one might be tempted to think only of suppression by for instance prohibiting the development or the exploitation of certain techniques, such as was initially the case regarding stem cell research in the United States. By initiating the communication and debate of all the stakeholders, however, one may try to find technical solutions in an earlier stage of the development. Or, conversely, it may become clear that certain technical solutions may not work, so that accompanying regulatory measures are called for, once an artifact is introduced in the market. Ensuring higher degrees of user-friendliness may be a typical example of the former approach, educating users may be a typical example of the latter approach.

In this section, we have emphasized the plurality of parties involved and the variety of responsibilities of those parties. Each of these parties may sometimes feel tempted to shun away from specific responsibilities. For instance: an engineer specialized in a very specific part of the development of a new artifact may think that he or she is not responsible for thinking about its broader social impact since other parties have responsibilities as well. The fact that consumer organizations or a governmental authority may have responsibilities with regard to the design, production and introduction of an artifact, however, does not exempt the engineer. All of the parties have responsibilities based on their expertise and capabilities. It is hard to see, how anyone of them, especially the engineer, could deny that his or her expertise and ability are relevant. This may again be illustrated with the example of weapon technology: it may not be realistic for weapon manufacturers to push off responsibility to end users that may use the weapons for better or for worse. When weapons are manufactured on a large scale, it may be assumed that they will be used sooner or later to some extent. Instead of pushing off responsibilities, it is preferable to have joint responsibilities. Instead of creating gaps in the responsibilities, i.e., parts of the research and development process where nobody is responsible, this may create joint responsibilities. We consider overlapping responsibilities an advantage rather than a drawback in these cases.

3.5 Conclusion

New technologies are changing the world we live in. Many benefits come with the development and introduction of these new technologies. Using the example of ultrafast communication technologies, we investigated typical consequences regarding the quality of information, privacy, security, and accessibility of information and communication. As these effects cover the different phases in developing and introducing new technologies, the question was raised who is responsible for these effects, particularly the drawbacks of new technologies. Hence, it was suggested to distinguish responsibilities to identify benefits and drawbacks versus responsibilities to respond to them. A second distinction was made regarding the parties involved in the different stages of the development and introduction of new technologies.

Sometimes the parties involved are tempted to shun away from specific responsibilities. However, the fact that there are more than one party bearing certain responsibilities does not exempt the parties involved to take up their specific responsibilities. Joint responsibility during the whole process of development and introduction is recommended. This may be achieved by communication by all the parties involved throughout all stages. In this way, they will have more overview over the whole process, benefits may be maximized and drawbacks and risks may be minimized. Minimizing drawbacks and risks may involve taking accompanying regulatory measures in cases where the drawbacks cannot be avoided, but this is not necessarily so.

References

Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., and Schneier, B. (1998) *The risks of key recovery, key escrow and trusted third party encryption*; A report by an ad hoc group of cryptographers and computer scientists. www.cdt.org/crypto/risks.

Akdeniz, Y. (1998) No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights. In: *4th International Conference on Ethical Issues of Information Technologies,* Ethicomp 98, Rotterdam.

Compaine, B.M. (2001) *The Digital Divide: Facing a Crisis or Creating a Myth*, Cambridge MA: The MIT Press.

Cotter, D., Manning, R.J., Blow, K.J., Ellis, A.D., Kelly, A.E., Nesset, D., Phillips, I.D., Poustie, A.J., and Rogers, D.C. (1999), Nonlinear optics for high-speed digital information processing. *Science,* 286, pp. 1523–1528.

Custers, B.H.M. (2003) *Effects of Unreliable Group Profiling by Means of Data Mining*. In: G. Grieser, Y. Tanaka and A. Yamamoto (eds.) *Lecture Notes in Artificial Intelligence, Proceedings of the 6th International Conference on Discovery Science (DS 2003)* Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag, Vol. 2843, pp. 290–295.

Custers, B.H.M. (2004) *The Power of Knowledge*, Tilburg: Wolf Legal Publishers.

Custers, B.H.M. (2008) Tapping and Data Retention in Ultrafast Communication Networks, *Journal of International Commercial Law and Technology*, 3(2), pp. 94–100.

Etzioni, A. (1999) *The Limits of Privacy*, New York: Basic Books.

Friedman, B., Kahn, P.H., Jr., and Borning, A. (2006). Value Sensitive Design and information systems. In: P. Zhang and D. Galletta (eds.) *Human-Computer Interaction in Management Information Systems: Foundations*, Armonk, New York; London, England: M.E. Sharpe, pp. 348–372.

Miller, D.A.B. (2004) Ultrafast Digital Processing. In A. Miller, D.M. Finlayson, and D.T. Reid (eds.) *Ultrafast Photonics*, Bristol, Philadelphia: Institute of Physics Publishing.

Mossberger, K., Tolbert, C.J., and Stansbury, M. (2003) *Virtual Inequality: Beyond the Digital Divide*, Washington DC: Georgetown University Press.

Pear, R, (2004) In a Shift, Bush Moves to Block Medical Suits. http://query.nytimes.com/gst/fullpage.html?sec=health&res=9B05EED6173DF936A15754C0A9629C8B63 (accessed on 14th August 2007).

Raessens, B. (2001) *E-Business, Your Business*. Utrecht: Lemma.

Schaller, R.R. (1997) Moore's Law: Past, Present and Future, *Spectrum*, IEEE, Volume 34, June 1997, pp. 52–59.

Van Dijk J.A.G.M. (2005) *The Deepening Divide: Inequality in the Information Society*, Thousand Oaks CA: Sage Publications.

Vedder, A. (2002) What people think about the reliability of medical information on the Internet. In: I. Alvarez, T. Ward Bynum, J. Alvaro de Assis Lopes, and S. Rogerson, (eds.) *The Transformation of Organisations in the Information Age: Social and Ethical Implications.* Lisboa: Universidade Lusiada, pp. 281–292.

Vedder, A. (2005) Expert knowledge for non-experts: Inherent and contextual risks of misinformation. *ICES, Journal of Information, Communication and Ethics in Society*, 3, 113–119.

Vedder, A. and Robert W. (2003) Reliability of information on the Internet: Some distinctions. *Ethics and Information Technology,* 5, pp. 211–215.

Vedder, A. and Daan L. (2006) Reliability and security of information. *Journal for Information, Communication and Ethics in Society*, 4(1), pp. 3–6.

Vedder, A.H. et al. (2007) *Van Privacyparadijs tot Controlestaat? Misdaad- en Terreurbestrijding in Nederland aan het Begin van de 21ste eeuw.* Studies Rathenau Instituut (Ext. rep. 49). Den Haag: Rathenau Instituut.