ETHICAL AND LEGAL ASPECTS OF INFORMATICS RESEARCH
ETHICAL AND LEGAL ASPECTS OF INFORMATICS RESEARCH
ETHICAL AND LEGAL ASPECTS OF INFORMATICS RESEARCH
Research is fascinating and its results often have a major impact on society. While that can be said of many areas of research, it is true beyond a doubt for informatics, a field evolving so rapidly that over the past ten years it has utterly transformed the way we communicate. Informaticians are behind self-driving cars and have made it possible to use our bank cards to make payments safely all over the world. It is precisely because informatics is so influential that we must be aware of the potential negative effects of informatics research. Should we simply permit everything that is possible? For example, should we allow researchers investigating computer system security to hack a bank’s system? How can we guarantee the privacy of those participating in research? Researchers increasingly find themselves pondering these and other ethical and legal issues. It is not always easy for them, and many areas of research still lack an ethical review mechanism. I am therefore delighted that the informatics researchers in our Academy Council for Technical Sciences, Mathematical Sciences, Informatics, Physics, Astronomy and Chemistry (TWINS Council) have initiated this advisory report.

The advisory committee, chaired by Jan Willem Klop, has conducted a detailed analysis of how researchers might assess ethical and legal dilemmas. It looked closely at the medical sciences, which have long had review mechanisms of this kind, and queried fellow researchers abroad.

Among other recommendations, the committee advises installing ethical review boards and sheds light on how such boards might operate. I am very much in favour of the committee's recommendations, but note that we must avoid a situation in which all university review boards develop their own local review mechanism. After all, it will not do to have a research proposal meet with approval in Groningen only to be
rejected in Nijmegen on ethical grounds. I am therefore a staunch advocate of the learning model that the committee proposes. What is very important is to make the opinions handed down by the various boards available in a central repository. I call on informatics researchers to take swift action in that respect.

I am especially pleased by the committee’s assertion that installing review boards does not discharge individual researchers from personal responsibility. The important task of raising awareness among future generations of researchers is one that must be taken up by academia. Some research schools have already made ethics a compulsory part of the curriculum for young trainee researchers. I hope that other research schools soon follow their example.

This advisory report is meant for the informatics community, but researchers in other fields come upon the same ethical dilemmas that appear to be inherent to informatics research. Moreover, informatics is growing increasingly intertwined with other fields. I therefore hope and expect that this advisory report will prove inspiring for other disciplines.

Finally, a comment about the scope of this report. At the start of the advisory process, the committee was asked to look into the ethical and legal aspects of big data as well. It soon became clear that this is an exceptionally broad topic that extends far beyond informatics. The Academy therefore decided to install a separate committee on big data. We expect that committee to issue its report early next year.

José van Dijck
President of the Royal Netherlands Academy of Arts and Sciences
Informatics research and its results have a huge influence on society. It goes without saying that both the public and research funding bodies increasingly expect an exhaustive review of the ethical and legal dilemmas associated with this research. For example, is it permissible to hack a public transport smartcard or a keycard allowing access to all government buildings when investigating the security of such systems? And if so, subject to which conditions? At the moment, it is up to the researchers themselves to make the ethical and legal judgement call, explicitly or not. And although a number of institutions are experimenting with ethical review boards, such initiatives are still in their infancy. In the years ahead, we must develop a transparent review mechanism and an efficient infrastructure for assessing the ethical and legal aspects of informatics research. The Academy believes that this advisory report will support continuing professional development in the field of informatics research.

The Academy has installed a committee whose task is: to identify ways to assess the ethical and legal aspects of informatics research.

The committee focused mainly on the dilemmas involved in research such as that conducted by informatics departments at Dutch universities and research institutes. Typical examples include research on network and computer system security, human-machine interaction, software reliability, and artificial intelligence. The ethical and legal aspects associated with collecting and using large (privacy-sensitive) data-sets fall outside the scope of this report. The Academy has established a separate ‘Big Data’ advisory committee to address that subject.

The committee collected and analysed information in various ways. First of all, it interviewed key figures in the field. This has allowed it to form a picture of how institutions
view this subject, and whether – and if so, how – they review their research and which
dilemmas they encounter along the way. As background for developing a review mech-
anism, the committee analysed the protocols utilised by Dutch and foreign institutions.
Medical science has already gained considerable experience in reviewing the ethics
of research proposals. The committee therefore looked in detail at how the medical
world is organised in that regard and what lessons we can learn from it. The com-
mittee presented the main outlines of its report to the research community during a
liaison group meeting. The participants’ comments at that meeting have been incorpo-
rated into this final report.

CONCLUSION 2.1

Society in general, but also – and in particular – research funding bodies are increas-
ingly asking scientists to conduct an exhaustive review of the ethical aspects of their
research. That is the case in many disciplines, but certainly in informatics, given its
enormous societal impact and importance. We must develop an ethical infrastructure
for informatics. This means that a transparent and distinguishable review mechanism
must evolve about which the field has reached consensus. In addition, we must seek
out an assessment method that is scrupulous and robust but also efficient and func-
tional without being too bureaucratic.

CONCLUSION 2.2

The medical sciences have already gained considerable experience in the ethical scru-
tiny of research. Because it places heavy emphasis on the consequences for human test
subjects, however, the system used in medical research cannot simply be transferred
across the board to informatics research. The ethical issues involved in informatics re-
search are highly specific to the field. Moreover, the law does not prescribe any form of
ethical assessment for informatics research. That is why informatics can draw on the
experiences of the medical disciplines but must develop its own review mechanism
and assessment method.

The collection and processing of personal data is very common in informatics
research, as are investigations into software or computer systems that are the prop-
erty of others. That is why this type of research soon raises legal questions, for
example concerning privacy or intellectual property rights. It is beyond the commit-
tee’s remit to conduct an exhaustive study of what the law does and does not permit
and the conditions and circumstances that apply in either case. The committee has
therefore outlined recurring dilemmas in various phases of research and described
potential measures for dealing with them. In specific cases, however, a legal expert
should always be consulted. In every phase of research, researchers must be aware
of the potential legal implications of their actions. How will my research affect the
privacy of others? Do the activities that I am undertaking within the context of my
research comply with statutory rules and contractual agreements governing intellectual property rights? Scrupulousness and proper documentation are advised. What many researchers do not realise is that ‘doing nothing’ can also lead to liability issues. Researchers have a duty of care, which may mean that they run the risk of legal sanctions if they ignore unusual patterns.

**CONCLUSION 3.1**

When selecting a research subject, researchers should give top priority to the interests of science and offer solid arguments for why their research will serve the interests of society. They should clarify how and to what extent their findings could affect the interests of third parties, including their privacy and intellectual property rights. Researchers and other relevant stakeholders should explicitly weigh the scientific and societal interests of their research against the interests of any third parties whose rights may be infringed. In short, the end does not always justify the means.

**CONCLUSION 3.2**

Informatics researchers have a duty of care. This means that remaining passive in certain situations could lead to their being held liable. Researchers and research groups should therefore remain vigilant and report any perceived risks to persons and society to compliance officers within their own organisations and, where necessary, to the enforcement authorities.

The ethical issues associated with IT have been the subject of worldwide interest in the field of ethics since the 1980s. The literature addressing this subject, however, can largely be found in the social and behavioural sciences and mainly concerns social media and the internet. There is no well-defined set of international guidelines for review boards in informatics research, nor is there a tried-and-tested model for organising reviews efficiently. Both for society and the research field itself, it is important to develop such a model in the years ahead. The committee therefore favours the installation of local Ethical Review Boards for Informatics (ERBIs). In the committee’s view, the ERBIs would have three important tasks:

1. to assess the ethical aspects of informatics research, so that research that clearly raises ethical questions would ideally commence only after the relevant research proposal was given the greenlight by the ERBI.
2. to promote continuing professional development, so that researchers and institutions can account for their informatics research in ethical terms, based on informed judgement;
3. to embody the core and promote the continuity of a community of expertise in which knowledge concerning this subject is documented and continues to advance. The ERBI would thus serve as the linchpin of an organisation’s ethical learning process.
The committee has identified a number of key success factors that will ensure the robustness of these ERBIs, including local engagement, speed of action, and the status and legitimacy of their opinions. Local engagement is hugely important because an ERBI can only function if the distance between the board and the researchers is minimal, both physically and in terms of sentiment. The committee therefore supports the installation of local review boards. It is very important, however, for the boards to develop a shared conceptual framework (review/action mechanisms). A national peer-review model can assist them in this.

**CONCLUSION 4.1**

One way that the informatics research community can live up to its ethical and public responsibility and demonstrate its awareness that informatics plays an important role in shaping society is to install an Ethical Review Board for Informatics, monitor the performance of this board, and reflect on the lessons learned in this manner.

**RECOMMENDATION 4.1**

The committee advises all governing bodies of institutes or departments active in informatics research to install an Ethical Review Board for Informatics (ERBI), either on their own or in cooperation with sister institutions. The primary task of the ERBIs is to assess the ethical aspects of informatics research. They can also function as the core of a community in which knowledge concerning this subject continues to advance.

**RECOMMENDATION 4.2**

Ethical assessment of informatics research is still in its infancy. No blueprint or ideal description of an Ethical Review Board for Informatics can be provided, nor does any set of predetermined standards exist. In addition, informatics is an exceptionally dynamic field, making it impossible to predict which issues will arise next year. ERBIs are advised to develop their own methods and set of standards, and to do so in close consultation with other ERBIs.

It is difficult to pinpoint precisely which type of research will raise ethical or legal dilemmas and the attendant risks. Nevertheless, in the interests of scientific progress and efficiency, an ERBI must identify, as quickly as possible, proposals whose ethical or legal aspects require further examination. As a starting point for discussion within ERBIS, the committee therefore proposes a review procedure that distinguishes between a more lenient and a more stringent assessment. The lenient, and therefore faster, procedure is for research of a more standard nature. The more stringent procedure is for non-standard research. A critical factor in the entire review cycle is the report issued by the ERBI and how it documents and shares the cases it has reviewed. It should preferably do so in a way that allows researchers and all other ERBIs to consult the reports easily. Specifically, that will allow all ERBIs to work together on developing a uniform review mechanism.
CONCLUSION 5.1
Ethicists use ethical value types to articulate the arguments advanced in the process of ethical assessment. Examples of value types are ‘respect’, ‘privacy’ and ‘wellbeing’. There are many different and divergent values that cannot be reduced to a single type, however. Values do not, furthermore, fit into neat classifications, and they may even conflict with one another. This is equally true of the values common in informatics research. This ‘value pluralism’ means that it is impossible to provide an unambiguous, unchanging review mechanism. Assessments will have to be made on a case-by-case basis.

CONCLUSION 5.2
The protocols and guidelines for ethical assessment currently used by many Dutch and foreign organisations are relatively limited in scope. The questions they pose generally concern the ethical aspects of identifiable research subjects. They rarely address the effects of research on society or the environment in terms of their ethical dimensions.

RECOMMENDATION 5.1
ERBIs are advised to develop an efficient and transparent procedure that distinguishes between a lenient and a more stringent assessment. The lenient procedure is meant for proposals that concern more standard research. The present advisory report outlines a possible review procedure of this kind.

RECOMMENDATION 5.2
ERBIs are advised to document their opinions properly and to make them available to researchers and other ERBIs. In the longer term, the committee recommends working to build a well-organised, shared repository where all decisions are available for perusal. Having a central repository of ‘ethical case law’ makes it possible to check for consistency and convergence between reviews and will help to construct a more uniform review mechanism.

Installing ERBIs and developing a shared review mechanism are important steps forward, but they are not enough. It is very important that all researchers become and remain aware of the ethical and legal aspects of their actions. Review boards and the governing bodies of institutions must not take responsibility away from individual researchers. University faculties must nurture a culture in which it becomes ‘normal’ to think about and discuss these subjects. To do this, they could consider:

- talking about ethical and legal dilemmas during regular and bilateral meetings;
- drafting a code of conduct or making practical agreements in this respect;
- appointing an ethics adviser;
- making training in ethics and integrity a compulsory part of a researcher’s education.
CONCLUSION 6.1

Informatics research, and the context in which it is conducted, are in a continuous state of transition. As a result, new ethical and legal issues are constantly arising in relation to research projects. It is not enough to have a review board conduct a one-off review of these issues at the start of a project. Research institutes and individual researchers must work constantly on raising ethical awareness and conducting ethical reviews and make these an inherent part of the organisation.
CONTENTS

FOREWORD 4

SUMMARY 6

1. INTRODUCTION 14
   1.1 Background 14
   1.2 Assignment and composition of the committee 15
   1.3 Methods 18

2. ETHICAL AND LEGAL ASPECTS OF INFORMATICS RESEARCH 19
   2.1 Introduction 19
   2.2 Typical examples of dilemmas 20
   2.3 What can we learn from medical research reviews, for example? 23
   2.4 Conclusions 25

3. LEGAL ASPECTS 27
   3.1 Introduction 27
   3.2 Choice of research subject 28
   3.3 Legal aspects in the various research phases 29
   3.4 Informatics researchers and their duty of care 35
   3.5 Conclusions 35

4. ETHICAL REVIEW BOARDS 36
   4.1 Ethics and Information Technology 36
   4.2 Ethical review at knowledge-based institutions 37
   4.3 Ethical Review Board for Informatics (ERBI) 38
   4.4 Practical guidance for ethical assessment 42
   4.5 Conclusions and recommendations 43
<table>
<thead>
<tr>
<th>5.</th>
<th>A REVIEW PROCEDURE IN OUTLINE</th>
<th>44</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>44</td>
</tr>
<tr>
<td>5.2</td>
<td>Ethical values</td>
<td>44</td>
</tr>
<tr>
<td>5.3</td>
<td>An international tour</td>
<td>46</td>
</tr>
<tr>
<td>5.4</td>
<td>The ERBI at work: proposed method</td>
<td>47</td>
</tr>
<tr>
<td>5.5</td>
<td>Reporting and storage</td>
<td>52</td>
</tr>
<tr>
<td>5.6</td>
<td>Conclusions and recommendations</td>
<td>53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.</th>
<th>WHAT ELSE IS NECESSARY?</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>55</td>
</tr>
<tr>
<td>6.2</td>
<td>Insights</td>
<td>56</td>
</tr>
<tr>
<td>6.3</td>
<td>Awareness</td>
<td>57</td>
</tr>
<tr>
<td>6.4</td>
<td>Embedding awareness</td>
<td>57</td>
</tr>
<tr>
<td>6.6</td>
<td>Conclusion</td>
<td>59</td>
</tr>
</tbody>
</table>

BIBLIOGRAPHY | 60 |
GLOSSARY | 62 |
ACRONYMS AND ABBREVIATIONS | 67 |

APPENDICES
1. Interviewees, reviewers and acknowledgments | 68 |
2. Resolution inaugurating the committee | 70 |
3. Protocols, checklists and guidance documents | 73 |
4. Questions for the initial review | 75 |
5. Questions about research method and approach | 77 |

INDEX | 81 |
1. INTRODUCTION

1.1 Background

The initiative for this advisory report was taken by the Academy Council for Technical Sciences, Mathematical Sciences, Informatics, Physics, Astronomy and Chemistry (TWINS Council). The informatics researchers in the TWINS council have observed that researchers in their field are increasingly coming up against ethical and legal dilemmas.\footnote{This report uses the terms ‘ethical’, ‘integrity’ and ‘lawful’. The common denominator for these three terms is that they all refer to ‘proper conduct’, as in ‘behaving as one should’. There is naturally a difference in the sense that we can disagree about what constitutes ethical behaviour and, to a lesser extent, about integrity in behaviour, but much less so about lawful behaviour, since the latter is set out in rules and laws. At the same time, we can also disagree about how rules and laws are interpreted and applied. In each case, the point is for researchers to think about their own conduct (in what are often new situations for them); in some cases the law, rules, case law or a code of conduct will provide more guidance than in another.} They also feel that the issues involved are growing ever more complex. In addition, both society and research funding bodies increasingly expect researchers to conduct an exhaustive review of the ethical aspects of their research and to ensure that their research approach is lawful. For example, the following criterion applies to research proposals submitted to the EU Horizon 2020 programme: ‘A proposal which contravenes ethical principles or any applicable legislation may be excluded from evaluation, selection and award procedures at any time.’

At the moment, it is frequently the researchers themselves who make the ethical or legal judgement call, explicitly or not. A number of institutions are following the lead of the medical, social and behavioural sciences by experimenting with ethical review boards for research proposals. This is a laudable development, but one that is clearly...
still in its infancy. In the years ahead, a transparent and distinctive culture of scrutiny must evolve about which the field has reached consensus, along with a review mechanism that is transparent and distinguishable as such for the research community and beyond. In addition, we must seek out a review method that does justice to ethical and legal frameworks while also operating efficiently and without too much bureaucracy. It is very important to start our search as soon as possible and not wait until a specific event forces us to take action. This advisory report is the Academy’s contribution to developing and embedding an ethical and legal review mechanism in the field of informatics research.

1.2 Assignment and composition of the committee

The Academy Board installed the Committee on the Ethical, Legal, Security and Safety Aspects of Big Data and Informatics Research to produce this advisory report. The committee consisted of the following persons:

- Prof. Jan Willem Klop (chair), VU University Amsterdam and Centre for Mathematics and Computer Science
- Prof. Jan Bergstra (University of Amsterdam)
- Prof. Frank van Harmelen, VU University Amsterdam
- Prof. Jeroen van den Hoven, Delft University of Technology
- Prof. Bart Jacobs, Radboud University Nijmegen
- Prof. Corien Prins, Tilburg University
- Melle de Vries, Royal Netherlands Academy of Arts and Sciences

Arie Korbijn (Academy Senior Policy Officer) acted as the committee’s official secretary.

Assignment

At the start, the committee was charged with the task of outlining a mechanism for reviewing the ethical, legal, and security/safety aspects of informatics research and related studies (see Appendix 2). This covered:

- the assessment of research on the security of networks, computer systems and access to the same;
- the collection and use of the large, often privacy-sensitive data sets (‘big data’) that are on the rise in numerous disciplines.
It was clear to the Academy from the beginning that the committee’s assignment was very broad in scope. The Academy Board therefore asked the committee to begin by exploring the outlines of a possible advisory report and, if necessary, to limit the subject. After lengthy discussion, the committee concluded that the assignment was indeed too broad to address in an advisory report meant to provide the necessary focus. The ethical and legal aspects associated with collecting and using large datasets (‘big data’) throughout the entire field of science are so numerous – and important – that they merit a separate advisory procedure. In addition, the target group of an advisory report on big data is much larger and more heterogeneous than a report on issues that are limited more or less to the informatics research community. In consultation with the Academy Board, the committee has therefore limited its assignment to the following:

Identify how we can assess the ethical and legal aspects of informatics research.

Note, however, that this report will of course cover the ethical and legal aspects of big data that are specifically related to informatics research.

We wish to mention here that it is impossible to make a strict distinction between ethical and legal aspects. Whereas legal aspects concern standards and values that are enshrined in law (in legislation, case law or codes of conduct) and stipulated in rules, ethical aspects are concerned, among other things, with precisely the same norms and values. Laws and regulations also, moreover, work in part with ‘open norms’, which – given the context – require a more rigorous interpretation. This interpretation is inspired partly by the norms and values proposed by ethics.

The committee’s original assignment refers to ethical, legal, and security/safety aspects of informatics research. The committee has omitted the security/safety aspects in its own description of its assignment. It chose to do so because security/safety do not merit a separate category and can in fact be regarded as a component of ethical aspects. In the examples drawn from informatics research, moreover, this report tends to address security, and less so safety. The Academy has now installed a separate committee to explore the broader subject of big data.

**Target groups**

This report will be interesting to various target groups. In the first place, it is intended for scientists working in the fields of informatics and information technology (IT). There are ethical and legal dilemmas at every level. This report is therefore meant for the heads of research groups and for researchers themselves (including trainee researchers). We hope that this report will offer guidance to everyone involved in
advising on or assessing the ethical and legal aspects of proposed research projects. In Chapter 4, the committee advocates the installation of ethical review boards. Our particular hope is that this report will help the members of such boards get started on their work.

Second, this advisory report is intended for administrators in the academic world, for example division or department heads, faculty administrators, and the members of governing bodies.

Every day, researchers and the heads of research groups are faced with choices concerning the direction and execution of specific research projects. It is not uncommon for political choices to influence the freedom of researchers to make such choices, and this too can give rise to ethical and legal dilemmas. Discussion and awareness play a significant role. This report can therefore also be important for the political world.

Last but not least, this report addresses the general public. In the end, society is the recipient of the benefits but also the risks and dangers of the trends discussed here. That is why this report is relevant to a wider readership and therefore for representatives of the media, for example science journalists and others who act as intermediaries between science and the public.

**Defining the research area**

The committee has focused mainly on dilemmas associated with research such as that conducted by informatics departments at Dutch universities and research institutes. Most ethical and legal issues arise in a number of specific subdomains. These are:

- computer security, data security, cryptography;
- data mining, machine learning, data science;
- robotics, drones, autonomous systems;
- human computer interaction, gaming;
- reliability, software quality;
- web technology;
- wearable computing, internet of things, embedded computing.

The committee compiled this list by surveying Dutch institutions and universities.

Note: the above classification also includes research themes related to big data, for example data-mining, machine learning and wearable computing. Our classification is by no means intended to exclude such research. The above classification does exclude the wider field of big data, where we find numerous other factors and areas of study,
specifically in the field of sociology (including social media) [Dijck, José van, 2013 and 2014], economics [Davenport, 2014; Davis, 2012; Lohr 2015a and b], commerce (see e.g. [Tanner 2014]) and social criticism [Morozov, 2013].

1.3 Methods

The committee has collected and analysed information in various ways. By conducting interviews with a number of key figures in informatics research (see the Appendix ‘Interviewees and reviewers’), the committee began to form a picture of how the various institutions view this subject, and whether – and if so, how – they assess research and which dilemmas and problems they encounter. As background for the review mechanism, the committee analysed a large number of protocols and documents issued by Dutch and foreign institutions. It met several times and, based on the information it collected and its own expertise, drafted an outline of the advisory report. This outline was presented on 15 June 2015 during a liaison meeting at the Trippenhuis Building in Amsterdam. It became clear at the meeting that there was support for the outline. Some participants worried, however, that too much bureaucracy would ensue. The points raised at that meeting have been incorporated into the final version of this report. In accordance with the Academy’s customary methods, the report was reviewed by external reviewers (see the Appendix ‘Interviewees, reviewers and acknowledgements’). The committee subsequently incorporated their comments into the report.
2. ETHICAL AND LEGAL ASPECTS OF INFORMATICS RESEARCH

2.1 Introduction

Informaticians are traditionally regarded as the architects of the digital world. In recent decades, it has become clear that they are also co-architects and co-designers of the social world. Much of our social interaction today takes place through electronic channels. The way these channels are set up, who controls them, and who controls the transmission of messages across them are all crucial to the social order and society. The old truism ‘knowledge is power’ has been broadened to ‘information is power’. That means that the technical decisions made by informaticians when designing and building computer systems often have direct ethical, societal and political consequences. This is a considerable responsibility, and it also raises new questions.

For example, should informaticians explore whether there are better algorithms for protecting privacy? Should they accept commercial contracts to optimise their machine learning software to recognise or exclude certain groups (suspects, more – or less – prosperous individuals, etc.)? Should they explicitly search out bugs or vulnerabilities in existing software, and if so, what should they do if they find them? To what extent should they facilitate the use of software to put a digital lock on certain information (relevant either to the public domain or public debate), for commercial or other reasons? Is it their responsibility to consider these and similar questions proactively and to draw attention to them?
We use the term ‘informatician’ here to refer to an academic researcher in the field of informatics or an allied discipline (information science, artificial intelligence, mathematics, and potentially even areas of public administration or law). Such researchers will typically be employed by a university or other institution of higher education, but could also work for public, semi-public or private organisations that allow them a reasonable measure of research autonomy. The term ‘data’ is used below in the broad sense, i.e. it covers not only data in the strict sense of the word but also software, information and metadata generated with the help of data.

### 2.2 Typical examples of dilemmas

The security of computer systems is an important research topic in informatics. It is a fast-evolving area of research. The same can be said of the ingenuity of ill-intentioned groups that attempt to access these systems. To improve our knowledge of such security issues, we need to understand how these people operate. But research of this kind raises numerous ethical and legal questions. We illustrate this below by giving a few examples. See also examples in [CBP, 2013].

**Pobelka botnet**

A botnet is a network of infected computers that can be used for criminal purposes, for example to collect codes for digital payment transactions and make them available for fraudulent purposes. A well-known example is the Pobelka botnet dismantled by two Dutch security firms in late 2012. This network was used to steal at least 750 GB of information, including from some 150,000 Dutch computers. The security firm Digital Investigation traced 750 GB of information that the attackers had stolen from infected PCs. That included data concerning the computer network structure of a large multinational, current and upcoming cases being handled by a renowned law firm, product development information at a leading high-tech company, precisely which staff member at a certain Ministry was working on which Parliamentary query, and information circulating at various newspaper editorial offices.

Such data is especially interesting from the vantage point of research. It can, after all, reveal just how botnets function and how they can be combatted. In complex cases, researchers may also be involved in actually dismantling ill-intentioned networks of this kind. There has, however, been considerable debate as to whether researchers are permitted to use such data. To what extent is this legally and ethically permissible? Should researchers save any data that has clearly been stolen and use it for research purposes? Does the end justify the means in that case? More generally, there is the question of whether researchers are implicated in online violations when observing
such violations is an essential part of their work, for example investigations of illegal, criminal or other unlawful online behaviour (child pornography, illegal downloading, etc.).

MIFARE Classic Chip and Megamos CRYPTO-1 algorithm in Volkswagen immobilisers

The firm NXP began marketing the MIFARE Classic Chip in 1995. These chips are used in a great many security and transport systems, for example in the Dutch public transport smartcard and in millions of keycards giving access to commercial and institutional buildings and sites, including government-owned properties. The chip uses radio signals to communicate remotely with receivers built into access gates, for example. To safeguard communication and prevent exploitation, the data is encrypted using the secret CRYPTO-1 algorithm. In March 2008, researchers at Radboud University Nijmegen discovered that the chip had a security vulnerability that allowed them to analyse the CRYPTO-1 algorithm and decode the cryptographic keys, using a relatively straightforward method. By combining these two points, they were able to clone a keycard.

As is customary in security research, the relevant researchers notified the chip manufacturer by means of a ‘responsible disclosure’ procedure (see the Glossary for a definition). Since the chip is used in numerous government and other systems and in the public transport smartcard, the researchers also notified the Dutch government and significant users. They also informed them that they would be publishing the results of their research in the conference proceedings of the ESORICS conference, although they would observe an embargo period to give NXP the opportunity to take action.

NXP responded by petitioning the court to prohibit this publication on pain of a one million euro penalty. NXP also asked the court to order the researchers to do everything within their power to force the conference organisers and reviewers to maintain confidentiality. NXP claimed that publication would violate its intellectual property rights, which would be an unlawful act. The District Court of Arnhem rejected the claim, however. In its view, there was not enough evidence to demonstrate that the chip’s algorithm was a copyright-protected work or eligible for protection of writings. NXP had not, moreover, made sufficiently clear why the right to publication should be restricted [Rechtspraak.nl, NJ 2008, 544, Computerrecht 2008, 140 with annotation by S.F.E. Verdonck].

Foreign courts sometimes rule otherwise in similar cases. In 2012, researchers in the same Radboud University group discovered vulnerabilities in the Megamos crypto algorithm, used in the electronic immobilisers installed in several makes of car,
including Volkswagen. Once again, they reported the weakness to the Swiss firm of EM Microelectronic by means of a responsible disclosure procedure. When Volkswagen heard that the researchers intended to publish their findings, they petitioned the court for an injunction. Because the paper’s lead author had taken a job in the United Kingdom by that time, the case was brought before the court in London. Volkswagen argued that publication would pave the way for the theft of millions of automobiles. In June 2013, the court in London found for Volkswagen and issued an injunction prohibiting publication. In the court’s view, Volkswagen’s interests outweighed the freedom of publication. The injunction lasted two years and was only cancelled after lengthy, time-consuming negotiations [Mols, 2013, Hof, van ’t, 2015].

**Research on effectiveness of blocking access to The Pirate Bay**

The Pirate Bay is one of the best-known websites for sharing files, usually those protected by copyright. The site makes it easy for users to share music, films or games with each other. Founded in Sweden in 2003, it was one of the 100 most-visited websites worldwide in 2013. A powerful entertainment industry lobby has been making a global effort to shut the website down. In the Netherlands, the anti-piracy foundation BREIN commenced litigation to force internet service providers to block access to The Pirate Bay. On 11 January 2012, the District Court in The Hague ruled in its favour and ordered ISPs Ziggo and XS4ALL to block access to The Pirate Bay. The ISPs protested but submitted to the ruling.

Given the dynamic nature of the internet, experts expected the bans to have little effect because users would quickly find ways of circumventing them. Until then, however, researchers had never actually studied the effect of such bans. A thorough understanding of that effect would be beneficial for the Dutch chapter of the ISOC (Internet Society Netherlands) and for both parties in the dispute, for example. Researchers at the University of Amsterdam therefore developed a tool that is able to measure the effectiveness of these bans. The tool collects data from The Pirate Bay website, including the IP addresses of individual users. The data collected in this manner is therefore sensitive and obtained from a website whose methods are legally and ethically debatable.

**Grindr**

Grindr (http://grindr.com) is a geosocial networking app for smartphones that facilitates communication between gay men. A geolocation function allows Grindr users to see which other users are in the area. The user interface displays small profile photographs of other Grindr users, arranged by distance (from nearby to far away). By
clicking on a profile photo, the user can view a short profile, use a chat function, send photographs, or report his own location.

Grindr was launched on 25 March 2009 by the US firm Nearby Buddy Finder, LLC. It soon became a worldwide hit. On 18 June 2012, Grindr announced that it had 4 million users in 192 countries, of whom 1.1 million were online daily. More than 1.5 million users are resident in the US, and London tops the charts as having the most users of any city (350,000). Grindr has approximately 15,000 users in the Netherlands.

Students in the System and Network Engineering research group at the University of Amsterdam discovered a vulnerability in this smartphone application. The vulnerability made it possible for them to access the underlying database and to manipulate the data. Given the nature of this application, the data is extremely privacy-sensitive. The vulnerability was reported to Grindr in accordance with a responsible disclosure procedure (see the Glossary for a definition).

2.3 What can we learn from medical research reviews, for example?

The Dutch Clinical Trials Act [Wet Mensgebonden Onderzoek, WMO] stipulates that medical research involving human subjects must be reviewed by an independent panel of experts. Such research is subject to the Act if it meets the following two criteria:

1. the research is medical in nature, and
2. human beings are subject to treatment or behavioural strictures.

The sole purpose of the Act is to protect human test subjects. This means that only their interests need be taken into account, without any obligation to consider all manner of broader ethical factors. Medical treatment that takes place within the context of patient care is also not covered under the Act and does not need to be submitted to a review board. Before a clinical trial can begin, it must be approved by a review board. There are two types of board in the Netherlands: the Central Board on Research Involving Human Subjects (CCMO) and 24 regionally certified Medical Ethics Review Boards (METCs). Most are associated with a university medical centre, a hospital or other such institution. In legal terms, however, the boards are autonomous administrative bodies (ZBOs) and are therefore legally independent.

Most medical research is assessed by an METC. Virtually every study involving competent adults is subject to review by an METC, as is therapeutic research and non-therapeutic observational research involving minors and adults incapable of giving informed consent. The law stipulates that certain types of studies must be reviewed by a single board in which expertise has been concentrated. That is the CCMO. Such
studies must be assessed on specific or specialist ethical, legal or societal aspects. That was the case for cell therapy studies, xenotransplantation, and stem cell research, for example. For more information, see www.ccmo.nl.

**METC requirements**

Only certified METCs may review research. To qualify as an METC, a review board must satisfy statutory requirements regarding composition, members’ expertise, methodology, and minimum number of reviews per annum (see Table 2.1).

<table>
<thead>
<tr>
<th>Requirements for METC certification</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Composition</td>
<td>Must consist of at least: one or more physicians, a legal specialist, an ethicist, a research methodologist and someone who represents the views of the test subjects. If the board is also to review drugs research, it must also include a hospital pharmacist and a clinical pharmacologist (may be represented by a single person).</td>
</tr>
<tr>
<td>Bye-laws</td>
<td>Must have bye-laws establishing certain minimum requirements regarding autonomy and so on.</td>
</tr>
<tr>
<td>Methods</td>
<td>The METC’s methods must be properly identified and described.</td>
</tr>
<tr>
<td>External experts</td>
<td>An METC must call in external experts if the relevant research so requires.</td>
</tr>
<tr>
<td>10 Protocols requirement</td>
<td>An METC is expected to review a minimum of 10 research proposals a year.</td>
</tr>
</tbody>
</table>

**Grounds for review**

The Act stipulates that an ethics board can only issue a positive review of a research protocol if that protocol satisfies a number of criteria. For example, the researchers must make plausible that the proposed study could produce new medical insights and that such insights cannot be achieved with other, less radical forms of medical research. Other requirements concern the staff actually conducting the experiments and the need to adequately safeguard the interests of the human test subjects.
Practice

To summarise, the procedure for reviewing the ethical aspects of medical research are as follows.

• The researcher decides whether the study must be reviewed under the Act.
• If so, he or she submits a research protocol to an METC or the CCMO.
• The METC or CCMO reviews the protocol on the basis of:
  – admissibility
  – statutory stipulations (specifically for test subjects incapable of informed consent)
  – comparison of pros and cons for individual or group

The review mainly considers the consequences of the research for the test subjects. Aspects not considered in the review include:

• group effects
• risks posed to society
• risks involved in treatment

Usefulness of medical research mechanism for informatics research

Because the ethical review of medical research places a heavy emphasis on the consequences for test subjects, the lessons that it can impart have only limited usefulness for informatics research. Very little informatics research involves human test subjects, while the ethical dilemmas that it involves are highly specific in nature. In addition, there is no statutory obligation to submit informatics research to an ethics review board. The statutory requirements to which an METC is subject (in terms of composition, methods and bye-laws) may, however, be useful for setting up ethics review boards in the field of informatics (see Section 4).

2.4 Conclusions

CONCLUSION 2.1
Society in general, but also – and in particular – research funding bodies are increasingly asking scientists to conduct an exhaustive review of the ethical aspects of their research. That is the case in many disciplines, but certainly in informatics, given its enormous societal impact and importance. We must develop an ethical infrastructure for informatics. This means that a transparent and distinctive review mechanism must evolve about which the field has reached consensus. In addition, we must seek out an assessment method that is scrupulous and robust but that also operates efficiently without being too bureaucratic.
CONCLUSION 2.2
The medical sciences have already gained considerable experience in the ethical scrutiny of research. Because it places heavy emphasis on the consequences for human test subjects, however, the system used in medical research cannot simply be transferred across the board to informatics research. The ethical issues involved in informatics research are highly specific to the field. Moreover, the law does not prescribe any form of ethical assessment for informatics research. That is why informatics can draw on the experiences of the medical disciplines but must develop its own review mechanism and assessment method.
3. LEGAL ASPECTS

3.1 Introduction

The collection or processing of personal data is very common in informatics research, as is the investigation of software or computer systems that are the property of others. That is why this type of research quickly raises legal questions, for example concerning privacy or intellectual property rights. This advisory report is not an exhaustive study of what the law does and does not permit and the conditions and circumstances that apply in either case. That would be beyond the remit of the committee. Moreover, the specific outcome of the applicable statutory framework depends heavily on context. That is why legal expertise must usually be called in in such cases. What we do in this chapter is outline the most important legal conditions for and implications of informatics research. We do this by assessing the intellectual property and privacy implications of various stages of such research.

The committee realises that the relevant statutory and regulatory context consists of more than the regulatory framework of these two domains alone. It also, for example, encompasses liability, computer crime, statutory provisions concerning security, and the integrity of systems. In our view, however, issues related to intellectual property and the protection of privacy take precedence and – as we will see – turn out to be relevant in virtually every situation. At the end of the chapter, however, we briefly address the special responsibility with which researchers are charged by the law and jurisprudence, i.e. the duty of care. For example, in what situations do informatics researchers have a duty not to ignore suspect or unusual patterns? Examples might include evidence obtained during their study that third parties are exploiting a security vulnerability. For years, the US National Security Agency (NSA) made use of an internet security vulnerability (known as ‘Heartbleed’). Instead of reporting the vulnerability to the relevant parties so that they could repair the system, the NSA
ethical and legal aspects of informatics research

monitored it in secret and, in doing so, violated the privacy of many individuals worldwide. The NSA is certainly not the only one to make improper use of security vulnerabilities. There is a commercial market for ‘zero-day exploits’, i.e. software developed especially to exploit security vulnerabilities, for example an ISP’s (see also the Glossary). A zero-day exploit can attack an IT system without the system’s vendor being aware of it. In short, those who control an exploit can monitor in secret, intercept data, install viruses and so on. If informatics researchers come across such practices during their research, their duty of care obliges them to take action, for example by pointing out the vulnerability to the system’s vendor, so that it can distribute a security update to users that disables the exploit [Prins, 2014; Grossman, 2014]. Duty of care issues arise most often in two categories of research that are highly commonplace in this field: research on software vulnerabilities and research that uses databases containing privacy-sensitive information (see also the cases in Chapter 2.2).

3.2 Choice of research subject

One type of research that is very common in informatics involves a computer security analyst studying the workings of an existing software package. For example, an analyst might study how an app streams data on a smartphone or tablet to find out which data it transmits from and to the user and to whom data is being transmitted. He or she might also study the extent to which a hacker can influence the workings of a pacemaker, a bank ID card, a voice-operated computer, or built-in automotive software.

The first question, of course, is whether a university-appointed informatician should even be studying such matters. There is little disagreement in that regard; in many cases, the public interest involved in such research justifies any negative consequences for enterprises, authorities or individuals. Critical and independent investigation of existing methods and techniques is common in other areas as well (for example research on the side effects of drugs), and has a long academic tradition. In some cases, the relevant manufacturer will be aware of the investigation, but that is also often not so.

The second question concerns the choice of research subject. In academic research, that choice is often the outcome of a fairly random procedure influenced by many different factors: the individual researcher’s personal interests or expertise, the availability of funding, the current state of science and, in turn, the potential contribution the investigation will make to scientific innovation, the social or commercial relevance of the study, and how accessible the software is. In practice, this type of vulnerability study often focuses on software in ‘small’ devices such as smartcards or smartphones because they are relatively easy to access compared to large-scale software systems managed by other parties.
Important points

When researchers select the research subject themselves, they must provide hard evidence of its scientific or social relevance, especially because the non-scientific implications of informatics research of this kind can be extremely significant. It is particularly important for them to clarify who stands to lose out – or perhaps profit – and in what way when data security fails and when such failures are revealed. If the researcher or the institute for which he/she works has a vested interest of any kind, it must be stated explicitly. The committee believes that such research should be undertaken only in the absence of such vested interests.

In addition, prior to commencing the study, the researchers must examine whether it could infringe the rights and interests of others. For example, by breaching a security system, the study may violate the right to privacy or intellectual property rights of parties other than the system’s vendor. If that is a possibility, the researcher or relevant research institute must explicitly weigh the scientific and societal interest that the study will serve against the third-party rights that may be violated. In doing so, the researcher or institute must be acutely aware that the ends do not always justify the means. If the violation of third-party rights goes too far, then it may be better not to carry out the study at all or only in modified form. The researcher must also ensure compliance with certain statutory requirements, for example adequate protection of any personal data involved in the study. Even if the researcher has taken the various interests into account, the study may still be contrary to the law in certain circumstances, for example because it violates the titleholder’s copyright in the software being investigated.

3.3 Legal aspects in the various research phases

This section discusses a number of issues that arise during the various phases of research and how they can be addressed.

3.3.1 Data acquisition and management

As soon as the research subject has been identified, the next step is usually to start collecting data. In research investigating software and data collections, research data can be acquired in different ways. The software may be available for free (open source), for payment, or be included in the purchase of a device. In the latter case, the researchers must first construct a memory dump, an activity that may involve breaching security in some way. The software can also be obtained illegally, for example from a pirate website. It will not always be at all clear who the software’s titleholders are, which rights are applicable, or what conditions apply under a possible licence. The software
may also be ‘sensitive’ and therefore not generally known. That would be the case if it were software used in bank ID cards. Subjects that could lead to legal or ethical dilemmas in this research phase include source reliability, secrecy, anonymisation, reverse engineering and secure storage. Researchers who study software and databases perform actions that can sometimes be regarded as legally relevant, for example duplication of software and databases under copyright protection. The consent of the titleholder may be required in that case. The following measures reduce the risk of legal problems arising.

• Document the source of the software as clearly as possible, including the applicable rights in the software or database. If the software or database is subject to intellectual property rights (copyright, patent or database rights): see whether it can be used under licence or one of the statutory grounds for utilisation. Note that it is only in very rare cases that statutorily legitimate grounds for utilisation apply. If a licence permitting use of the software is not yet available, then it must be obtained.

• Ensure the encrypted storage of sensitive software, where possible on a fully isolated medium that is not connected to the internet. Ensure encrypted communication in cases where multiple researchers are collaborating and results and findings are exchanged by email, for example.

• Ascertain whether use of the software involves personal data. If so, identify the reason for using this data and ensure that such use complies with the various requirements of scrupulousness stipulated in the Dutch Personal Data Protection Act [Wet bescherming persoonsgegevens].

3.3.2 Data processing and use

The software acquired in the previous stage may not be in a human-readable format. If not, it will have to be decompiled first. The process of disassembling and analysing the workings of a device (or its software) is an element of reverse engineering. EU Directive 2009/24, on the legal protection of computer programs, states that reverse engineering is only permitted by law in specific cases (see Insert 3.1). Briefly, that means that:

• decompilation/reverse engineering is not allowed if not explicitly permitted in the software licence. Proprietary licences generally do not permit this.

• Observation, study and testing are allowed as long as they involve actions covered under the licence, or actions necessary to use the software (i.e. to load and run the program). This can be useful when studying how an app streams data on a smartphone or tablet to find out which user data is being transmitting where. Other types of study may well require decompilation, but Art. 5(3) of the EU Directive on legal protection of computer programs provides no basis for this (assuming that it is prohibited under the licence).
• According to Art. 6 of the Directive, *decompilation/reverse engineering* is permitted ‘to achieve the interoperability of an independently created program with other programs’, provided that it is restricted to the parts of the program that provide for interoperability (i.e. the ‘interfaces’). Given its limited scope, this provision will have little if any usefulness for security research. Whether the provision would be useful for security research focusing on interface security between computers is unclear; so far there have been no court rulings on this question.

**INSERT 3.1:**

**ART. 5(3) EU DIRECTIVE ON THE LEGAL PROTECTION OF COMPUTER PROGRAMS AND ART. 45I DUTCH COPYRIGHT ACT [AUTEURSWET]**

A licensee who has obtained a lawful copy of a computer program may observe, study, or test the functionality of this program without the consent of the titleholder in order to determine which ideas and principles underpin any element of that program as long as that person's acts are covered by that licence; he or she may also load and run the program and perform other acts that are necessary to use the computer program provided that he or she does not infringe the exclusive copyright in that program.

Important to the data processing stage is for the researchers to understand, model, analyse and test the software. Testing may involve interaction with ‘live’ systems. For example, if the study concerns an app's communication behaviour, the researcher will want to have a specific user try out the app. The user will try out various user options that the software titleholder may or may not have anticipated. The owner of the server to which the app is connected may detect such unforeseen behaviour and respond to it in some way that has consequences for the user. A similar situation may arise when a manipulated bank ID card or public transport smartcard is read by a standard card reader. To the extent possible, testing should be carried out in the researcher's own environment, separate from any third-party infrastructure. The researcher must have urgent reasons for bringing the software into contact with the ‘live’ environment. He or she must avoid damaging that environment in that case. In particular, access must never be in any way personally advantageous for the researcher, nor should he or she be able to inspect or alter protected data. Because testing and the possible processing of software or databases for that purpose may require a legally relevant act (they involve ‘duplication’ of software or ‘derivation’ of data), the titleholder to the software or databases must, in principle, consent to the act. Specifically, this means that the titleholder to the software and/or environment must be informed about the experiments in advance. Article 6:162(2) of the Dutch Civil Code, concerning unlawful acts, makes provision for the possibility that, in specific cases, certain circumstances may justify annulling the unlawful nature of an unlawful act. In short, researchers can find justification for their tests in the legal doctrine of the unlawful act, but they must be able to demonstrate beyond a doubt that the circumstances justify violating third-party rights. Generally speaking, these circumstances will need to touch on more than the interests of science alone but also affect the public or general interest.
The following measures reduce the risk of legal problems arising.

- When testing software and possibly breaching data systems, researchers must do everything possible to preclude their or other research group members’ being able to inspect third-party personal data that may be present in the system. Researchers’ first priority is to adhere to the principle of data minimisation, i.e. to keep the amount of personal data involved in the study to a minimum. They must also satisfy the other standards of scrupulousness stipulated in privacy legislation.
- If researchers encounter serious vulnerabilities in this phase of their study, the ‘problem owner’ (usually the software vendor) must be informed as quickly as possible. This is the first step in the responsible disclosure procedure. The researcher must also share any knowledge that will help remove the vulnerabilities. The omission or delay of responsible disclosure can be justified in this phase only if it becomes clear that the problem owner can or will shut down the research immediately on unreasonable grounds, for example by taking legal action.
- It often takes irrefutable evidence to convince a problem owner that the software contains a vulnerability. Such evidence should be minimal / innocent / symbolic. It may, for example, consist of a list of files stored on a protected system (without showing their sensitive content) or an unauthorised transaction valued at 1 euro-cent.

3.3.3 Distribution and publication of research results

This phase may well give rise to dilemmas if the study has uncovered security vulnerabilities. Where that is the case, the researchers involved must focus on removing the vulnerabilities as quickly as possible while simultaneously minimising any damage. Both points go without saying, but one does not necessarily lead automatically to the other. The fastest way to remove a vulnerability is to disclose it; it is then that vendors feel the greatest pressure to solve the problem. Disclosure of a software vulnerability increases the risk of exploitation, however. There is a further risk that the vendor will sue the researchers or research institute for damaging its reputation or claim damages of another kind. The claim may even be successful if the researchers failed to act with the necessary scrupulousness when publishing their results. On the other hand, vendors do not always take action when a vulnerability is reported confidentially, so that the vulnerability remains (and is eventually discovered and exploited by others).

Disclosure of vulnerabilities is standard practice in cryptography and computer security. It forms part of a scientific process that produces the best possible security mechanisms, with some researchers engaged in ‘making’ and others in ‘breaking’. There is broad acceptance, even outside academia, that keeping vulnerabilities ‘under wraps’ does more harm than disclosing them. It is, however, important to do so responsibly, through responsible disclosure. Responsible disclosure involves:
• notifying the problem owner about the vulnerability at an early stage;
• offering to help remove the vulnerability;
• after a period of grace, disclosing the vulnerabilities (to prevent zero-day attacks).

Problem owners must of course be informed about the intention to disclose the vulnerability. There is sometimes discussion about how long problem owners should be given to resolve the problem (in other words, the length of an embargo on publishing research results). The Dutch Ministry of Security and Justice has published guidelines for responsible disclosure that indicate a sixty-day embargo for software and a six-month embargo for hardware. In practice, however, this need not set limits on the research process. If the researchers inform the problem owner prior to submitting their paper to a conference or journal, then there is usually enough time to resolve the problem before the paper is actually published.

Under the Dutch responsible disclosure policy, company websites must describe how vulnerabilities should be reported and how they are then handled. The experience of some bigger companies (KPN, banks) with responsible disclosure have been positive.2 The biggest disadvantage—and risk for researchers—of the procedure is that the problem owner will use the report not to remove the vulnerability as much as to silence the messenger. Problem owners can do this by intimidating researchers, holding them liable, seeking a court injunction to halt publication, or a combination of the foregoing. This is a realistic risk. In 2008, NXP initiated summary proceedings asking the court to issue an injunction on researchers at Radboud University who had uncovered vulnerabilities in the company’s MIFARE Classic Chip. The Dutch court did not issue the injunction, partly because it would have placed restrictions on freedom of speech. In 2013, Volkswagen obtained an injunction from a London court in a case concerning chip vulnerabilities in immobilisers. The injunction lasted two years and was only cancelled after lengthy, time-consuming negotiations. The paper, which was finally published in 2015, differs from the original by only one sentence (see cases in Section 2.2).

The following measures reduce the risk of legal problems arising.

• In the interests of responsible disclosure, no preprints of a paper should be published on the web. Researchers are advised to notify the conference programme committee (in the person of its chair) or the editor of the journal about the sensitive nature of the paper, so that the referees and others can be informed accordingly. It is important that all these persons are aware of their duty of confidentiality. At the same time, these parties will want the researcher or his/her institute to submit an indemnification statement. Researchers are advised to consult a lawyer about this.

2 See for example the article by Dutch landline and mobile telecommunications company KPN in: http://cryptome.org/2014/01/nl-cyber-sec-2013.pdf.
• The paper itself should focus on the scientific aspects of the vulnerability, for example the design flaws, the necessary methodological or other improvements, and the lessons learned. The authors must do everything possible to avoid turning it into a manual for hackers. They can do this, for example, by publishing the mathematical background but not a detailed exposition in the form of ‘attack software’. They must also avoid any situation whereby the results can be used to unearth personal data and, consequently, the identity of individuals.

• Where research might provoke commercial enterprises to take legal action, the researchers should inform the head of the relevant research institution in advance. Legal action of this kind may pose a considerable financial risk to the entire institution, and require a great deal of time and energy from its management; in many such cases, summons are issued against both the research institution and the researchers. Because summons may also be issued against the researchers as part of a strategy of intimidation, the attendant risks must also be assessed.

• In the Netherlands, the risk of an injunction being issued on an academic publication seems small if the researchers have proceeded with the scrupulousness expected of them by the prevailing scientific standards, have acted in the general interest and dealt scrupulously with any third-party interests, have not used any illegal sources, have not caused unnecessary damage, and have complied with the responsible disclosure guidelines. If any of the co-authors are foreign, legal proceedings before a foreign court are possible, however. Rulings by foreign courts may differ from those of Dutch courts (see the MIFARE case in Chapter 2).

3.3.4 Storing and archiving both the data and the research results

After the research results have been published, both they and the underlying research material and accompanying correspondence must be archived and stored. It is important to do so for purposes of perusal and accountability in the future. It is far from customary for published research results to include the underlying research material. Researchers must therefore be especially careful to archive this material. If it contains data that can be traced to natural persons or identifiable enterprises (other than the titleholders or those responsible for the software or databases investigated), then the researchers must even archive it in anonymised form. They must also consider to what extent archiving underlying material complies with any relevant intellectual property rights. Where necessary, contractual arrangements (licence) should be made. Finally, it is important for researchers to realise that the applicable rules of law may be at odds with ethical considerations. For example, propagating an Open Access policy for ethical reasons may conflict with the protection of privacy. That is why extra care must be taken to weigh up the various interests involved within the specific context in which the study is taking place.
3.4 Informatics researchers and their duty of care

Both private law – specifically, the law on unlawful act – and criminal law – in Art. 450 of the Dutch Criminal Code – hold that persons can be held liable for remaining passive in certain situations. The assumption here is that liability, and with it penalisation, are called for because certain forms of passiveness are unacceptable in our society. One well-known example is that of an observer standing on the edge of a pond who fails to help a drowning child. It is difficult to say in advance where the precise boundaries are between the legal obligation to act, to warn, and to provide assistance. However, in situations in which a passive observer acts in a certain capacity and, as a result, has a duty of care towards the victim, he or she is more likely to be held liable. Duties of care can be reinterpreted for the digital environment and are consequently also applicable there. The specific capacity that imposes an extra measure of responsibility on an observer may in some instances apply to informatics researchers, in view of their expertise. In other words, if the idea is not to remain passive but to raise the alarm after observing anomalies associated with system vulnerability, then it should be possible to expect more from an informatics researcher than from the average internet user. The committee advises researchers and research groups to be vigilant about detecting irregularities in systems and to facilitate reporting matters to the enforcement authorities where necessary.

3.5 Conclusions

CONCLUSION 3.1
When selecting a research subject, researchers should give top priority to the interests of science and offer solid arguments for why their research will serve the interests of society. They should clarify how and to what extent their findings could affect the interests of third parties, including their privacy and intellectual property rights. Researchers and other relevant stakeholders should explicitly weigh the scientific and societal interests of their research against the interests of any third parties whose rights may be infringed. In short, the end does not always justify the means.

CONCLUSION 3.2
Informatics researchers have a duty of care. This means that remaining passive in certain situations could lead to their being held liable. Researchers and research groups should therefore remain vigilant and report any perceived risks to persons and society to the compliance officers within their own organisations and, where necessary, to the enforcement authorities.
4. ETHICAL REVIEW BOARDS

4.1 Ethics and Information Technology

The ethical issues associated with IT have been the subject of study in the field of ethics since the 1980s. A voluminous literature has evolved in the field of computer ethics.\(^3\) This evolution originated in the United States. The Institute of Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM), as well as the International Federation for Information Processing (IFIP)\(^4,5\) have close ties with this research community, resulting in a series of codes of conduct, protocols and ethical principles for informatics researchers and IT professionals. The field of internet research\(^6\) has a substantial body of literature. However, much of it was initiated in the social and behavioural sciences and mainly concerns social media and the internet. At present, it does not yet offer any well-defined guidelines for Ethical Review Boards (ERBs) in informatics.

The pragmatic approach that we have chosen to take in this advisory report is consistent with key insights obtained in computer ethics in recent decades. These include:

(i). Computer technology has specific properties that give rise to unique moral issues (for example concerning artificial intelligence and autonomous systems);

\(^3\) (See for example, *The Cambridge Handbook of Information and Computer Ethics*, Floridi (ed.) CUP, 2010); and the entry on ‘Computer Ethics’ (by Terry Bynum) in *The Stanford Online Encyclopedia of Philosophy*.)


\(^5\) [http://courses.cs.vt.edu/professionalism/WorldCodes/IFIPRecommendation.html](http://courses.cs.vt.edu/professionalism/WorldCodes/IFIPRecommendation.html)

(ii). Computer technology is a meta-technology and it is therefore omnipresent wherever there is smart technology;

(iii). The ethical values upheld and the choices made by researchers and designers influence the design of IT products and services. In other words, IT is not a value-neutral phenomenon, but bears the values of its makers, designers, researchers and conceptualisers;

(iv). Assessing IT involves not only computational artefacts, algorithms, software, IT architectures and IT infrastructures, but also socio-technical systems that encompass hardware and software as well as social (guidance, user instructions and customs), legal and institutional aspects. The entire sum of these parts and components and the interaction between them are the true practical significance of IT products or services. The story is the same outside the domain of IT: a nuclear power plant can only be safe if reactor design is accompanied by numerous specific measures, special institutions, laws, expertise, protocols, and a culture of safety. Scrutiny of informatics research must continuously allow for the way in which the research results are or could be embedded in the broader social context.

It is beyond the remit of this report to provide an overview of the literature and the state of research in the rapidly growing field of applied computer ethics. Interested readers should consult a number of recent survey and introductory articles [Hoven, 2010; Sullins, 2012; Zevenbergen, 2015]. Here, we suffice by providing a practical mechanism for reviewing the ethical aspects of informatics research in the Netherlands.

4.2 Ethical review at knowledge-based institutions

Chapter 1 already referred to the stricter requirements that EU research funds impose on the ethical quality of research proposals and the underlying reasoning and arguments for this approach. It is no longer enough to fill in a form and tick enough right answers in a list of questions to gain funding approval. This raises questions about the nature of the expertise involved, its locus, and the institutional context of ethical evaluation in the broad field of informatics research. Where, by whom, and in what manner should the ethical aspects of informatics research proposals be reviewed? The answer to this question must allow for the lessons learned working with similar review authorities and bodies in other disciplines, such as medicine. In addition, any new authority must adapt itself to the ecosystem of ethical evaluation that has recently taken shape in the world of research and higher education. After all, multiple authorities have been added in recent years to the list of those charged with deciding on ethical issues, e.g. committees concerned with labour conflicts, sexual harassment, equal opportunity, academic integrity, intellectual property matters, liability, and corporate
governance issues associated with participations in start-ups. In other words, a fairly dense institutional infrastructure has emerged at universities whose reach extends to a wide range of ethical matters, or issues that involve significant ethical aspects. The question that is now being raised concerns an authority that can assess the ethical aspects of technical, engineering and, more specifically, informatics research, alongside those that already exist in medicine and health care (medical ethics review boards), behavioural and social science research (human trials board) and research involving laboratory animals (animal testing board).

4.3 Ethical Review Board for Informatics (ERBI)

4.3.1 Need for an ERBI

The committee believes it would be advisable to extend the existing ethical infrastructure at Dutch knowledge-based institutions to cover the ethical review of research and research proposals submitted by researchers affiliated with institutes or faculties and departments that conduct research in the broad field of informatics in general. Such research exerts no less influence on human beings and society than medical, behavioural and social science research. Informatics research may well be more far-reaching and has at least as much impact as medical research, and it can affect the interests of those involved and of society just as forcefully as medical and behavioural science research. It also represents a sizeable societal and economic sector with all the attendant controversies and differences of opinion. Informatics is also a unique and distinctive field. In the committee’s view, this is reason enough to establish its own ethical review procedure. An Ethical Review Board for Informatics (ERBI), to which researchers can submit proposals for effective and efficient review, should consist of independent informatics researchers with special expertise, at least one legal specialist, and an ethicist (both with an understanding of and affinity for IT issues).

Some institutions have already started experimenting with such a structure. For example, the Electrical Engineering, Mathematics and Computer Science Faculty at the University of Twente established an Ethics Committee some time ago, and the University of Amsterdam, VU University Amsterdam and the Center for Mathematics and Computer Science (CWI) have installed a joint Ethical Committee for Information Sciences. The University of Twente has also appointed an ethics advisor who can help researchers work through ethical dilemmas. Delft University of Technology has established a board that focuses on the conduct of human trials in the setting of a university of technology. However, the scope of this board makes it possible to submit research proposals that do not involve human test subjects, but use only personal data.
It is important for an ERBI to clarify which aspects it can advise on to avoid confusion with other boards, such as the medical ethics review boards, the animal testing boards, and the academic integrity committees (plagiarism, fraud, etc.). There are also questions of demarcation concerning the relationship between law and ethics. Legal and ethical questions are always difficult to untangle. This is especially true in informatics because things are changing so quickly, often resulting in conceptual confusion, and confront us with new phenomena. The result is a constant stream of normative ethical issues in a legal terra incognita. Questions also arise concerning IT issues that we can expect will be subject to regulation in the foreseeable future. That makes it very important to have a legal specialist on the ERBI.

### 4.3.2 Tasks and success factors

In the committee’s view, the ERBI would have three important tasks:

1. Its first task would naturally be to review the ethical aspects of informatics research. Ideally, research that clearly raises ethical issues would commence only after the relevant proposal is given the greenlight by the ERBI.
2. Second, the ERBI would promote the necessary continuing professional development, so that researchers and institutions can account for their informatics research in ethical terms, based on informed judgement.
3. Third, the ERBI would contribute to its organisation’s ethical learning process, and it would embody the core and promote the continuity of a community of expertise in which knowledge concerning this subject is documented and continues to advance. We are, after all, dealing with a field that is in the throes of development (and will remain so), and in which shared learning is important.

The committee’s interviews and liaison meeting have revealed considerable support for this idea. Some individuals have expressed worries about the review process becoming too bureaucratic and time-consuming, however. Other points of debate have concerned the mandate and composition of the ERBI. Based on these comments and initial experiences working with a number of ERBIs, the committee believes that a number of factors are important to ensure the success of an ERBI:

i. **Proximity to and support within the community.** ERBIs will only be robust if the distance between them and researchers is minimised, both physically and in terms of sentiment. If one or more members of the ERBI were to come from a researcher’s own unit, he or she would feel less hesitant about requesting its opinion at an early stage. To increase support, members of the ERBI must be regarded as authoritative by their fellow researchers. That will also speed up recognition of the ERBI as a distinct entity. Local proximity also has practical
advantages, as more frequent meetings of the ERBI become easier to organise. That is why the committee prefers local ERBIs (within a faculty, research institute or university) to a national ERBI for all informatics research, for example. There is also a drawback to proximity, of course: an applicant and a reviewer may be too well acquainted. Care must be taken to avoid conflicts of interest owing to close working relationships between reviewers and researchers. The customary rules for reporting potential conflicts of interest when reviewing and refereeing papers, manuscripts and research proposals should also apply here.

ii. *Speed.* Frequent meetings and speed in reviewing proposals will both help ensure the robustness of ERBIs and the confidence that researchers place in them. Researchers are often under great time pressure and face inexorable and important deadlines. To ensure that the ERBIs can manage a large number of research proposals efficiently, we propose a selection and review procedure in Chapter 5.

iii. *Status of the opinion.* The normative status and legitimacy of an ERBI's opinion will both be important. Although researchers are expected to have made their own ethical assessment, and although they cannot discharge themselves from their moral responsibility, they must be able to depend on the judgement of the ERBI. On the other hand, the ERBI members must be indemnified by the university against liability claims. The ERBI should be appointed by the governing body or executive board of the relevant research unit. The ERBI will also make official recommendations to the executive board or governing body about whether or not to proceed with a research proposal. Operational responsibility for following up these recommendations should lie not with the ERBI but with the governing body. The ERBI should maintain a proper archive, including minutes of its meetings, and should be accountable to the governing body or executive board (preferably on an annual basis).

iv. *Scope and demarcation.* An ERBI should make crystal clear what purpose it does and does not serve. To do that, it must answer a number of questions. The first concerns the disciplinary background of the applicants. The ERBI's work should not be limited to proposals originating in informatics faculties, but also review proposals from other faculties that conduct informatics research. At universities of technology, for example, faculties of mechanical engineering (robotics and high tech systems), civil engineering, aerospace engineering, and systems engineering, policy analysis & management also carry out informatics research.

v. *Scale and locus.* Not all faculties are large enough to generate a sufficient number of proposals, so they could decide to work together or to set up a joint ERBI. It is important for these local boards to coordinate their work and learn from one another, however. Ideally, the ERBIs should form a network that functions as a learning organisation. The Academic Integrity Committees (CWIs) can serve as an example. In just a few years' time, all Dutch universities have established CWIs. The Royal Netherlands Academy of Arts and Sciences (KNAW), the Netherlands Organisation for Scientific Research (NWO) and the Association of Universities
in the Netherlands (VSNU) have together founded the Netherlands Board on Research Integrity (LOWI), to which petitioners can appeal decisions taken by the governing body of their own university. The chairpersons of the CWIs now also meet at national level to discuss lessons learned and to share best practices and anonymised ‘ethical case law’. They also plan to make recommendations to the VSNU about additions to the Netherlands Code of Conduct for Academic Practice. A similar process of institutionalisation would work for the ERBIs. The committee believes that ERBIs should not embark upon this independently, but should work with other ERBIs. They can engage in a process of peer-review, for example by coordinating predetermined standards and case histories, and by sharing ideas and experiences. SURFnet is an example of a network that has worked with a similar structure. SURFnet has set up a community consisting of the members of the Computer Security Incident Response Teams or CSIRTs associated with its affiliated institutions. This community aims to generate synergies among security experts and organises meetings and training courses for that purpose. The community members set the agenda for the meetings themselves. The community has also drafted membership rules and a code of conduct.

**Distributed research projects**

Research projects are increasingly undertaken in cooperation with other institutions. This also makes demands on the way in which ERBIs will be organised and how they can coordinate their actions with one another. Dove et al. (2016) identified and analysed one particular point of concern for setting up a robust ERBI network. In their paper, they looked at the ethical aspects of multi-site research, i.e. research distributed across different institutions, locations, or even countries. This is a common situation in international research with a heavy emphasis on data. There are no top-down international regulations for such research, and that is why bottom-up approaches have been developed in a few places.

Dove et al. sketch three principles and accompanying models facilitating mutual coordination between sites in the case multi-site research, which could therefore involve multiple ERBIs. The ‘reciprocity’ model is based on the principle that the members of an ERBI network recognise one another’s decisions. Advantages of this model are that it allows the process to remain flexible and preserves local autonomy. Disadvantages are the ‘danger’ of inconsistent or incompatible opinions, confusion about quality differences between the opinions of differing members, and a troublesome implementation process during the start-up phase.

The ‘delegation’ model is based on the principle that the members of the network decide as a group which member or members should review the relevant research.
Advantages of this model are that there is less risk of inconsistency and that it is possible to divide up tasks based on local expertise. Disadvantages are that delegation makes for difficult choices, it is harder to follow up on reviews, and there is less scope for dissenting opinions.

The underlying principle of the ‘federation’ model is the creation of a central ERBI to which representatives of the various ERBI network members would be delegated. Advantages are cost-effectiveness because this system avoids duplication, a reduction in the number of inconsistent reviews, and a basis for building a group culture for reviews. Disadvantages are the difficulty of dealing with local and cultural differences, the different power relationships that may emerge in a federation, and the potential difficulty of reaching mutual agreement.

One of the paper’s important conclusions is that there is currently no efficient, satisfactory system at hand for reviewing data-intensive multi-site research. For the time being, the authors therefore recommend an ad hoc, bottom-up approach. This would ideally take place with the consent of the relevant funding bodies. As more trials are run with the various models and as they continue to be refined, more ‘systematic’ solutions can be implemented. Relevant metrics should be used to evaluate the quality and efficiency of ERBI networks. This observation confirms the committee in its belief that the Netherlands must endeavour to set up a network of local ERBIs that will together develop a predetermined set of standards.

### 4.4 Practical guidance for ethical assessment

There is no blueprint or ideal description of an Ethical Review Board for Informatics, nor is there any set of predetermined ethical standards to guide its work. We can also assume that the environment in which the ERBIs must operate will be subject to constant technical, scientific, ethical and legal changes. Many of the informatics issues of today differ from those of a year ago, and it is impossible to predict all the issues that will arise next year. That is why an ERBI must develop methods and predetermined standards for itself that (a) accommodate the relevant law and case law, (b) follow best practices in applied computer ethics, and (c) are consistent with the state-of-the-art conceptualisation of ERBIs. An ERBI must also ensure that it keys into new trends in IT and the discipline of informatics. Its members will have to stay abreast of such trends.

In Chapter 5, we outline a general framework that ERBIs can use to support and structure their work. We suggest using a triage model in this context, based in part on limited experience working with such models. We also sketch the contours of an ethical review mechanism that is not meant as an ethical checklist, but rather as a way that ERBI members can articulate relevant ethical considerations when discussing the
ethical acceptability of research proposals. Finally, we also raise various points of concern and offer a number of checklists that address significant aspects of IT research. Together, these materials offer guidance to informatics researchers and ERBI members.

4.5 Conclusions and recommendations

CONCLUSION 4.1
One way that the informatics research community can live up to its ethical and public responsibility and demonstrate its awareness that informatics plays an important role in shaping society is to install an Ethical Review Board for Informatics, monitor the performance of this board, and reflect on the lessons learned in this manner.

RECOMMENDATION 4.1
The committee advises all governing bodies of institutes or departments active in informatics research to install an Ethical Review Board for Informatics (ERBI), either on their own or in cooperation with sister institutions. The primary task of the ERBIs is to assess the ethical aspects of informatics research. They can also function as the core of a community in which knowledge concerning this subject continues to advance.

RECOMMENDATION 4.2
Ethical assessment of informatics research is still in its infancy. No blueprint or ideal description of an Ethical Review Board for Informatics can be provided, nor does any set of predetermined standards exist. In addition, informatics is an exceptionally dynamic field, making it impossible to predict which issues will arise next year. ERBIs are advised to develop their own methods and set of standards, and to do so in close consultation with other ERBIs.
5. A REVIEW PROCEDURE IN OUTLINE

5.1 Introduction

Enormous advances have been made in the field of ‘computer ethics’ or the ‘ethics of IT’. Progress will continue in the period ahead thanks to the rise of numerous and influential emergent technologies, including – but by no means limited to – cybersecurity, drones, big data, artificial intelligence, robots, sensors and quantum computing. High ethical standards will be set not only for these specific fields, but for informatics research in general. We are already seeing signs of this in the requirements that have been imposed by research organisations and their review procedures. The approval of an ethics review board or procedure is often required for publications, funding or project acquisition.

5.2 Ethical values

Ethical considerations can refer to interests, needs, preferences, rights, duties, responsibilities and character traits. They can draw attention to the consequences for people’s health, happiness or monetary gain, and they can emphasise private intentions. When considering the legal aspects of a matter, we apply the principles laid down in laws. Equally, when we consider the ethical aspects, we have recourse to principles enshrined in ethical and moral values. Ethical values are generally accepted categories used to describe ethical considerations, for example ‘respect’, ‘privacy’, ‘happiness’, ‘dignity’, ‘safety’, and ‘sustainability’. Whenever people consider the ethics of a matter, they use ethical value types to articulate ethical considerations. There are many different and divergent values that cannot be reduced to a single type, however. This is
known as ‘value pluralism’, which we will explain in the following section. Taken as a whole, ethical values reflect the moral complexity that typifies our lives and our societies. Our ethical systems and ethical reflection on those systems are correspondingly complex and diverse in nature.

**Consequences of having a complex value domain**

The complexity and diversity of the value domain has consequences for the ethical assessment of informatics research. That is something that we would do well to take into account. The philosopher Isaiah Berlin puts it this way: the universe of ethical values has a highly complicated structure. Values cannot be ordered along a linear scale whereby one of two values is more important, more valuable, than the other. They are not commensurate. Values may also conflict with one another, or a set of values can be inconsistent. This insight is known as value pluralism, and it has significant consequences for the work of ERBIs. The first consequence is that some situations will require ERBIs to choose between different values that they wish to enforce or promote. Another consequence is that there are no a priori, unchanging rules for ethical assessment. Situations cannot be fit into neat classifications or positioned tidily in the value domain. This also means that an ERBI cannot create an unalterable review mechanism. That is why the committee cannot offer ERBIs a ‘manual’ for reviewing research. What we have attempted to do is provide guidance, and a differentiated review procedure. That procedure will need to develop gradually, informed by cumulative insight and a growing body of ‘ethical case law’.

The foregoing observation begs the question of why it has been possible in medicine, with its Medical Ethics Review Boards, to develop a robust ethical review mechanism. Our impression is that the situation in medical research may differ from that in informatics research in the breadth of the problem, which favours pluralism over systematization. More specifically, the law has given METCs a very narrow review mechanism that focuses specifically on risks posed to human test subjects. The focus of the mechanism is therefore so restricted that it is considerably simpler to define the criteria and conduct reviews.

**Ethical values in informatics research**

Table 5.1 provides an incomplete list of ethical values applicable in informatics research. Despite our assertion above that it is not possible to come up with a uniform classification or structure for the value domain, the committee has attempted to structure matters to a certain degree by dividing the values that are most commonly involved in informatics research into three columns (Table 5.1). The left-hand column contains those values that are primarily ascribed as predicates to a single individual
(John is safe, John is healthy, happy, etc.). The middle column contains values that primarily describe a relationship between two individuals. The right-hand column contains values that mainly refer to a moral quality of the surrounding social system.

**Table 5.1 Ethical values common in informatics research**

<table>
<thead>
<tr>
<th>Primarily applicable to a single individual</th>
<th>Primarily applicable to the relationship between two individuals</th>
<th>Primarily applicable to a social system</th>
</tr>
</thead>
<tbody>
<tr>
<td>health</td>
<td>responsibility</td>
<td>respect</td>
</tr>
<tr>
<td>wellbeing</td>
<td>accountability</td>
<td>dignity</td>
</tr>
<tr>
<td>physical integrity</td>
<td>justice</td>
<td>non-discrimination</td>
</tr>
<tr>
<td>happiness</td>
<td>equity</td>
<td>transparency</td>
</tr>
<tr>
<td>privacy</td>
<td>solidarity</td>
<td>trust</td>
</tr>
<tr>
<td>security</td>
<td>autonomy</td>
<td>democracy</td>
</tr>
<tr>
<td>safety</td>
<td>confidentiality</td>
<td>freedom</td>
</tr>
<tr>
<td>knowledge</td>
<td>access</td>
<td>utility</td>
</tr>
</tbody>
</table>

**The interests of others: stakeholders (direct and indirect) and affected persons**

Ethics primarily involves allowing for the interests, rights and needs of others and the restrictions that they impose on promoting self-interest. Sound conceptualisation ensures that ‘others’ are represented in the ethical assessment, even if they are not actually present or cannot speak for themselves, for whatever reason. Their safety, wellbeing, happiness, freedom and privacy can still influence decision-making in this manner. They may be technology users of a few years hence, or people who will feel the impact of that use in one way or another some years after the relevant technology is introduced. The field of ethics has been active in the ethical assessment of technology for some time now, for example in Social Cost-Benefit Analyses (SCBAs), Technology Assessment (TA), Privacy Impact Assessments (PIA), Data Protection Assessment, Ethical and Legal and Social Aspects (ELSA) and more recently in the EU’s Responsible Research and Innovation (RRI). All these approaches devote considerable attention to identifying and conceptualising ethically relevant persons and groups in connection with the ethical assessment of technology.

**5.3 An international tour**

To acquire input for drafting a review procedure – one that can serve as a starting point for the ERBIIs advocated in Chapter 4 – the committee has collected and analysed the
ethical protocols and guidelines of Dutch and foreign organisations (see Appendix 3). A number of general observations can be made in this regard:

- **Limitations in scope:** Most of the available protocols and guidelines concern only the ethical aspects of identifiable research subjects. That is, for example, the case for the human test subjects of medical or biometric experiments, serious games and videotaped sessions, surveys, etc. They rarely address the effects of the relevant research on society or the environment in terms of their ethical dimensions. The literature that we have identified also rarely considers national security or ‘dual uses’ issues.

- **Common core:** Virtually all the research protocols and ethical guidelines are reasonably likeminded about the importance of such subjects as informed consent, invasive interventions, and the participation of minors and vulnerable groups. Almost all of the protocols address these matters.

- **Principle of proportionality:** Many of the protocols and guidelines are based on the principle of proportionality: obligations related to accountability, documentation, reporting and monitoring depend on the risk and scope of the relevant research and the type of experiment being conducted. For example, detailed Research Data Management Plans and Privacy Impact Assessments (PIAs) are only required for studies that have will a considerable impact on large groups of participants.

- **Responsibility for students:** Many protocols emphasise that if students carry out the research, a member of the academic staff must bear the responsibility for ethical approval.

Our international tour clearly confirms that there is no ready-made, generic review mechanism waiting to be created. Although the common core identified in international protocols and guidelines gives us something to go by, we have also noted that that core is exceedingly limited in scope, leaving numerous problematic issues unaddressed. That makes it all the more necessary for the ERBIs to work together on developing a review mechanism.

### 5.4 The ERBI at work: proposed method

Researchers are expected to think closely about ethical values in relation to their research and the risks that it could pose, directly or indirectly, to all direct and indirect stakeholders and affected persons. The ethical values listed in Table 5.1 can serve as a starting point in this regard. An ERBI will be asked to form an opinion about the way in which the proposed research will make a positive or negative difference, both now and in the future, to all those potentially involved or affected by it, not only in terms of the study’s aim, intended or unintended and anticipated or unanticipated results and effects, but also the procedures and methods used. In other words, questions must be
raised concerning the privacy and safety of individuals whose data will be used, but also about the study’s impact on social exclusion or discrimination in the longer term. In this section, we propose a procedure that will allow ERBIs to work efficiently (see also Figure 5.1 on the next page). It is based on the triage principle, i.e. quickly placing proposals into different categories based on the complexity of the relevant ethical assessment.

Role of the researcher

In some cases, researchers can simply use their common sense while preparing their research proposal to avoid an unnecessary step in the review process. For example, many purely theoretical studies are clearly ethically neutral and do not require review. If a researcher believes that his or her study may not be ethically neutral, it must be submitted to an ERBI. Familiarity with cases such as those described in Section 2.2 or a more general ethical/legal awareness of the potential risks, dilemmas and dangers involved will help a researcher make this decision. Such decisions will also be easier if the relevant research field makes an active effort to raise general awareness of this subject. The following chapter presents our recommendations in this regard.

Some research proposals must be assessed by a review board in a different field. Examples include certain types of medical research that must be submitted to an METC (see Chapter 2.3). Researchers who are uncertain about this can consult the ERBI. Ideally, the researcher and ERBI will work together in such instances, although we wish to note that, at the moment, there is no clear division of responsibility between the individual researcher and the ERBI during this first step of the procedure.

Start of the procedure: intake assessment

For each proposal submitted to an ERBI, the secretary should check whether the relevant researcher has followed proper procedure by submitting the proposal to an ERBI rather than another authority. Once that has been verified, the following step can begin.

Review: is a lenient procedure sufficient?

In this step, the ERBI determines whether the proposal qualifies for the lenient procedure, i.e. whether the research can be seen as more or less ‘standard’ in nature. The ERBI can use checklists for this purpose (an example is given in Appendix 4). The checklists can help it examine two criteria that are (largely) unrelated:
Figure 5.1 Proposed review procedures

Research proposal

- Researcher decides
  - Not ethically problematical
    - No review
    - green light
  - May be ethically problematical
    - ERBI decides
      - Reviewed elsewhere in another field

Lenient procedure: standard research, small subcommittee, at most 2 weeks

- (i) Minimum risk
  - Green light
- (ii) Customary research practice
  - Green light

Stringent procedure: non-standard research, full ERBI, at most 4 weeks

- Green light
  - Passes after amendment
- Red light
  - Fails after amendment

Report and storage

Iteration of amendments

Appendix 4 checklist

- (i) Minimum risk
- (ii) Customary research practice

Appendix 5 checklist
1. **Minimal risk appraisal:** in a minimal risk appraisal, the checklist serves to determine whether the research involves more than only a minimal risk. Minimal risk is defined as the level of risk customary in everyday life.

2. **Customary research practice appraisal:** this means determining whether the proposed study meets standard research criteria. These criteria frequently differ from one discipline or subdiscipline to the next; one of the first tasks of an ERBI will be to compile lists of criteria for each discipline/subdiscipline. The lists will evolve gradually and should be shared among the various ERBIs.

Research that passes one of both appraisals may undergo the lenient review procedure, for example with the review being conducted only by the secretary and chairperson of the ERBI (or, if multiple departments are involved, by a relevant member of the ERBI). In those research units that are already working with this scenario, this procedure usually does not take more than two weeks. Examples of similar procedures are given in Insert 5.1.

### INSERT 5.1 EXAMPLE PROCEDURES

One of the faculties that distinguishes between a lenient and a stringent procedure is the Faculty of Electrical Engineering, Mathematics and Computer Science at the University of Twente, which introduced the concept of ‘standard research’ in its ‘Protocol for assessing the ethical permissibility of proposed research’. Many studies carried out in faculties are not entirely new. Viewed from a methodological and ethical perspective, some research is in fact merely a minor adaptation of earlier research. That is why a distinction is made here between standard and non-standard research. Standard research is research that was conducted on a more or less regular basis in the past. The lenient procedure applies to such research. Research that can be regarded as standard has been defined for every research group. Similar procedures are also used by the School of Computer Science and Statistics at Dublin University and by Delft University of Technology. At Delft, all proposals are submitted directly to the chairperson, who sorts them provisionally into cases that require discussion and cases that the chairperson believes do not involve any ethical problems meriting discussion. A list is kept of all proposals that are submitted, which is passed on to all members of the review board. The board members are free to query the chairperson’s decision and ask that this decision be reconsidered.

**Stringent procedure**

If the proposed research does not satisfy one of the two criteria described above, then a more thorough appraisal and/or more information is required. The full ERBI should review this type of research, and in some cases the proposal can be amended in consultation with the relevant researchers. The procedure is not expected to take more than a month.
As further guidance, the committee has distilled a number of questions from the international checklists and our own analysis that can help the ERBI in its subsequent review. These are grouped into four topics and concern:

a. the aim of the research
b. the results and benefits
c. the research method and approach
d. affected persons and stakeholders

(a) Aim of the research

- Can a plausible argument be made that the research is inconsistent with existing or future legislation or ethical values and ideals, human rights and standards of public conscience, and human dignity?
- Does the aim of the research concern outcomes that could lead to a deterioration of ethical values such as health, wellbeing, autonomy, safety, a sense of security, privacy, confidentiality, responsibility, transparency, accountability, liability, fairness, equality, social justice, and human dignity?
- Does the aim of the research focus in any positive sense on human health, wellbeing and happiness?
- How can the research (provided it is not purely theoretical in nature) benefit society; what contribution can we expect it to make to solving society’s problems or tackling major societal challenges?

(b) Results and benefits

- **Risk of dual use:** Could the results, artefacts or systems ensuing from this research be used, direct or indirectly, to manufacture arms?
- **Risk of misuse:** Could the result of the research
  - potentially be used for criminal, terrorist or other illegal purposes?
  - be harmful in any way to users, or be used to discriminate against or oppress people?
  - be used to make it more difficult or impossible for certain relevant parties to take responsibility for their actions, or to make the chance of users committing legal or ethical violations more likely?
  - have a negative influence on the environment, security, or health?

(c) Research method and approach

In the checklists and protocols that the committee analysed, the vast majority of questions concern the research method and approach. Appendix 5 provides an example of a detailed checklist addressing this aspect.
(d) Affected persons and stakeholders

- Have the interests of all relevant stakeholders and affected parties been considered?
- Are there any groups or parties in society who would be fiercely opposed to this research, and if so, why?
- Who might be affected by the research and its results?
- Could the research have effects that only become visible in the longer term?
- Are there any especially vulnerable groups that could be disadvantaged by the research?
- How would society change if the research and its results were to have a huge impact and gain general acceptance?

5.5 Reporting and storage

After rounding off the procedure, the ERBI must document and communicate its opinion. The ERBI may not always be able to reach consensus. In such cases, the dissenting opinions should be documented, as it may be necessary at a later time to understand why the rest of the board did not find them sufficiently persuasive. The opinion set out in the report must be based on a satisfactory assessment of the various interests and values involved, although that assessment need not have led to a single set of conclusions.

The report will naturally be sent to the researcher or researchers involved, but also to the management of the relevant research organisation. The researcher will be expected to comply with the ERBI’s final recommendation, which may be issued after he/she has been heard by the board, received its rejoinder, and, if necessary, amended the proposal. This is mainly of relevance when the ERBI advises against proceeding with the research. However, it is up to the management of the research organisation, and not the ERBI, to see that the research is not carried out in the manner described in the original research proposal.

As indicated earlier in this report, the review mechanism must evolve gradually. It is therefore extremely important for ERBIs to store their reports in a way that makes them accessible to researchers but also to other ERBIs. In the longer term, ERBIs should work on building a repository that permits perusal of all their decisions. Providing access to ‘ethical case law’ in this way makes it possible to check for consistency and convergence between opinions.

It is possible in highly exceptional cases that the ERBI will urgently recommend proceeding with the research because it involves major third-party interests. Two recent examples should serve to explain our reasoning. One example, which will have dramatic consequences in the short term, concerns research on the ZIKA virus. Detection,
computer vision techniques and other advances may very well be categorised as informatics and IT research, both now and in the future. Another recent example, this time with dramatic consequences in the long term, is the recent call by the United Nations for intensive, large-scale research on sea-level rise. This would, once again, involve imaging techniques as well as data analytics. The study of phenomena that pose a threat to humanity transcends the individual interests of a researcher or even a research unit.

In issuing a positive recommendation of this kind, which goes well beyond noting the absence of any ethical or legal objections to the research, the ERBI would address itself more to the research organisation’s management than to the applicant researcher. The latter is, after all, free to decide not to carry out the research.

We will conclude our discourse about addressing research whose urgency far outweighs the interests of researchers and the relevant authorities by touching on a more general question, i.e. to what extent should an ERBI play a pro-active role with regard to certain types of research. This would be alongside the ERBI’s primarily reactive role that was the focus of the previous chapters. An ERBI may find itself in an ideal position to recommend carrying out productive or promising research. Further study – to some extent stemming from the wished-for evolution of the ERBI’s methods – will have to show whether a pro-active role of this kind is compatible with researchers’ duty of care, as discussed in Chapter 3.

5.6 Conclusions and recommendations

CONCLUSION 5.1
Ethicists use ethical value types to articulate the arguments advanced in the process of ethical assessment. Examples of these value types are ‘respect’, ‘privacy’ and ‘wellbeing’. There are many different and divergent values that cannot be reduced to a single type, however. Values do not, furthermore, fit into neat classifications, and they may even conflict with one another. This is equally true of the values common in informatics research. This ‘value pluralism’ means that it is impossible to provide an unambiguous, unchanging review mechanism. Assessments will have to be made on a case-by-case basis.

CONCLUSION 5.2
The protocols and guidelines for ethical assessment currently used by many Dutch and foreign organisations are relatively limited in scope. The questions they pose generally concern the ethical aspects of identifiable research subjects. They rarely address the effects of research on society or the environment in terms of their ethical dimensions.
RECOMMENDATION 5.1
ERBIs are advised to develop an efficient and transparent procedure that distinguishes between a lenient and a more stringent assessment. The lenient procedure is meant for proposals that concern more standard research. The present advisory report outlines a possible review procedure of this kind.

RECOMMENDATION 5.2
ERBIs are advised to document their opinions properly and to make them available to researchers and other ERBIs. In the longer term, the committee recommends building a well-organised, shared repository where all decisions are available for perusal. Having a central repository of ‘ethical case law’ makes it possible to check for consistency and convergence between opinions and will help to construct a more uniform review mechanism.
6. WHAT ELSE IS NECESSARY?

6.1 Introduction

In the foregoing, we discussed the establishment of review boards and the setting up of a review mechanism to facilitate informatics research that is both ethically and legally responsible. But there is more needed than review mechanisms and review boards. There are several reasons for this. First of all, many things can alter once a research project gets under way, leading to changes in the very substance of the proposal, for example. Cumulative insight may lead to the course of the project being shifted, or to a different choice of methods and techniques. The project circumstances can also change owing to trends in society and/or advances in technology. Something that was considered possible or desirable today may be regarded as impossible or undesirable tomorrow – and vice-versa. New ethical issues are constantly arising in the field of informatics research. In such circumstances, a review board may come to see its initial opinion of a research project in a different light later on.

The second reason to take matters beyond a review mechanism and a board that conducts a one-off review of a research proposal is more psycho-social in nature. Introducing an single assessment point during the research start-up process focuses all minds on passing that one assessment. An isolated review thus elicits the desired behaviour at that moment, but will not guarantee ‘sustainable’ ethical behaviour. The risk is that the review will become an end in and of itself. The aim of this advisory report, however, is to get researchers to consider ethical and legal aspects in every phase of research.

We can add a third reason to this list: the importance of acting scrupulously. Scrupulousness is important not only to protect the image of science but also because this
aspect can be taken into account if the research unexpectedly leads to a claim and the
matter ends up in court. As we indicated in Chapter 3, researchers also have a duty of care.

In this chapter we offer some tips for promoting lasting ethically and legally responsi-
ble conduct in informatics research within organisations. After sharing several insights
borrowed from efforts to ensure academic integrity, we look at how the necessary
awareness of ethical and legal aspects can be created. We then suggest ways of embed-
ding a culture of awareness in organisations. The chapter concludes with a number of
additional suggestions.

Note that the committee by no means wishes to suggest that an institute must now
devote all its attention and energy to managing the ethical and legal aspects of
research. It is also not suggesting putting vast numbers of new procedures and rules
into place. What we must constantly bear in mind is that it is not the means but the
end that is important: to protect those freedoms and values recognised by society that
also play a role within the context of informatics research. An awareness that such
research could undermine those freedoms and values is not inevitable. That is why we
must take action, based on our responsibility to society and the value that we place in
science. Claims, problems and disasters must be avoided whenever possible. A certain
investment is thus justified.

6.2 Insights

In our efforts to deal consciously with the ethical and legal aspects of research, we can
learn a great deal from recent efforts concerning academic integrity. The academic
and research communities have done well to invest heavily in this in recent years, and
have further discovered that more is needed than agreeing on a code and setting up a
complaints committee. Lasting awareness requires combination of different measures.
We share a few insights below:7

- Personal ethics cannot be imposed. Individuals make their own moral decisions.
- Nevertheless, ethical positions and discussion can help shape an individual’s ethi-
cal character.
- Explanation, discussion and training in ethics makes internalisation and actualis-
ation possible.
- Role models and a culture of integrity supported by a well-defined, facilitatory
policy are crucial to internalisation and actualisation.
- Academic integrity issues require continuous awareness in every phase of
research.

---

7 These insights are borrowed from a theme issue on integrity in *Tijdschrift voor Hoger
• To ensure the effectiveness and legitimacy of a code of conduct, it is important for parties to work together to draft it, to draw attention to it regularly, and to enforce it without hesitation.
• The prevailing atmosphere must be one in which everyone can say what must be said.

6.3 Awareness

The context of informatics research is changing rapidly. In addition, informatics research increasingly encroaches on other domains, both in science and in society. All this raises various ethical and legal questions, such as those identified in Chapter 2. Questions of a legal and – in particular – ethical nature are generally difficult to answer. Indeed, that is one of their distinguishing features. In many cases, more than one answer is plausible. Ethical assessments often have a personal side to them. And even when an issue seems to have been resolved, new ones often arise.

Asking the right questions is just as important as giving the right answers (if we can even assume that they will be adopted unequivocally and by common consent). If we fail to ask the right questions, claims, problems and disasters lie ahead. That is why awareness and judgement are important. What is vital in this context is the ongoing discourse with others, querying one another. What is the level of ethical awareness at your own institute or institution? Has anything ever happened that, in retrospect, would be difficult or impossible to account for from an ethical or legal perspective? If so, what did your organisation learn from this experience? Did it lead to any decisions being made? Is there an institute-wide frame of reference for values and standards (whether or not documented or partially documented in writing)? What items are on the agenda for bilateral and plenary meetings? What matters can be discussed frankly and openly (and which not)? What is seen as a threat? Which mores are passed on to students and to new researchers and other staff at the institute? How do people at your organisation regard the review board (or the possibility of establishing one)? Do they know what matters are discussed by review board (and where differences of opinion arise)?

Once both the management and researchers are acutely aware of the ethical and legal aspects of informatics research, and once a culture of accountability and enquiry has evolved, then informatics research is less likely to lead to claims, problems and damage.

6.4 Embedding awareness

Awareness is essential, but raising awareness is not something that happens automatically. It is advisable to embed a culture of awareness in the organisation, so that it becomes inherent to the way it thinks and works. We can offer various tips in that regard, for example:
• Talk about the ethical and legal aspects of research during regular and bilateral meetings. Such interaction shows that few things go without saying when it comes to ethical and legal aspects.

• Make agreements (for example about adopting a code of conduct or protocol).

• Appoint a part-time ethical adviser to provide solicited and unsolicited advice and have this person report regularly on new trends and issues.

• Make ethics a compulsory part of the PhD programme and new staff members’ induction period. Make clear to PhD candidates and to other researchers that their research can also have an indirect impact on ethical values.

These tips emphasise that thinking about and clarifying ethical and legal aspects are communal efforts and reinforce awareness of those aspects. Everyone knows that it takes time to foster a particular culture, and that the full attention of management is an important prerequisite for success. A mere set of agreements and initial training will not lead to a lasting change in culture.

In addition to the foregoing tips and beyond reviewing a project proposal for new research, we recommend making at least the following agreements – for example, as part of a code of conduct – in order to raise awareness in every phase of research:

• Require every relevant research plan to include a section on ethics and an appraisal of the legal aspects (in the shape of a risk analysis).

• Organise a mid-term check on the ethics section of the research plan, in addition to reviewing the research proposal at the start.

• Require researchers to report on any ethical and legal issues that they have encountered and that remain at the conclusion of their research.

It is important for the institute’s management to monitor compliance with such agreements, for example by drawing attention to them during bilateral meetings and by placing them on the agenda for plenary meetings. That is not something that should be left to a review board.

By embedding a culture of awareness in the manner outlined above, organisations can prevent the ethical and legal aspects of research from turning into a mere procedural matter. After all, some research does not follow the research plan – review – funding award route. Researchers must take their ethical responsibility seriously by maintaining constant vigilance and by ascertaining for themselves whether the timely advice of fellow researchers, an ethics adviser, or a review board is needed.
Embedding awareness outside one's own institute

Looking beyond our tips for embedding a culture of awareness in one’s own institute, we can also suggest joining initiatives beyond the institute's four walls. One example would be to organise peer-review sessions with other review boards. This approach can help promote learning as well as the quality of research. ‘Disputation’ in which researchers ask one another the right – i.e. awkward – questions, both within and outside their group, can be seen as a form of ‘harmony’ whose purpose is to improve the quality and outcomes of the research itself.

6.6 Conclusion

CONCLUSION 6.1
Informatics research, and the context in which it is conducted, are in a continuous state of transition. As a result, new ethical and legal issues are constantly arising in relation to research projects. It is not enough to have a review board conduct a one-off review of these issues at the start of a project. Research institutes and individual researchers must work constantly on raising ethical awareness and conducting ethical reviews and make these an inherent part of the organisation.
BIBLIOGRAPHY


CBP (2013). *CBP Richtsnoeren beveiliging van persoonsgegevens*.


Dijck, José van (2014). *Big data, grand challenges. Over de digitalisering van het geesteswetenschappelijk onderzoek*. Clariah pubilcation.


Executive Office of the President President’s Council of Advisors on Science and Technology (2014). *Report To The President: Big Data And Privacy: A Technological Perspective*.


Lohr, Steve (2015a). *Data-ism: The revolution transforming decision-making, consumer behavior, and almost everything else.*


The glossary entries, which we have curtailed in number, are meant to give readers a quick first impression or jog their memories. We have limited ourselves to terms and phrases that actually appear in this report. For the more exhaustive *Internet Security Glossary*, see https://tools.ietf.org/html/rfc2828. Another option is the *Glossary of ICT terminology* at http://www.ict4lt.org/en/en_glossary.htm. Yet another useful glossary can be found at http://whatis.techtarget.com/.

**attack software**
Largely self-explanatory term that refers to software meant to exploit vulnerabilities in a system in order to gain unauthorised access to it. A synonym of malware, malicious software.

**autonomous systems**
i. *in internet technology*: independent subnetworks of the internet that have their own routing protocols and addressing. They are islands in the internet sea.
ii. *in robotics*: systems like robots that can operate autonomously in unstructured environments, such as self-driving cars.

**computer security, cybersecurity**
Another largely self-explanatory term that now refers to a major discipline. The relevant Wikipedia entry provides an exhaustive and informative summary of the various facets of computer security, security risks, prominent authors and researchers in this area, and references and further reading.

**corporate governance**
Concerns the aspects and structure of management and governance in enterprises, related processes and relationships, and the responsibilities of managers and governing bodies.
**cryptography**
The art and science of encryption. Scientific efforts in this area – which have major implications for privacy – draw on deep mathematical insights (number theory, prime numbers, prime factorisation) and the emerging technology of quantum computing.

**data analytics**
The study of ‘raw’ data meant to support or improve decision-making in commerce and industry and to test existing models or theories in science. It is related to data-mining, but where the primary purpose of data-mining is to expose hidden patterns and connections, data analytics draws inferences and conclusions from existing knowledge.

**data fusion**
One of the biggest threats to privacy in the digital society. Data fusion is the process of integrating multiple databases with personal data, each database being ‘suitably confidential’ in the sense that the persons behind the data cannot be reconstructed (identified) by the database output. Integrating seemingly confidential databases may unexpectedly result in their no longer being confidential. A famous example is described in [Lane et al., 2014]. In this case, researchers linked online video streaming company Netflix’s anonymised customer viewing data to viewer movie reviews posted on IMDb (the Internet Movie Database). After linking, 96% of the Netflix users could be uniquely identified.

Example 2: linking an anonymised database containing sensitive patient data to a database of non-sensitive data.

**data mining**
Research in large data corpora meant to:

- uncover patterns in how events are related or lead to other events (association and sequencing);
- classify and cluster facts;
- predict future events based on patterns found in the data (predictive analytics).

Like data analytics, data mining is used in science (mathematics, genetics) and the commercial sector (market research) [Tanner, 2014].

**data science**
A new, interdisciplinary field emerging at the intersection of data mining, data analytics and other areas and derived from mathematics (especially statistics), informatics, pattern recognition, artificial intelligence, High Performance Computing, and visualisation techniques. One of the significant drivers behind the emergence of data science...
is machine learning; see elsewhere in this Glossary. There are countless applications in biology, economics, commerce and the financial world.

**data security**
Related to computer security but focuses more specifically on defending data against attack or corruption due to other causes. The data defence methods may be software- or hardware-based.

**dual use**
In general, the ‘dual use’ dilemma concerns technology that can be used for different purposes. Usually this refers to peaceful versus military purposes.

**embedded computing, embedded system**
An electronic component of a larger system, often equipped with sensors, with its own microprocessor and with integrated hardware and software. There are countless examples in consumer electronics, automobiles, and hospital equipment. See also http://www.esi.nl/

**gaming, serious gaming**
A line of research important for educational purposes and for the development of virtual reality and many other applications, for example pilot training.

**human computer interaction (HCI)**
Designing technology to optimise interaction between user and computer, making use of applications borrowed from cognitive science and software and hardware engineering design.

**informed consent**
Obtaining consent after the implications and consequences associated with a study have been made clear and after receiving proof that the human test subject has a clear understanding of the same, before involving them in a medical or other type of experiment. Based on the ethical guidelines applicable in the relevant field or in medical or other research, such as IT.

**internet of things (IoT)**
The growing ‘internet network’ of items, vehicles, buildings and embedded systems made of hardware, software and sensors. One well-known (and still rather futuristic) example is the vigilant refrigerator that detects that it is running low on a certain food item and orders that item from the right shop, or a robot vacuum cleaner that can be ordered to vacuum the floor remotely, by smartphone.
**invasive interventions**
In medical terminology, surgical interventions, as opposed to non-invasive interventions that do not involve incisions, for example laparoscopy, medical imaging, radiotherapy, endoscopy or other techniques.

**life logging**
See reality mining.

While many see life logging and reality mining as promising, there is also a darker side, as argued by internet critic Evgeny Morozov in his recent book *To save everything click here* [Morozov, 2013]. Novelist Dave Eggers has also painted a dystopian picture of the darker side [Eggers, 2014].

**machine learning**
An area of informatics that has emerged from pattern recognition studies and artificial intelligence. It concerns the analysis and design of algorithms for processing data and extracting predictions. Typical areas of application include OCR, search engines, and computer-vision. The field was once defined as being specifically geared towards making computers capable of ‘learning’ without explicitly programming them to do so.

**NBIC**
Acronym for the cluster of emerging, converging technologies consisting of nanotechnology, biotechnology, information technology and cognitive science.

**New Deal on Data**
Slogan invented by Alex Pentland, a prominent theoretician and philosopher of the Big Data revolution. According to Pentland, Big Data is a big deal, comparable in importance to the economic and social welfare programme (1933 to 1938) coined the ‘New Deal’ by US President Franklin D. Roosevelt [Pentland, 2014a and 2014b].

**reality mining**
Involves collecting and analysing data on our social behaviour in order to detect useful patterns. Made possible by the rise of ubiquitous computing and countless devices. An associated term is life logging.

**responsible disclosure**
Term used in the field of computer security describing the preferred procedure that researchers should follow if they discover a vulnerability of a system. The procedure gives the vendor of the system enough time to remove the vulnerability before the researchers publish their findings. In the case of the Radboud University group that discovered a vulnerability in the MIFARE chip (see p. 21 of this report), the self-imposed embargo on publication was approximately six months. See also http://www2.ru.nl/media/pressrelease.pdf.
(The time that elapses between discovering and repairing a vulnerability is also related to the notion of a zero-day attack, whereby attack software is used to exploit the vulnerability on the very day that it is discovered.) Alongside ‘responsible disclosure’, the term ‘coordinated disclosure’ is also popular.

**reverse engineering**
A customary technique (many different versions exist) for analysing hardware and software systems without modifying the system itself in order to study its design and functionality. The reverse engineering of smartcards is destructive because the analysis involves taking the smartcard apart layer by layer.

**robotics**
A discipline at the interface between mechanical engineering, electrical engineering and computer science. See also ‘autonomous systems’.

**philosophy of technology**
The philosophy of technology studies the relationships between technology and ethics, in particular the implications of technology for human beings and society. It covers a broad spectrum of domains, from research and culture to politics. One of the more important insights today is that it is better for technological developments and ethical oversight to take place simultaneously, and not sequentially (co-shaping) [Verbeek, 2014].

**ubiquitous computing, pervasive computing, ambient intelligence**
All three terms are names for the growing omnipresence of computing devices which, unlike the traditional desktop computer, take the form of countless smaller ‘thinking objects’. Examples include intelligent refrigerators, fitness trackers, and RFID tags. Life logging and reality mining also form part of ubiquitous computing.

**vulnerabilities in computer security**
Computer system weakness that an attacker can exploit to gain unauthorised access.

**wearable computing**
Related to ubiquitous computing and life logging. A few examples suffice: Google Glass, Apple Watch and other smart watches, step counters and fitness trackers.

**zero-day exploit**
In general, ‘exploit’ refers to the exploitation of a computer system vulnerability. The attack is often in the form of code written especially to misuse a security flaw, for example in an internet service. ‘Zero day’ refers to the fact that the software vulnerability is unknown to the software’s authors, giving them zero days to protect the system against attack [Grossman, 2014].
### ACRONYMS AND ABBREVIATIONS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM</td>
<td>Association for Computing Machinery</td>
</tr>
<tr>
<td>CBP</td>
<td>College Bescherming Persoonsgegevens [Dutch Data Protection Authority]</td>
</tr>
<tr>
<td>CCMO</td>
<td>Centrale Commissie Mensgebonden Onderzoek [Central Committee on Research Involving Human Subjects]</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incidence Response Team</td>
</tr>
<tr>
<td>CWI</td>
<td>Commissie Wetenschappelijke Integriteit [Academic Integrity Committees]</td>
</tr>
<tr>
<td>CW&amp;I</td>
<td>Centrum voor Wiskunde en Informatica [Centre for Mathematics and Computer Science]</td>
</tr>
<tr>
<td>ELSA</td>
<td>Ethical and Legal and Social Aspects</td>
</tr>
<tr>
<td>ERB</td>
<td>Ethical Review Board</td>
</tr>
<tr>
<td>ERBI</td>
<td>Ethical Review Board for Informatics</td>
</tr>
<tr>
<td>HCI</td>
<td>Human Computer Interaction</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>KNAW</td>
<td>Koninklijke Nederlandse Akademie van Wetenschappen [Royal Netherlands Academy of Arts and Sciences]</td>
</tr>
<tr>
<td>METC</td>
<td>Medisch Ethische Toetsings Commissie [Medical Ethics Review Boards]</td>
</tr>
<tr>
<td>MKBA</td>
<td>Maatschappelijke Kosten Baten Analyse [Social Cost-Benefit Analysis]</td>
</tr>
<tr>
<td>NBIC</td>
<td>Nanotechnology, Biotechnology, Information Technology, Cognitive Science</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>RRI</td>
<td>Responsible Research and Innovation</td>
</tr>
<tr>
<td>SURF</td>
<td>Higher education and research partnership for ICT in the Netherlands</td>
</tr>
<tr>
<td>TA</td>
<td>Technology Assessment</td>
</tr>
<tr>
<td>TWINS</td>
<td>Raad voor de Technische Wetenschappen, Wiskunde, informatica, Natuur- en Sterrenkunde en Scheikunde van KNAW [Academy Council for Technical Sciences, Mathematical Sciences, Informatics, Physics, Astronomy and Chemistry]</td>
</tr>
<tr>
<td>VSNU</td>
<td>vereniging van universiteiten [Association of Universities in the Netherlands]</td>
</tr>
<tr>
<td>WMO</td>
<td>Wet Mensgebonden Onderzoek [Clinical Trials Act]</td>
</tr>
</tbody>
</table>
APPENDIX 1
INTERVIEWEES, REVIEWERS AND ACKNOWLEDGMENTS

- Prof. Emile Aarts, dean of the faculty of Mathematics and Information Science, Eindhoven University of Technology (at the time of the interview)
- Prof. Herbert Bos, professor of Systems and Network Security, VU University Amsterdam
- Prof. Jan Friso Groote, professor of Computer Science, Eindhoven University of Technology
- Evelijn Jeunink LL.M, legal advisor, SURFnet
- Prof. Johan Jeuring, professor of Information and Computing Sciences, Utrecht University
- Prof. Joost Kok, professor & academic director of Leiden Institute of Advanced Computer Science (LIACS), Leiden University
- Prof. Ronald Leenes, professor of Regulation by Technology, Tilburg University
- Prof. Jan van Leeuwen, professor of Information and Computing Sciences, Utrecht University
- Prof. John-Jules Meyer, professor of Information and Computing Sciences, Utrecht University
- Prof. Jos Roerdink, professor of (Medical) Computing Science, University of Groningen
- R. Rogier Spoor, MSc., Manager Middleware Services, SURFnet
- Prof. Gerrit van der Veer, head of the Human-Computer-Society programme, Open Universiteit of the Netherlands and emeritus professor at VU University Amsterdam
- Aimee van Wynsberghe, assistant professor of Philosophy of Technology at the Department of Philosophy, Ethics Advisor for the Centre for Telematics and Information Technology (CTIT), University of Twente
- Scientific Technical Council, SURF
Reviewers

The following persons reviewed the draft report:

- Prof. Natali Helberger, professor of Information Law, University of Amsterdam
- Prof. Catholijn Jonker, professor of Artificial Intelligence, Delft University of Technology
- Prof. Maarten de Rijke, professor of Information Processing and Internet, University of Amsterdam
- Prof. Peter Paul Verbeek, professor of Philosophy of Technology, University of Twente

Acknowledgments

The Academy owes the reviewers a debt of gratitude. We have adopted as many of their suggestions as possible. The reviewers bear no responsibility for the substance of the report.

Our gratitude also extends to the above-mentioned discussion partners. We would also like to thank those who attended the liaison meeting at the Trippenhuis Building on 15 June 2015, in particular our speaker, Frits Rosendaal, Professor of Clinical Epidemiology at LUMC Leiden, and our moderator Jaap van den Herik, Professor of Law and Informatics at LIACS Leiden.
APPENDIX 2
RESOLUTION INAUGURATING THE COMMITTEE

Having regard to Article 8 of the *Academy’s Regulations*, and considering that certain advances in technology and changes in society are making the ethical, legal and safety/security aspects of informatics research increasingly important, and that large-scale data collections – many of them privacy-sensitive – are being used in a growing number of scientific disciplines, the Board of the Royal Netherlands Academy of Arts and Sciences has decided, at the proposal of the TWINS Council and the Social Sciences Council, to install the advisory committee on the **Ethical, Legal and Safety/Security Aspects of Big Data and Informatics Research**, hereafter ‘the committee’.

**Section 1. Assignment**

The committee is charged with the task of outlining a mechanism for reviewing the ethical, legal, and security/safety aspects of informatics research and related studies. This covers:

- the assessment of research on the security of networks, computer systems and access to the same;
- the collection and use of the large, often privacy-sensitive data sets (‘big data’) that are on the rise in numerous disciplines.

The intended review mechanism must have the support of the research community. The committee will therefore involve relevant representatives of the field.

Given the breadth of the assignment, the committee will begin by exploring the outlines of a possible advisory report and, if necessary, limit the subject that it addresses. After the Academy Board has discussed the outlines, it will decide whether the committee is to continue as planned or whether its assignment should be amended.
Section 2. Composition of Committee and Appointment Period

The following persons are appointed to the Committee in a private capacity:

- Prof. Jan Willem Klop (chair), VU University Amsterdam
- Prof. Jan Bergstra, University of Amsterdam
- Prof. Frank van Harmelen, VU University Amsterdam
- Prof. Jeroen van den Hoven, Delft University of Technology
- Prof. Bart Jacobs, Radboud University Nijmegen
- Prof. Corien Prins, Tilburg University
- Melle de Vries, Royal Netherlands Academy of Arts and Sciences

The committee has been installed for the duration of the advisory process. The committee is asked to deliver its report before 1 July 2015.

The committee will be assisted by the Academy’s Bureau in accordance with the Director General’s instructions.

Section 3. Quality Assurance

Prior to their appointment, the members of the committee familiarised themselves with the *Code ter voorkoming van oneigenlijke beïnvloeding door belangenverstrengeling* [Code of conduct to prevent inappropriate influence owing to conflicts of interests] and filled in and returned the declaration contained therein before the committee’s first meeting.

The committee members have familiarised themselves with the Academy’s *Handleiding adviezen KNAW* [Manual concerning Academy Advisory Reports] as adopted by the Academy Board on 21 May 2013. The peer review policy is described in Appendix B to the Academy’s Manual concerning Academy Advisory Reports of 19 July 2013. There will be no deviation from that policy.

Section 4. Follow-up and Communication

The committee will follow up and provide for communication concerning its findings.

Section 5. Costs and Remuneration

The committee members will be reimbursed for their travel expenses in accordance with Article 18(2) of the Academy Regulations.
Section 6. Confidentiality

The members of the committee will observe confidentiality in respect of all information that becomes known to them in the context of the implementation of this resolution and that can be considered to be of a confidential nature.

Adopted in Amsterdam on 10 February 2014 by the Board of the Royal Netherlands Academy of Arts and Sciences.

On behalf of the Academy Board,

Dr K.H. Chang
Director General of the Royal Netherlands Academy of Arts and Sciences
APPENDIX 3
PROTOCOLS, CHECKLISTS AND GUIDANCE DOCUMENTS

- University of Bath, Department of Computer Science, 13-point checklist.
- University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Protocol for assessing the ethical permissibility of proposed research in the Faculty of Electrical Engineering, Mathematics and Computer Science.
- University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Checklist for submitting a research proposal to the Ethics Committee.
- University of Nottingham, School of Computer Science, Research Ethics Review Checklist.
- University of Dublin, Trinity College, Faculty of Engineering, Mathematics and Science, School of Computer Science and Statistics, Research Ethics Application.
- University of Duisburg Essen, Division of Computer Science and Applied Cognitive Sciences, Faculty of Engineering, Begutachtung von Forschungsvorhaben durch die Ethikkommission der Abteilung für Informatik und Angewandte Kognitionswissenschaft, Basisfragebogen.
- University of Limerick, Faculty of Science and Engineering, Research Ethics Committee, Guidelines for Research on Human Persons by Faculty or Students and the Operational Guidelines for University of Limerick Research Ethics Governance Committees.
- University of Edinburgh, Research ethics checklist.
- Economic and Social Research Council (ESRC), United Kingdom, Guidance for Applicants.
- Griffith University, Human Research Ethics Committee, Expedited Ethical Review Checklist.
- City University London, Ethics forms and guidance documents.
- Delft University of Technology, code of ethics, and project templates.
- University of Amsterdam, ethical code.
The following documents and checklists mainly address data management.

- Data Science Association, Data Science code of professional conduct
- Boston University Libraries, Research Data Management, Overview of data management plans, templates and checklists:
- University of Auckland, Research Data Planning Checklist
APPENDIX 4
QUESTIONS FOR THE INITIAL REVIEW

• Is the research subject to review under the Dutch Clinical Trials Act (WMO)? Then it must be submitted to an METC for review.
• Does the research involve the use of living material, living beings, plants, animals, people, embryos, or human or animal tissue? Then it may have to be submitted to the Animal Testing Board.
• Does the research involve the use of information or data concerning or potentially applicable to identifiable persons?
• If the answer to the previous question is no because the data is anonymised, is there a chance that the data can be de-anonymised, making persons identifiable?

In the case of human test subjects

1. Has the subject provided his or her informed consent? Do the test subjects include minors or vulnerable individuals?
2. Are the test subjects confronted with sensitive topics (sexual activity, drug use, addiction, etc.)?
3. Are the test subjects exposed to activities that they could experience as traumatic or embarrassing?
4. Is the research likely to meet with resistance from participants because of aspects related to ethnic background, religious beliefs, gender, sexual orientation or cultural background?
5. Are the test subjects given drugs, placebos or other substances, or are invasive or other potentially hazardous procedures employed?
6. Are blood or tissue samples taken from the test subjects?
7. Do the test subjects experience pain or more than minor discomfort?
8. Can the research cause the test subjects to experience mental distress, fear or anxiety, or otherwise lead to negative consequences?
9. Must all test subjects be tested regularly for a longer period of time?

---

8 From Delft University of Technology.
10. Do the test subjects receive any payment beyond reasonable compensation for their expenses and time?

11. If the participants are quoted, is their consent requested?

12. If photographs are used, is the consent of the participants requested?

**Data protection**

1. Does the research involve text or audio, film or video recordings that make it possible to trace individual persons? \(^9\)

2. Is the purpose for which personal data is being used made explicit and is there a lawful basis for that use (for example consent or a public interest)?

3. Are the stakeholders and affected persons informed that their personal data is being used?

4. Is personal data shared with non-EU countries?

---

\(^9\) For more general discussion on personal data see [CBP, 2013].
APPENDIX 5
QUESTIONS ABOUT RESEARCH METHOD AND APPROACH

The principle of proportionality should be adhered to when using this type of checklist.

General information

• Title of the project
• Lead researcher
• Other researchers
• Brief description of the project
• Place research will take place
• Name of organisations involved

General questions

• Have you submitted this or a similar project to the ERBI? (Yes/No)
• Are any external items being used in the research? (Yes/No)
  If yes, do the items belong to the participating research partners?

• Is the owner of the item aware of its use? (Yes/No)
  If not, why not?

• Have you obtained legal advice? (Yes/No)
  If yes, please attach the relevant document

• Have disclosures been agreed? (Yes/No)
  If yes, with whom and about what matters?

9 Source: Informatics Institute, University of Amsterdam.
• Is the research sensitive in terms of publicity? (Yes/No)
If yes, can you briefly describe what is sensitive about it?

**Domain-specific questions**

**Data storage**

- What are the participant/authors expectations of privacy?
- Is the data easily searchable and retrievable? Is the data subject to open data laws or regulations?
- Does the data privacy policy contradict ethical principles?
- What measures safeguard data at the site of data collection?
- How long will the data be stored on the servers?
- Does this contradict the time frame indicated by the researcher or institutional policies?
- What happens to the data after the researcher completes work on the service?
- How are the data destroyed?
- How will cross-border data be handled if IP addresses are considered by one country to fall under privacy regulations?

**Databanks**

- Where is the data stored?
- How long will the data exist in the repository?
- What consent is needed for subsequent data use?
- Does the remixing/mashing of data enable identification of individual or group identities or enable any additional risks to participants?
- In the case of shared data, what conditions were placed on data use by the original researcher, if any?
- Regardless of conditions, what ethical responsibilities may require consideration by later users?
- What mechanisms are in place to ensure appropriate data provenance and ownership? How will images/audio be effectively anonymised?

**Security**

- Are you searching for a vulnerability in a network or application?
- Does the owner of the information system know you are searching for vulnerability?
- Are the activities in conflict with regulations?
- Which law applies? Dutch, US . . .?
- What is the impact of the vulnerability?
• Does the vulnerability affect anyone’s privacy?
• How do you communicate with the owner of the vulnerability?
• How can researcher ensure that author/participant understands and agrees that content or interaction may be used for research purposes?
• Is the communication archived or easily searchable and retrievable?
• Is the data subject to open data laws or regulations?
• How long does the third party provider or ISP preserve the data and where?
• Could privacy be achieved through anonymization of email content and/or header information?

**Special interest forums**

• How do terms of service (TOS) articulate privacy of content and/or how it is shared with third parties?
• Regardless of TOS, what are community or individual norms and/or expectations for privacy?
• Does the author/subject consider a personal network of connections sensitive information?
• Is the data easily searchable and retrievable?
• If the content of a subject’s communication were to become known beyond the confines of the venue being studied would harm likely result?
• Is the conversation thread or forum perceived as public or private by the author(s)/subject(s)?
• How is profile, location, or other personally identifying information used or stored by researcher?
• How is informed consent or protection of privacy achieved?
• How are vulnerable persons identified and protected?
• If non-active archives are used, how is vulnerability or harm defined and how are potential or actual subjects protected?

**Social networking**

• How do the terms of service articulate privacy of content and/or how it is shared with third parties?
• Does the author/participant consider personal network of connections sensitive information?
• How is profile or location information used or stored by researcher? Does author/participant understand and agree to interaction that may be used for research purposes?
• Does research purpose and design balance possible conflicts between participant and researcher perceptions of public/private and sensitive/nonsensitive?
• Does the dissemination of findings protect confidentiality?
• Is the data easily searchable and retrievable?
• If the content of a subject’s communication was ever linked to the person, would harm likely result?

**Personal spaces**

• Could analysis, publication, redistribution, or dissemination of content harm the subject in any way?
• If the content of a subject’s communication were to become known beyond the confines of the venue being studied would harm likely result?
• Does the author/participant consider personal network of connections sensitive information?
• Does author/participant consider the presentation of information or venue to be private or public?
• Do the terms of service conflict with ethical principles?
• Is the author/subject a minor?

**Virtual worlds**

• Should these virtual worlds be considered ‘public’?
• What constitutes ‘privacy’ in such places?
• Should avatars be considered as persons and afforded the same protections as human subjects?
• Will the process of requesting consent itself cause harm?
• How and when should consent be sought?
• What requires consent?
• To what extent do users perceive their interactions and communication to be private in these spaces?
• How do Terms of Service specify researcher presence, anonymity of users, and privacy/confidentiality?
• To what extent and in what ways could research activities interfere with or compromise a user’s play or outcomes in the game?
• How should researchers juggle their own multiple roles?
• Could data be used to identify a user’s physical location and other sensitive demographic information?
INDEX

A
academic integrity 37, 39, 56
Academic Integrity Committees 40, 67
access 6, 15, 20, 21, 22, 23, 28, 31, 46, 52, 62, 66, 70
access gates 21
accountability 34, 46, 47, 51, 57
affected parties 52
affected persons 46, 47, 51, 76
algorithm(s) 19, 21, 37, 65
ambient intelligence 66
animal testing board(s) 38, 39, 75
anonymisation 30
app 22, 28, 30, 31
Apple Watch 66
archiving 34
artificial intelligence 6, 20, 36, 44, 63, 65
Association of Universities in the Netherlands 40, 67
attack 64, 66
zero-day 33, 66
attack software 34, 62, 66
autonomous systems 17, 36, 62, 66
autonomy 20, 24, 41, 46, 51
avatars 80
awareness 5, 9, 11, 17, 43, 48, 56-59

B
bank ID card(s) 28, 30, 31
bans 22
behavioural sciences 8, 14, 36
Berlin, Isaiah 45
big data 5, 6, 15, 16, 17, 44, 65, 70
biotechnology 65
botnet 20

C
case law 10, 14, 16, 41, 42, 45, 52, 54
CCMO 23, 25, 67
checklist 42, 49, 50, 51, 73, 77
child pornography 21
chips 21
code of conduct 10, 14, 41, 57, 58
cognitive science 64, 65
commensurate 45
computer
crime 27
ethics 36, 37, 42, 44, 61
security 17, 28, 32, 41, 62, 64, 65, 66
systems 7, 15, 19, 20, 27, 70
technology 36, 37
vision 53, 65
confidentiality 21, 33, 46, 51, 72, 79, 80
copyright 21, 22, 29, 30, 31
corporate governance 37, 62
co-shaping 66
criminal law 35
CRYPTO-1 algorithm 21
cryptography 17, 32, 63
Customary research practice 49, 50
cybersecurity 44, 62

analytics 53, 63
corpora 63
fusion 63
mining 63
science 17, 63
security 17, 29, 64
database(s) 23, 28, 30, 31, 34, 63
data protection 76
data storage 78
decompilation 30, 31
delegation 41, 42
democracy 46
digital payment transactions 20
dignity 44, 46, 51
dilemmas 4-10, 14-20, 25, 30, 32, 38, 48
disclosures 77
Disputation 59
drones 17, 44
dual use 51, 64
*Dutch Clinical Trials Act* 75
Dutch Ministry of Security and Justice 33
*Dutch Personal Data Protection Act* 30
duty of care 8, 27, 28, 35, 53, 56

**E**

Eggers, Dave 65
electrical engineering 66
embedded computing 17, 64
embedded system 64
embedding 15, 56, 58, 59
EM Microelectronic 22
engineering
electrical 66
mechanical 40, 66
engineering design 64
equity 46
ESORICS conference 21
ethical 2, 8, 9, 15, 36, 37, 38, 42-46, 57, 67, 70, 73
ethical case law 10, 41, 45, 52, 54
ethical infrastructure 7, 25, 38
ethical review boards 8, 36, Chapter 4
ethical value types 10, 44, 53
ethicist 24, 38
ethics advisor 10, 38, 58
ethics and integrity 10
*EU Directive 2009/24, on the legal protection of computer programs* 30
exploit 28, 62, 66

**F**

federation 42
fitness trackers 66
freedom 17, 22, 33, 46

**G**

gaming 17, 64
genetics 63
Google Glass 66
Grindr 22, 23
grounds for utilisation 30
guidelines 8, 10, 33, 34, 36, 47, 53, 64

**H**

hackers 34, 60
happiness 44, 46, 51
HCI 64, 67
health 44, 46, 51
Heartbleed 27
high performance computing 63
Horizon 2020 14
human computer interaction 17, 64
human-machine interaction 6
human rights 51
human test subjects 7, 23-26, 38, 45, 47, 75
human trials board 38

**I**

illegal downloading 21
IMDb 63
immobilisers 21, 33
indemnification statement 33
informatician 20, 28
informatics 1-20, 25-29, 35-40, 42-46, 53, 55-57, 63, 65, 70
information technology 16, 36, 65, 67, 68
informed consent 23, 25, 47, 64, 75, 79
injunction 22, 33, 34
innovation 28, 61
integrity 10, 14, 27, 37, 39, 56
intellectual property rights 7, 8, 21, 27, 29, 30, 34, 35
interfaces 31
internet 8, 17, 22, 27, 30, 35, 36, 62, 64, 65, 66
internet of things 17, 64
interoperability 31
interviews 18, 39
invasive interventions 47, 65
investigation 27, 28
IoT 64, 67
IP addresses 22, 78
IT system 28

J
justice 15, 46, 51

K
keycard 6, 21
knowledge 8, 9, 19, 20, 32, 37, 38, 39, 43, 46, 63
KPN 33

L
labour conflicts 37
laparoscopy 65
liability 8, 27, 35, 37, 40, 51
liaison meeting 18, 39
licence 2, 29, 30, 31, 34
life logging 65, 66

M
machine learning software 17, 19, 64, 65
malicious software 62
malware 62
market research 63
mathematics 20, 63
mechanical engineering 40, 66
medical ethics review boards 38, 39
medical imaging 65
Megamos CRYPTO-1 algorithm 21
memory dump 29
metadata 20
METC 23, 24, 25, 48, 67, 75
MIFARE Classic Chip 21, 33, 65
minimal risk 50
misuse 51, 66
Morozov, Evgeny 18, 65
multi-site research 41, 42

N
nanotechnology 65
NBIC 65, 67
Netflix 63
Netherlands Board on Research Integrity 41
New Deal on Data 65
non-discrimination 46
NSA 27, 28
NXP 21, 33

O
OCR 65
open access policy 34
open source 29

P
pacemaker 28
passive 8, 35
peer(-)review 9, 41, 59, 71
Pentland, Alex 65
personal data 7, 27, 29, 30, 32, 34, 38, 63, 76
pervasive computing 66
philosophy of technology 66
physical integrity 46
Pobelka botnet 20
preprints 33
Principle of proportionality 47
privacy 4, 6, 7, 8, 10, 15, 19, 23, 27, 28, 29, 32, 34, 35, 44, 46-48, 51, 53, 63, 67, 70, 78, 79, 80
privacy-sensitive 6, 15, 23, 28, 70
private law 35
problem owner 32, 33
programs 30, 31
proportionality 47, 77
proprietary licences 30
protocol(s) 7, 10, 18, 24, 25, 36, 37, 47, 50, 51, 53, 58, 62, 73
public transport smartcard 6, 21, 31

Q
quantum computing 44, 63

R
Radboud University 15, 21, 33, 65, 71
reality mining 65, 66
reciprocity 41
reliability 6, 17, 30
repository 5, 10, 52, 54, 78
research protocol 24, 25
resolution inaugurating 70
respect 5, 10, 44, 46, 53, 72
responsibility 5, 9, 10, 19, 27, 35, 40, 43, 46, 47, 48, 51, 56, 58, 69
responsible disclosure 21, 22, 23, 32, 33, 34, 65, 66
reverse engineering 30, 31, 66
RFID tags 66
robotics 17, 40, 62, 66
robots 44, 62
Roosevelt, Franklin D. 65

S
safety 15, 16, 37, 44, 46, 48, 51, 70
scrutiny 7, 15, 26
sea-level rise 53
search engines 65
security 4, 6, 15, 16, 17, 20, 21, 27-29, 31, 32, 33, 41, 46, 47, 51, 62, 64-68, 70, 78
security vulnerabilities 28, 32
sensors 44, 64
serious gaming 64
smartcards 28, 66
smartphone(s) 22, 23, 28, 30, 64
smartphone application 23
social media 8, 18, 36, 60
software 6, 7, 17, 19, 20, 27-34, 37, 62, 64, 66
licence 30
package 28
quality 17
reliability 6
systems 28, 66
titleholder 31
vendor 32
vulnerability/vulnerabilities 28, 32, 66
solidarity 46
stakeholders 8, 35, 46, 47, 51, 52, 76
start-ups 38
statutory and regulatory 27
statutory requirements 24, 25, 29
SURFnet 41, 68

T
tablet 28, 30
technology
bio 65
computer 36, 37
information 36, 67, 68
nano 65
terms of service (TOS) 79
testing 30, 31
transparency 46, 51
triage model 42
triage principle 48
trust 46

U
ubiquitous computing 65, 66
University of Amsterdam 15, 22, 23, 38, 69, 71, 73, 77
unlawful act 21, 31, 35
utility 46

V
value domain 45
value pluralism 10, 45, 53
values 10, 16, 37, 44-47, 51, 52, 53, 56-58
virtual reality 64
virtual worlds 80
voice-operated computer 28
Volksvagen 21, 22, 33
vulnerability/vulnerabilities 19, 21, 23, 27, 28, 32, 33, 34, 35, 62, 65, 66, 78, 79

W
wearable computing 17, 66
web technology 17
wellbeing 10, 46, 51, 53

X
XS4ALL 22

Z
ZBOs 23
zero-day attack 66
zero-day exploit(s) 28, 66
Ziggo 22
ZIKA virus 52