Security for the Digital World within an Ethical Framework

Digital Enlightenment Series
Volume 1

ISSN 2542-3746 (print)
ISSN 2542-3754 (online)

Security for the Digital World within an Ethical Framework

by the Digital Enlightenment Forum

IOS Press

ISBN 978-1-61499-723-8 (print)
ISBN 978-1-61499-724-5 (online)
DOI 10.3233/978-1-61499-724-5-i

Publisher
IOS Press BV
Nieuwe Hemweg 6b
1013 BG Amsterdam
The Netherlands
tel: +31-20-688 3355
fax: +31-20-687 0019
email: info@iospress.nl
www.iospress.nl

PRINTED IN THE NETHERLANDS

Contents

Are we going to continue on the road and just allow the governments to do more and more and more control - more and more surveillance? Or are we going to set up something like a Magna Carta for the worldwide web and say, actually, now it's so important, so much part of our lives that it becomes on a level with human rights?

Unless we have an open, neutral Internet we can rely on without worrying about what's happening at the back door, we can't have open government, good democracy, good healthcare, connected communities and diversity of culture. It's not naive to think we can have that, but it is naive to think we can just sit back and get it.

Tim Berners Lee on BBC Radio, March 2014

Preface: Security, Privacy and Ethics in the 21st Century

Digital technologies are now deeply and inextricably embedded across the entire sphere of human activities. People no longer think of the online world as only virtual, in the sense of it 'not being real'. On the contrary, they view digital services and applications as an essential part of their lives and as carriers of great benefits as well as significant threats.

Along with providing immense opportunities for citizens who respect the Rule of Law, the global digital environment also provides a new space for criminals, terrorists and others with malicious intent. Child pornography, hate speech, incitement to violence, piracy of intellectual property, fraud and money laundering have migrated online, and attacks on networks and information infrastructures proliferate. Consequently, cybercrime and cybersecurity have become major concerns.

The global digital space has evolved largely according to the maxim that, at least in theory, "people should enjoy the same autonomy, rights and freedoms online as they do offline". Nevertheless, arbitrary restrictions on access to the Internet and digital media, and unbounded attempts by government or companies to monitor our online activities often interfere with fundamental rights, such as freedom of expression and information, freedom of association, and the protection of our privacy.

How do we maintain the freedoms and as well benefit from the abundant opportunities that the digital ecosystem brings – to express ourselves, to be creative as professionals as well as responsible citizens, to share our opinions freely – while also building into the same digital space adequate safeguards against attacks that intend to harm? How, in short, can we reconcile liberty, security and ethical behaviour in the digital world? The Digital Enlightenment Forum (DigEnlight) takes the firm position that the new regulatory and legal safeguards required in our digital world should continue to be developed within a framework that integrates in the process the new dimension of "digital ethics".

In the last three years such issues have been the focus of intense debate within DigEnlight. This has included the Forum 2015 held in Kilkenny in March 2015; Workshops on Cyber Security for Europe (Brussels, May 2014); Security, Surveillance and Civil Liberties in Cyber Space (Brussels, November 2015); and

Digital Ethics (Brussels, March 2016); and conferences on the Internet of Things (Brussels, November 2015); and Trusted Data Management in Health Care (Amsterdam, June 2016) also dealing with related topics. Reports from all of these are available on the DigEnlight website: **http://digitalenlightenment.org**.

This White Book attempts to draw together these various strands emanating from diverse viewing angles, as well as differing "schools of thought".

It constitutes, we believe, a meaningful contribution to the on-going efforts.

Executive Summary

Digital technologies are now deeply embedded across the entire sphere of human activities. As well as providing immense opportunities for citizens who respect the Rule of Law, the global digital environment also provides a new space for criminals, terrorists and others with malicious intent. Consequently, cybercrime and cybersecurity have become major concerns.

The area of security and privacy online raises acute ethical issues. Respect for privacy and consequences of profiling and filtering; ethics of consent, information collection and storage; right to be forgotten; Internet of Things and Big Data; digital artificial body implants and augmented reality – among many others – all have an ethical dimension. Moreover, digital ethics will increasingly have to accommodate decisions made by autonomous systems (robots, profiling systems, embedded systems, driverless cars, etc.), which are outside of direct human control.

With its increasing reliance on technology-mediated markets, the new digital world significantly exacerbates existing asymmetries of power, knowledge and money in society. The expectation is that individual decisions within the market context will create change as some kind of emergent behaviour. Yet individual citizens may be unwilling or incapable to act and, even when they do, their personal choices are being expressed through technologies over which they have little or no control. Since online privacy and trust involve too many competing and unequal interests to be resolved easily, an elite few get to make decisions of wide-ranging impact for the many.

The power differentials between governments and digital corporations, on the one side, and individual citizens and consumers, on the other, and the ethical issues that arise are at the heart of important debates about how we negotiate the digital world. In particular:

1. **Cybersecurity is being viewed through the prism of national security:** The interface between cybersecurity issues and human rights is becoming ever more complex. State actions aimed at countering cybercrime, threats to cybersecurity and threats to national security (including from terrorism) are increasingly intertwined. The boundaries between civil law enforcement and national security agencies (including intelligence agencies) are being blurred, with both parties increasingly dependent on monitoring and surveillance within the digital environment. Governments

are amassing personal data about people's lives at an unprecedented scale, while surveillance of the public is also becoming the remit of private companies. Across the field there is a severe lack of democratic oversight and control.

2. **Internet governance does not reflect the new realities**: The way the Internet is governed has not kept up with realities 'on the ground'. Although in theory the Internet is governed by principles of international human rights legislation and respect for the rule of law, in practice Internet governance arrangements are not sufficiently robust for these principles to be applied effectively. The role of private companies, which are not subject to international human rights law and often operate under foreign jurisdictions, is increasing. Post-Snowden there is a realisation that existing privacy safeguards are insufficient. Polls indicate that at present people do not see privacy as a priority issue in their lives; yet experience shows that their active engagement will be vital in effecting change.
3. **The personal data ecosystem calls for new approaches to privacy and trust**: The issue of trust is central to cybersecurity concerns and to wider debates regarding the privacy of personal data. Users are increasingly concerned about the ways in which their data is being used, shared and re-used and no longer feel they exert any control. Meanwhile, big data is seen by corporations and governments as the new frontier, offering up new interpretations and insights based on inferences from personal data harvested from elsewhere. This is of particular concern in the security field, where techniques such as filtering and profiling are being used in a manner that directly impinges on human rights. New ethics-based approaches to trust and privacy attuned to the emerging personal data ecosystem are urgently required. Innovative models are emerging across several domains that aim to empower citizens to take control of their personal data.

The challenges thrown up by the global digital society are now so profound and wide-ranging that we need to radically rethink our approach to human rights for the digital age. **The new regulatory and legal safeguards required in our digital world should continue to be developed within a framework that integrates in the process the new dimension of "digital ethics"**.

Addressing the ethical dimension can bring new perspectives on fundamental issues such as: the way in which technology mediates our lives and relationships; the role of non-human agents in everyday systems; the increasing influence of platforms and ecosystems; and the ethical dilution we often experience as a result of digital value chains. The digital ecosystem needs to be underpinned by a solid

ethical framework: one that promotes ethical innovation and supports the practical implementation of ethical principles in the global digital environment.

In restoring trust and enhancing confidence in the Internet, DigEnlight strongly supports moves toward a new social compact based on common, ethics-consistent norms and values. Governments, businesses, law enforcement and intelligence agencies, civil society and other stakeholders should collaborate in taking steps to build confidence around the right to privacy online and respect for the rule of law.

We offer the following Recommendations to help realise a global social compact for digital security and privacy based on ethical principles:

- **Recommendation 1**: The EU should develop a framework for cooperation between Member States on security and cybercrime that includes the activities of national security agencies and provides clear descriptions of the scope of state security and civil law enforcement and their inter-relations. It should be citizen-centric and stimulate increasingly "smart" regulation addressing privacy needs and requirements.
- **Recommendation 2:** Specific policy should be developed within the Digital Single Market (DSM) concerning the production and trade (within EU and beyond) of cybersecurity services and products for the civil as well as for the military and state security markets.
- **Recommendation 3**: DigEnlight should seek dialogue with relevant organisations on the ethical dimensions for digital security and privacy, focusing in particular on cross-cultural issues. This dialogue could be based on the proposal of GCIG[1] for a Social Compact and should lay out a proposal for a set of rules to support designers and developers to deliver ethics-aware services and products.
- **Recommendation 4**: Industry should adopt a shared ethics framework for online data security and privacy within digital business models, including principles of responsibility, accountability and traceability, through self-regulation. The EU and Member States should encourage these approaches and complement them by appropriate regulation if and as needed.
- **Recommendation 5**: Industry and Governments should cooperate to systematically promote EU-wide awareness of the exploding business value of personal data as well as privacy rights and security risks online and mobilise citizens in the search for acceptable, ethics-consistent solutions. DigEnlight will contribute to the development of awareness and the creation of required skills.

[1] Global Commission on Internet Governance, www.ourinternet.org

- **Recommendation 6**: Develop a multidisciplinary research and innovation agenda for a sustainable, ethical and human-centred digital world with attention to mastering complex techno-socio-economic systems and the effects of ever more data, processing power and connectivity.
- **Recommendation 7**: Promote the exchange of views and best practices on ethical principles and approaches both within the EU and internationally. Seek models for useful cooperation, and policy instruments and institutions to enable bridge building and common standards development.

Digital Technology Disrupting the Ethical Basis of Society

Digital technologies are increasingly disrupting the ethical basis of our society. New technologies have a profound social dimension, leading us to re-evaluate the relationship of humans to technology that increasingly mediates every aspect of our lives. The speed and complexity of change seems to lead to a dilution of ethical and social consciousness and a sweeping away of accountability and responsibility for personal behaviour and its results ("it's the system's fault").

Ethical issues relating to digital technologies become particularly acute in the area of security and privacy. Respect for privacy and consequences of profiling and filtering; ethics of consent, information collection and storage; right to be forgotten; Internet of Things and Big Data; digital artificial body implants and augmented reality in neurobiology – among many others – all have an ethical dimension. Moreover, digital ethics will increasingly have to accommodate decisions made by autonomous systems (robots, profiling systems, embedded and connected systems, driverless cars, etc.), which are outside of direct human control.

These changes represent more than simply a transition from offline to online. Digitalisation and networks are changing society in fundamental ways. In particular, they challenge our conception and understanding of trust.

In the pre-digital era trust relied on a social contract between actors at individual, community, regional and national level.[2] [3] Individuals, governments, companies and communities effectively established agreements and practices over what constituted acceptable behaviour. This social contract is breaking down. Nation states, which traditionally have been the defenders of rights and freedoms, are being weakened by neo-liberalism and globalisation. Electronic communication dilutes individual responsibility and adherence to social norms. The rise of global terrorism is leading to power passing to agencies which are increasingly seen as being outside of democratic controls. The open nature of the Internet and the escalating pace of innovation circumvent legislation and regulatory frameworks cannot keep up.

[2] Millar (2015)
[3] O'Hara, Bus in Digital Enlightenment Forum Yearbooks 2013, 2014

With the erosion of the nation state and of organised institutions, increasingly societal concerns are being left to the marketplace to resolve.[4] Rather than imposing (supra)national laws and regulations or creating economic incentives through grants and tax rules, we rely on the concerns and personal choices of individual citizens to create societal change. On the issue of obesity, for example, individual citizens are being left to police their unhealthy food consumption rather than regulating the food industry or promoting healthy eating. We rely too much on individuals' personal choices to invest in solar panels, buy organic food, and use their cars less often rather than creating long term strategies to make our economies more sustainable. The hope is that individual decisions 'in the marketplace' will create such change as some kind of emergent behaviour. Yet individual citizens may be unwilling or incapable to act. Society is atomising and it is becoming more difficult to find common norms and values. As a consequence, we see a fracturing of the reference points for a shared political and social life.[5]

What has all this got to do with security, privacy and civil liberties? Well, the marketplace is increasingly digital. Personal preferences can now be expressed more directly, through direct interaction with the consumer or the citizen. These preferences can also be measured by monitoring our behaviour on the digital platforms we use. Technology platforms such as smart electricity meters and personal health monitors provide feedback to users that allow them to adjust their behaviour where necessary. This information is not only shared with the people directly concerned, but it is also shared and processed for other purposes, often in a non-transparent way without the user's explicit knowledge or consent. In short, our personal choices are being expressed through technologies over which we have little or no control.

The new world order exacerbates existing asymmetries of power, knowledge and money in society. Everything we do online is mediated through at least one other party who is able to collect, aggregate, pseudonymise and anonymise our data. The terms and conditions under which we surrender our data are often unclear. When users click "I agree", it is often with a sense of coercion, to access essential information or services, rather than through truly informed consent. Relinquishing control over their data is the price they must pay. This leads to distorted outcomes; users accept a 'bargain' that is in the short term attractive, but in the long term far less oriented towards their interests than they may suspect. Since online privacy and trust involve too many competing and unequal interests to be resolved easily, an elite few get to make decisions of wide-ranging impact for the many. Moreover, it has become apparent that digital networks are the subject of

[4] Hoepman (2015)
[5] Crawford et al (2014) referencing papers by Mark Andrejivic and Nick Couldry & Joseph Turow

massive and creeping surveillance by states and private corporations, without sufficiently strong democratic controls being available.

The power differentials between governments and digital corporations on the one side and individual citizens and consumers on the other are at the heart of a number of debates about how we negotiate the digital world. They influence how:

- states undertake surveillance on their citizens, within or without the rule of law (Section 2);
- the Internet is governed and human rights are positioned within the online world (Section 3);
- the market power of digital corporations is exercised in emerging areas such as personal and health data, which represent the new frontiers for both the big data economy and for mass surveillance (Section 4).

The following sections survey the field in each of these areas, setting out the issues, while Section 5 outlines the contribution of ethics to these debates. Recommendations that flow from this for DigEnlight and for the wider stakeholder community are then presented.

Cybersecurity Viewed through the Prism of National Security

2.1 Concepts and principles

One of the key challenges in this debate is in finding a common frame of reference. The whole field is peppered with concepts and terms that are open to interpretation and context dependent. Terms such as 'security', 'liberty', 'privacy', 'ethics', and 'public good' vary not just from one observer to another, but from one culture to another and evolve over time. The main concepts are sketched here in outline in order to help structure the debate.

Security and the public sphere

Security is a complex concept, deeply rooted in European philosophy and history.[6] It encompasses both the private and social sense of security (of being safe and secure in one's home, for example) and the political, public and military sense (a society that safeguards its people and secures its own future). At the turn of the Millennium, the hope was to broaden the political, public concept in order to embrace the social approach as well. This was reflected most evidently in the Millennium Goals, which addressed the challenge of global poverty and the lack of development. Security in the social sense was regarded as one, if not the most important means to international peace.

It did not take long, however, before the traditional framework, based on securing the public sphere, re-emerged in the wake of the financial crash, terrorist attacks and the rise of political extremism. Security threats became the 'other side' of globalisation. Whether rightly or wrongly, the notion gained momentum that states must respond to these threats through increased surveillance measures. As surveillance technologies became more and more sophisticated, some saw this as an opportunity to secure the public sphere through digital means. Unlike 20th century security policies, however, globalisation turned the national public sphere into a *global* public sphere that ignores national borders and/or national laws.

As far as its own policies are concerned, the European Union has adopted a definition of security as "protecting people and the values of freedom and

[6] See EGE (2014) for an overview.

democracy, so that everyone can enjoy their daily lives without fear".[7] The European Agenda on Security, issued in 2015, aims to strengthen the tools that the EU provides to national law enforcement authorities to fight terrorism and cross-border crime.[8] In particular, the Agenda focuses on improving information exchanges and operational cooperation between law enforcement authorities. It also mobilises a number of EU instruments to support actions through training, funding, and research and innovation. Finally, the Agenda sets out a number of targeted actions to be taken at EU level, to step up the fight against terrorism, organised crime and cybercrime. This has led to a blurring of the boundaries between civil security through law enforcement, and state security through national security agencies (NSAs), including intelligence services. Moreover, there is still a lack of common EU definitions of the concepts and few frameworks or rules on how to guarantee that NSAs are subject to democratic control.

The notion of surveillance, too, comes with a rich and textured layering of meaning. With origins in the French verb *surveiller* (to oversee), it first entered English during the French Revolution when 'surveillance committees' were set up to monitor the actions of foreigners, dissidents and suspect persons. As noted above, in the digital age surveillance has become intricately bound up with the notion of security. However, not all security technologies involve surveillance in a direct way and not all surveillance technologies have security as their stated goal.

Dignity, privacy and liberty

The term human dignity (or personal dignity) is frequently cited in digital ethics debates. This, too, is an extremely broad concept; arguably so broad that it risks becoming devoid of practical meaning.

In the wake of the Industrial Revolution, the human rights movement sought to secure the wider social good by reducing obstacles to respect for the individual. The resulting framework, codified in the Universal Declaration of Human Rights (UDHR), takes as its starting point the inviolability of human dignity. Personal dignity can be understood as a fundamental moral property of people that they are normative agents worthy of respect. It is also a foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data. Violations of dignity may include objectification, where a person is treated as a tool serving someone else's purposes.

In the information technology world protecting the dignity of users and others affected by computing systems has long been accepted. In 1992 the Association for Computing Machinery (ACM) included in its code of ethics a commitment that:

[7] European Council quoted in EGE (2014)

[8] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/index_en.htm

"Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity."[9]

Privacy is an integral part of human dignity and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for erosion of privacy and dignity through large-scale personal data processing. In the 21st century, with all activity potentially always online, the challenges to privacy and dignity are of an entirely different order. The nature of personal data is likely to change radically as technology increasingly allows individuals to be re-identified from supposedly anonymous data. In addition, machine learning and the merging of human and artificial intelligence threaten to undermine concepts of the individual's rights and responsibilities.

Finally, there is the concept of liberty. There are two lines of understanding here. The first sees liberty as a negative normative value, where an individual is free **from** certain constraints and restrictions. The second is liberty as a positive normative value, where a person is free **to** act in certain ways. Building on this duality of liberty, we cannot understand the relationship between liberty and security as one of balance or trade-offs: rather they are mutually constitutive and each requires the other to operate.

A further issue is the tension between individual and collective or societal security. The role of the individual is essential in the relationship between liberty and security. But there is also a growing discourse on the collective good, which stresses the increasing value placed on putting the collective good above and before that of the individual. Can we say that liberty stops where it endangers society? It is often said that individual freedom stops where the freedom of another is threatened. But who is to decide how and when that threat arises? If we are to avoid this becoming a political question then we would need to define not just what we mean by liberty but also define the nature of the danger to society.

The role of privacy is important here too. Privacy is essential to the health of a democratic society, not just an individual right. Society benefits from the ability of people to exercise their rights and freedoms. Privacy rights, like most other rights, are not absolute. Someone for whom there are sound grounds for suspicion of involvement in a serious crime or terrorist activity might forfeit privacy rights while the purported offences are investigated. But any such breaches of privacy, and the methods used to accomplish them, should be accountable and transparent.

[9] Quoted in Kamphorst (2012)

2.2 Cybersecurity trends and challenges

Cybersecurity and human rights

Cybersecurity issues often touch on human rights, for example when they involve monitoring of the activities of individuals in cyberspace; pulling of data on individuals (or that may also relate to individuals) from cyberspace; or the storing, sharing, analysing and further usage of such data, including profiling and its associated consequences.[10] Any such monitoring or collection, etc., constitutes *ipso facto* an interference with at least the privacy rights and the right to data protection of such individuals, and possibly with their rights to freedom of expression, freedom of association, and freedom of religion. Moreover, if such measures are taken as part of criminal investigations (or may lead to such investigations), they raise fair trial – and fair investigation – issues.

The interface between cybersecurity issues and human rights is complicated and is aggravated:[11]

- if the measures involve cooperation – and data exchanges – between state and private entities, in particular companies active in cyberspace, such as Internet Service Providers (ISPs), mobile network operators (MNOs), and social network service providers (SNSs);
- if the measures involve cooperation – and data exchanges – between law enforcement agencies and national security agencies; and/or
- if there are transnational/international aspects to the measures, i.e., if they either involve actions of entities in one country that directly affect individuals (in terms either of their data or their rights) in other countries (such as the pulling of data from a server in one country for analysis in another country). Similarly, if they involve cooperation between entities, whether public or private, in different countries.

Of course, if several of these factors are present, the complications are multiplied.

Cybersecurity and national security

Cybercrime and cybersecurity have become major concerns. These threats are increasingly transnational, and while there is broad international consensus on the need for action, there is much less agreement on specific threats, or even what constitutes a threat.

Approaches to cybersecurity and the role of the intelligence services in combating cyber threats vary markedly between Member States.[12] In general,

[10] See CoE (2014) for a detailed discussion of human rights aspects.
[11] CoE (2014) and Korff (2014)

cybersecurity issues are increasingly being viewed through the prism of national security. Four issues stand out:[13]

1) State actions aimed at countering cybercrime, threats to cybersecurity and threats to national security (including from terrorism) are increasingly intertwined. The boundaries between such activities are blurred, and the institutions and agencies dealing with them work more closely together. Some of these agencies are subject to judicial oversight but others are inherently secret and controlled only politically.
2) States are now co-ordinating their actions in all these regards, although with no agreed common framework or rules.
3) The work of national security and intelligence agencies increasingly depends on monitoring the activities of individuals and groups in the digital environment.
4) Instead of *ex post facto* law enforcement, the emphasis is now on intelligence and prevention, with law enforcement agencies using techniques – and technologies – previously reserved for national security agencies.

Efforts to define cybersecurity as inherently being part of national security present a serious threat to the rule of law.[14] Firstly, individuals suspected of a wide range of crimes – including crimes not in any way involving violence – are increasingly treated as, or on a par with, "terrorists" and others "threatening the fundamental [constitutional] order of the State". Secondly, the law enforcement agencies in states supposedly strongly committed to the rule of law increasingly not only work with, but are beginning to adopt the methods, practices and ethos of the security agencies, who have too often been shown to have little regard to the rule of law.

All of this was brought into stark relief by the Snowden affair.[15] Before the Snowden revelations regarding the US National Security Agency and its partner agencies, most people assumed that surveillance was limited to what was necessary and proportionate for the agencies to fulfil their prescribed role. People assumed that oversight mechanisms were in place to ensure that surveillance was appropriately constrained. We now know that mass surveillance has become the norm. Nations are amassing personal data about people's lives at an unprecedented

[12] For a detailed review of the current situation see FRA (2015).
[13] CoE (2014) and FRA (2015)
[14] Korff (2014)
[15] EGE (2014), CoE (2014)

scale, far beyond most people's wildest expectations. Furthermore, surveillance of the public is becoming the remit of private companies as well as nation states, although for different purposes.

It is clear that there is a severe lack of democratic oversight across this whole field. Agencies (and companies) have taken advantage of a regulatory vacuum. Under the guise of national security, intelligence and law enforcement agencies have embarked on courses of action that would be illegal in the offline world. As one respondent on the DigEnlight blog noted: "Placing 'cyber' in front of a word is a signal that normal rules of law do not apply here." If we want to preserve the State under the Rule of Law (*der Rechtsstaat, l'État du Droit*), we must fight these emerging trends, and in addition bring the Member States under a common EU set of rules and definitions to enable an effective cooperation between services and control on their activities.

Internet Governance Does Not Reflect the New Realities

The Internet is, in theory, governed by principles that stress the need to apply public international law and human rights law equally online and offline, and to respect the rule of law and democracy on the Internet.[16] These principles recognise that Internet governance involves multiple stakeholders and urge all public and private actors to uphold human rights in all their operations and activities, including the design of new technologies, services and applications. They also call on states to respect the sovereignty of other nations, and to refrain from actions that would harm persons or entities outside of their territorial jurisdiction. In practice these principles remain largely declaratory and aspirational. Actual Internet governance arrangements are not sufficiently robust to be relied on to ensure the application of these principles in practice. The fact that the USA has, partly because of its corporate dominance and partly because of historical arrangements, more control over the Internet than any other state also has to be taken into account and is an issue in discussion in the Internet Governance Forum (IGF). The UN's recent declaration of Access to the Internet as a human right may be a first step towards more general principles.[17]

Meanwhile, private-sector control of the Internet is increasing. Much of the Internet infrastructure and the wider digital environment is controlled by a handful of private entities, almost all of them US corporations. Private companies are not directly bound by international human rights law and it is more difficult to obtain redress against such companies. In addition, private entities are subject to the national laws of the countries where they are established or active, which may not always conform to international law or international human rights standards.

For individuals, too, the idea that we must abide by the laws and mores of the country where we live is problematic and likely to become more so. The ability to effectively "be" in another country (through video links and geo-location of IP address), as well as the increasing global mobility of people, means that it is increasingly difficult to decide what laws and mores a person should operate under.

[16] CoE (2014)

[17] UN Human Rights Council (HRC) resolution on "The promotion, protection and enjoyment of human rights on the Internet" (A/HRC/32/L.20). Linked at https://digitalenlightenment.org/news

Should it be those of the country where they are situated today; or where the service they are accessing is provided from (if that can be determined); or the country where they normally reside? The whole concept of laws and mores needs fundamentally rethinking.

In Europe, data privacy has long been an area of public concern. The realisation post-Snowden that effective safeguards are lacking came as an unpleasant surprise to many and has heightened citizens' anxieties. In theory, national and international law restricts how states use technology to infringe human rights, even for national security purposes. Yet time and again these restrictions have been shown to be lacking.

Overall, people do not see privacy as a priority issue for research and innovation. In a 2014 Eurobarometer survey only 11% of people ranked the protection of personal data as a high research priority for the next 15 years.[18] In the public mind, data protection ranks alongside quality of housing: nice to have but very far from essential. Despite all the fuss, in the EU privacy is still a political rather than a social priority. As with environmental issues and promoting healthy lifestyles, experience suggests that things will not really change until individual citizens become better informed and start taking matters into their own hands.

[18] Quoted in Floridi (2014)

The Personal Data Ecosystem Calls for New Approaches to Privacy and Trust

4.1 Trust and the personal data ecosystem

An aspect common to both cybersecurity concerns and to wider debates on the privacy of personal data is the changing nature of trust.

In the pre-digital era the issue of trust was straightforward. A user chose to disclose their data to others based on the level of trust in their relationship.[19] Generally this involved an implicit calculation: "Is the value I get from disclosure greater than the risk of something bad happening, given what I know about the integrity of the other party?" The march of technology has taken away the decision to disclose or not disclose. Apps and mobile devices mean people are "always on". Ubiquitous sensors and monitors, such as mobile phone location sensing, CCTV with face recognition, and embedded systems, collect data about us wherever we are. And the power of big data analytics allows inferences to be made from data brought together from many different sources. In a post-digital world we no longer have the ability to assess the integrity of those making use of our personal data. In effect, trust is broken.

There is a growing gap between users' expectations and the ways in which their data is actually being used, shared and re-used. Even where use is 'legal' it may not be 'legitimate' and even less 'ethical'. A user might sign up to a usage statement that was more general than they realised; or they may be opted in by default; or there may be an implicit consent step of which they were not made sufficiently aware. Either way the outcome would come as an unpleasant surprise to the data subject.

European legislation attempts to address these issues. The updated General Data Protection Regulation (GDPR) requires organisations that process personal data to implement appropriate technical measures to protect individual's rights.[20] By default, organisations should only collect the minimum personal data they need, and allow individuals to control the distribution of their personal data. The GDPR also requires companies to make it easier for users to download all of their data, for

[19] Wilton (2014)
[20] Brown (2014)

example so that it could be uploaded to a competitor service, bringing market pressure to bear.

But the boundary between public and private knowledge is rapidly and dramatically changing as the personal data ecosystem expands.[21] Firstly, more personal information is becoming public that previously was known only to the individual and disclosed to trusted others. Secondly, more information about the individual of which they were previously unaware is also being shared, and thereby made public. Thirdly, there is inferred data: data about individuals – and also groups of individuals – based on inferences from personal data harvested from elsewhere.

It is this third category – the reliance on inferred data – that is the most challenging. Inferred data relies on finding small patterns in large data sets for which context or assumptions for collection are often not or only partly known. The data algorithms are programmed and the results interpreted without context, often without any sensitivity or respect for the individual. Correlation does not mean causation. But once data has been interpreted, it becomes real and is reinforced without the subject having any opportunity to correct errors. The risks to privacy here are two-fold. Firstly, anonymous data can be processed with increasing sophistication, allowing users to be re-identified. Secondly, inferences are being drawn not from data we have disclosed about ourselves, but from the data disclosed by others. The net effect is to dilute the accountability for data use and any resulting harm, making recourse impractical or even impossible.

Thus, the big data economy further accentuates the power and knowledge asymmetries. One commentator has called big data a "honeypot, where a lot of money can be made in a domain with no rules".[22] Another has warned of big data becoming "the oil of the 21st century, a new way of making money – big money".[23] Yet another has talked of a "big data divide" between us and our data.[24] Not only are we rarely granted access to our own data, we lack the capability to analyse and make sense of it, particularly in the context of other users. Access to data sets, together with the technologies, infrastructure and expertise to analyse them, reinforce power differentials between those who have the capacity to make use of big data and those who are simply part of the sorting process. Nowhere is this more true than in the field of security where, as we have seen, techniques such as filtering and profiling are being used in a manner that directly impinges on human rights.

[21] Wilton (2014), Wilton (2016), Crawford (2014)
[22] Millar (2015)
[23] Helbing (2015), p.14. The book offers a wide ranging critique of the opportunities and risks arising from big data and how these forces can be harnessed to create a smarter society.
[24] Mark Andrejevic quoted in Crawford et al (2014)

The open data movement has sought solutions through making data publically accessible. This movement claims that open data will support democratic politics and individual liberty, unequivocally allowing individuals to use the wealth of data produced by governments and enterprises to take greater control over their lives and improve both their material and social conditions. However, some commentators have criticised this view as naïve, arguing that the open data movement has failed to understand the constructed nature of data.[25] Social privilege becomes embedded in the datasets as they are constructed; users have differential capabilities (in particular differences between citizens and enterprises); and data systems inevitably impose their own norms. In all of these areas, it can be argued that open data has the potential to exacerbate rather than alleviate injustices, necessitating a general theory of information justice.

Whether open or not, it is clear that many of the myths around big data need to be debunked. Big data are seen as reliable, value-neutral sources of information. But data of any size do not operate in a social vacuum. Databases, however large, are still structured in ways that privilege certain ontologies and obscure others. Social theory tells us that aggregated, individual actions cannot, in and of themselves, illustrate the complicated dynamics that produce social interaction. Data sets are not, and never can be, neutral and theory-free repositories of information waiting to give up their secrets. They require the active interpretation of experts, each of whom has their own bias and blindspots. Big data, whether applied in the security field or more generally, is increasingly seen as an area in need of deeper critical engagement and a stronger ethical dimension.

4.2 Personal data repositories

Alternative governance models are emerging across several domains that aim to empower citizens to take control of their own data. So-called personal data repositories are analogous to a bank account where individuals are able to safely and securely store, manage and actively share their data on transparent terms. Some of these personal data banks are intended as not-for-profit cooperative organisational structures owned by the citizens. Revenues from citizen-controlled secondary use of data would be invested in projects and services that benefit members and society at large.

Some of these new, value-based infrastructures are already being piloted. One such case is MIDATA.coop, a Swiss initiative building a citizen-centred repository for personal health data.[26] It is owned by citizens as a cooperative; is not-for-profit,

[25] Johnson (2014)
[26] Trusted Data Management in Health Care, DigEnlight Conference Report (2016)

built on open source code; has transparent governance; and operates to the highest security standards (based on data encryption). MIDATA is foreseen as a federation of national personal data cooperatives providing a common IT structure and data exchange platform, similar to the way SWIFT operates for financial exchanges. The MIDATA.coop organisation has been founded, a legal and ethical framework for cooperatives is under development, and the first pilot projects started in Switzerland in May 2016.

Another example is MyData, a model for human-centred personal data management and processing that is user controlled.[27] It enables data to be used to create new services which help individuals to manage their lives. The approach empowers users to manage their data and privacy, adopts open formats that make data easy to access and use, and promotes an open business environment that avoids proprietary data lock-ins.

[27] Poikola et al (2014)

Ethics Can Help: Towards a Framework for Digital Ethics

5.1 The contribution of ethics

What can ethics contribute to this debate? What are the ethical issues relating to cybersecurity, privacy and big data?

Digital ethics aims to understand how subjects – human beings, organisations, computers, software, connected objects, drones and robots, etc. – must act and behave towards each other and those around them. As noted in the Introduction, digital ethics will also have to deal with decisions made by autonomous systems.

Increasingly, the digital world throws up issues that challenge our most fundamental conceptions of human rights, such as the right to security, to privacy and human dignity, and to freedom of expression and information. It is not simply a matter of needing to balance one right against another. Arguably, the challenges are now so profound and wide-ranging that we need to radically rethink our approach to human rights for the digital age.

Digital ethics precedes and extends law, which largely tracks the evolution of digital behaviour with regulation, more often than not endorsing *fait accompli* usage.[28] We need to think more deeply than that. It is necessary to create rules very early on, for example on whistleblowers and other forms of behaviour that challenge accountability and transparency, in order that everyone acts with best intentions in the digital world, without disturbing others and the environment.

In its debates around security and privacy DigEnlight has identified many issues and relationships with an ethical dimension. Some of the most significant are:

1) *Disempowerment and loss of human agency*: In our technologically-oriented society, almost every action we are able to take (what ethicists call our 'agency') is mediated, either through technology, such as computers, phones etc., or through third parties, such as banks, the retail supply chain, telcos, Internet service providers, identity providers, and so on. Ethically, the fact that what we do is mediated often moves us further from the

[28] Floridi (2013)

consequences of our decisions and actions. Even more fundamentally, the prevalence of technology-mediated phenomena distances us from societal norms such as equality, fairness, and justice, and so challenges our core understanding of what it means to be human. The asymmetry in power between individuals/users and service providers (both commercial and public) leaves us feeling disempowered and that we are losing our human agency. Can we design systems that empower users and so restore human agency, and what does this mean in reality?

2) *The ethics of non-human agents*: A growing number of digital agents are non-human and in some cases are increasingly capable of autonomy (robots, drones, self-driving cars, etc.). Algorithms are responsible for decisions in a wide range of areas these days (for example in stock marketing trading), and any algorithm that makes decisions is not ethically neutral. Some algorithms are adaptive, able to learn and adjust their behaviour over time. We have to understand how such actors affect us and our societies. Autonomous systems, such as self-driving cars will react to changing conditions and deal with circumstances that they have never encountered before, without human intervention. Does it make sense to think of these technological systems as ethical agents in their own right? Is there a fundamental ethical principle based on 'global' human values? What is the ethical status of machines that are increasingly autonomous and might even, at some point, be described as conscious?
3) *The ethics of platforms and eco-systems*: As more and more activities come to be mediated by technology, the platforms by which that mediation takes place are increasingly influential. They articulate themselves carefully to users, clients, advertisers and policy-makers, making strategic claims for what they do and do not do, and how their place in society should be understood. In effect, platforms are becoming curators of public discourse and values. Yet the ethical implications of this change have received little attention.

   Again, much of the influence of platforms is due to the power of hidden – and unknowable – algorithms. Algorithms are not the same as software code, which is (or can be) made visible and subject to intellectual property laws. They underlie the methodologies and business models of the digital world. Facebook's algorithms, for example, choose which pictures and adverts users are shown when they login, giving them enormous power over users. This has important consequences as Facebook evolves from a social media network to a commercial platform funded primarily by advertising. There is a risk that we are unable to define the ownership of

algorithms and hence lose the ability to attribute responsibility for them and the actions that result.[29]

4) *Ethical dilution:* The issue of costs and benefits is critical to this debate. Humans are not good at making trade-offs and seldom make decisions in a rational way. For example, we tend to scrimp on purchasing insurance because the costs are short term whereas the benefits, in terms of payouts, are long term (or may not accrue at all). Similarly, in social networks we over-share because the benefits come first and the costs come later.

   Part of the problem with digital value chains is that individuals' ethical judgements about the disclosure or collection of personal data get distorted (one could also say 'diluted') by a number of practical factors. The apparent benefits may be immediate – interacting with one's social circle – whereas the costs/disbenefit (e.g. intrusion of privacy, security infringements, monetisation of personal data) may be deferred and remote. Even where disclosure takes place actively and willingly, the user may be doing so on the basis of a flawed, incomplete or misleading set of assumptions. When the ecosystem is so complex, it is all too easy to blame someone or something else, and cause and effect become difficult to attribute. The impact on a given individual may be minimal even though the overall effect may be significant (e.g. mass interception of communications). And some forms of harm, such as damage to a person's reputation, can be difficult to quantify in ways that allow clear remedial action to be defined.

5.2 Ethical frameworks for digital security and privacy

The digital ecosystem needs to be underpinned by a solid ethical framework. As the European Data Protection Supervisor has pointed out, better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics.[30]

Ethics is often seen as a barrier to innovation in digital technologies by imposing unnecessary constraints. Yet the assumption that ethics and innovation contradict is not necessarily true. Rather we should think of ethics as an innovation challenge and encourage technologists to come forward with solutions that reinforce ethical behaviours. Value-based design, for example, draws on a long

[29] In the UK, the Royal Society is addressing the role of algorithms as part of its investigation into the potential impacts and applications of machine learning. See http://royalsociety.org/news/2015/11/machine-learning/

[30] EDPS (2015)

tradition in ethics-based innovation (see box). Moreover, the issue is wider than just data: we have to consider aspects such as software (implemented rules and machine learning) and storage as well. Without an all-embracing 'ethics of computation', we will miss the scientific problem.

Time is not on our side, however. Mass adoption of digital technologies is already underway and we have a critical window within which to build ethical values into digital structures which will define our society.

This should not be an esoteric, academic exercise. On the contrary, much research into ethical practices already exists and at a more practical level ethical behaviours are well understood.[31] However, there is a clear gap between the existing research and the practical implementation of ethical principles in the modern digital environment.

In developing such a framework, we need to consider at least four basic elements:

- A clear conceptual model of ethical principles that reflects human dignity and fundamental rights;
- Ensuring ethical practices are built on existing regulatory compliance;
- Ethics in the research and design process;
- Ethics and operational practice.

Essentially, the aim should be to give practitioners a toolkit for putting ethical data-handling into practice. It should address issues such as: distinguishing ethics from legal compliance; the rationale for ethical practices and how to assess the costs and benefits; how to build ethical principles into product and service design and development processes; operationalising ethical approaches across the organisation and adapting them to different cultures and jurisdictions and their evolution.

[31] Wilton (2014) and Wilton (2016)

Ethical Innovation

Value-based design or value-sensitive design is one school of thought where interesting new ideas are emerging.

The argument here is that innovation in digital technologies has become fixated on functionality. A continual drive for more and better functionality has created 'hype cycles' where industry buyers and end-users are fed insufficiently mature technologies at ever increasing rates. This self-inflicted pressure to keep up with the hype cycle often leads to even the most obvious and rudimentary values, such as the usability of systems, being neglected. Managers and end-users alike lose sight of the true benefits of IT as they get caught up in the never-ending quest for the Next Big Thing.

Value-based design stresses an approach to innovation that supports human values rather than simply innovation for its own sake. It may be viewed from two perspectives. Firstly, value-based design can be used to consciously foster value creation through IT. Secondly, it protects values that could be undermined or destroyed by thoughtless IT design. If IT managers and engineers focus on creating IT values throughout the entire design process while rigorously controlling for value risks, they would support the flourishing of human beings much more than they do today.

Spiekermann, one of the leading protagonists of this school, explains the potential of adopting value-based design as follows:[32]

"Machines would then be designed to strengthen people's values such as health, increase their sense of privacy, freedom and autonomy, help them trust, and so forth. In the long run, we could even envision that machines support the development of cognitive skills such as learning, help them rediscover their senses, have more ethical integrity, be more just in their decisions and so on."

Also drawing inspiration from the value-sensitive design tradition, Kamphorst has set out guidelines regarding the 'rights' of autonomous agent systems in relation to human users or operators.[33] One such guideline is that: "Under no circumstances may an autonomous agent ever be harmful to anyone's personal dignity". Another is that: "Autonomous agent systems should be respectful of people's autonomy. They may not diminish a user's autonomy, unless otherwise directed by law".

5.3 Towards common norms

The development of the global digital connected society requires trust and security based on sound regulation of the use of personal data. Yet this is hampered by conceptual differences between states and between stakeholders on issues relating to privacy and data protection and, more broadly, on the issue of

[32] Spiekermann (2015)
[33] Kamphorst (2012)

universality of human rights within the digital space. The opposition between these two factors is reaching crisis: society's ability to fight crime and combat terrorism is being threatened; consumers' trust in the digital products and services essential for innovation and economic growth is being eroded; and citizens' trust in the way governments and businesses collect and use private data is being undermined.

So what is to be done? How can we forge a global digital environment that is safe and secure, and based on firm ethical foundations? Can we develop a basic informational ontology for a digital world comprised not just of humans but also information entities? How, in short, do we reconcile security, privacy and ethics in the twenty-first century?

In the wake of the Snowden revelations about surveillance by the state, there have been several calls within DigEnlight debates for "a new social covenant or contract". Tim Berners Lee has proposed a "Magna Charta for the Internet" (see frontispiece to this report) while, more recently, the Global Commission on Internet Governance (GCIG) has called for a new social compact for digital privacy and security.[34] Consensus is growing around the need for an agreement, which includes implicit social and moral rules as well as explicit technical and legal rules, between parties constituting a society in the digital world, which of course includes the role of artificial intelligence and information systems.

DigEnlight strongly supports the concept of **a new social compact for the global digital society based on common norms and values**. Governments, businesses, law enforcement and intelligence agencies, civil society and other stakeholders should collaborate in taking steps to build confidence around the right to privacy online and respect for the rule of law.

Is it feasible or desirable, given the global nature of the Internet, to aim for global ethical values and guidelines? How can we accommodate such a diverse range of interests and objectives? The answer, surely, is that we at least have to try. Attempts to adapt frameworks and approaches from the pre-digital world have been largely unsuccessful, partly because of the huge asymmetries in power. But the fact that existing frameworks have not delivered should not deter us from seeking alternatives. We should strive for an ideal while being brutally realistic about the problems and differences, for example the extent to which values vary between cultures and across time.

While we will never overcome or remove the power asymmetries in society, much more could be done to empower individuals to play a more active role. People need to be given the power and means to develop themselves as autonomous, creative entities whose dignity is respected.

[34] GCIG (2016)

Transparency is one way of empowering individuals and accommodating dynamic values. Greater transparency rebalances control in favour of the individual. It enables people to understand how they might be manipulated and act against it. Auditability, judicial oversight, etc. are democratic mechanisms that help to keep asymmetries in check. We need transparent and open political processes with governments responsible and accountable to their citizens. We also need transparent, auditable and accountable processes, services and products in enterprises and other organisations which comply with the political decisions.

This move toward a global social compact for digital security and privacy based on ethical principles is outlined further in the Recommendations that follow.

Recommendations

6.1 Develop ethical cooperation on security and cybercrime

Recommendation 1: The EU should develop a framework for cooperation between Member States on security and cybercrime that includes the activities of national security agencies and provides clear descriptions of the scope of state security and civil law enforcement and their inter-relations. It should be citizen-centric and stimulate increasingly "smart" regulation addressing privacy needs and requirements.

The CoE Commissioner for Human Rights has set out a thoughtful agenda on how the regulatory environment in Europe relating to digital security and privacy needs to be reformed and modernised.[35] Among many other issues, the report calls for Member States to bring the activities of national security and intelligence agencies within an overarching legal framework. Until there is increased transparency on the rules under which these services operate – domestically, extraterritorially and/or in co-operation with each other – their activities cannot be assumed to be in accordance with the rule of law.

DigEnlight echoes this call. Stakeholders should work towards a Europe-wide framework for cooperation on cybersecurity and cybercrime that is citizen-centric and based on ethics principles. There should be clear and common rules on aspects such as:

- Respecting human rights in actions against cybercrime, including all obligations under European and international law.
- The extraterritorial exercise of national jurisdiction in relation to transnational cybercrimes.
- The activities of NSAs and the scope of, and inter-relations between, state security and civil law enforcement.
- The regulation of private companies that impose restrictions that are in violation of the human rights obligations under European law.

[35] CoE (2014)

- Constraints on and respect for national jurisdictions online (for example, the supremacy of laws within the country of residence when it comes to freedom of expression).
- Transparent legal frameworks on the use of filtering and blocking and guarantees of judicial oversight.

Such an ethics-based approach is important in ensuring that human rights are respected around the world and Europe can play an exemplary role here. The EU's approach to privacy is already influential internationally, with over 100 countries having adopted the Data Protection Directive or similar laws. The GDPR presents the opportunity to spread the EU's sphere of influence even further. Europe needs to retain momentum and seize the opportunity to put a coordinated European approach at the heart of a global privacy- and data protection framework based on ethics and human rights.

The GDPR is very new and there will be scope for exchanges between parties as experience develops. In particular, it will be useful to explore the lessons from these experiences for personal data repositories and any further regulatory reforms that might be needed (e.g. in enabling citizens to have the legal right to a digital copy of all their personal data).

Existing policy instruments, such as the Network and Information Systems (NIS) Directive (see Recommendation 2) and GDPR, must continue to evolve so as to address both technological developments and privacy needs and requirements. We need 'smart regulation' that reacts quickly to new markets and applications, for example by removing barriers to innovation in areas such as personal medical devices and freeflow of data.

In the longer term, we may need to think about bringing data protection law directly within the remit of human rights legislation. For example, it could be argued that data collection and processing should only be allowed where there was a 'justified interest' for the actors concerned or for society and that all such actions would be subject to provisions on dignity and human rights. In practical terms this would equate to a major change in thinking on data protection: but by the time the next revision of the GDPR comes around – in say 5-10 years' time – it may well be in the mainstream. Certainly, we should start the debate now.

6.2 Develop a European framework for cybersecurity products and services

Recommendation 2: Specific policy should be developed within the Digital Single Market (DSM) concerning the production and trade (within EU and beyond) of cybersecurity services and products for the civil as well as for the military and state security markets.

With cybersecurity products and services of growing importance in a number of policy domains, it is in the EU's strategic interest to retain control over their development and trade. From the standpoint of defence policy, such control will be essential to keep ahead of rogue states or communities in order to protect cyberspace. Independence is also essential in the context of foreign policy (the 'friends' of today can be the 'enemies' of tomorrow) and social policy (i.e. retaining the ability to adapt security measures to our own security and privacy culture).

At present Europe's Digital Single Market (DSM) does not function effectively in relation to security-sensitive products and services. Each Member State has its own definitions and rules in relation to these products and services and there are differences in implementation and interpretation of import and export regulations. Some Member States act partially in accord with UN recommendations and/or with US practice with respect to export rules, for example in the implementation of certain economic sanctions. In general, each Member State follows a trade policy for cybersecurity products and services that is aligned to its own national interests. This creates a big economic disadvantage for the EU cybersecurity industry and a strategic political disadvantage for the EU as a whole.

The EU urgently needs a common approach. A well-functioning Single Market for cybersecurity products and services will lead not only to stable and strong opportunities for the EU cybersecurity industry, it will also enhance Europe's political influence in international debates.

Important parts of the required policy framework are already in place. The Directive on Security of Network and Information Systems (so-called 'NIS' directive), which came into force in 2016, is the first comprehensive piece of EU legislation on cybersecurity and a fundamental building block for future work in this area. It requires companies in critical sectors, such as energy, transport, banking and health, to adopt risk management practices and report major incidents that can affect the DSM to their national authorities. It also obliges online marketplaces, cloud computing services and search engines to take similar security steps. Greater cross-border cooperation on these issues is also foreseen, including

through the new Cybersecurity Public Private Partnership (CPPP), a partnership with industry on cybersecurity.[36] The CPPP will focus on early stage research and innovation, including engagement with end-users to elicit future requirements for cybersecurity solutions.

DigEnlight welcomes the recent Commission Communication on Cybersecurity, which announced the launch of the CPPP and other market-oriented policy measures to boost industrial capabilities in Europe.[37] The EU must cease the opportunity presented by the CPPP and other policy instruments to create an agenda to build its own globally competitive cybersecurity industry. This should include (but not be limited to) measures in relation to:

- Stimulating **responsible security and privacy research** by the EU industry and research community; (see Recommendation 5)
- **Transparent procurement** of cybersecurity products, preferably from EU companies;
- **Transparently enforced trade rules** on export and import of cybersecurity products similar to those for other military materials, recognising also that some technologies have dual use.
- **Certification** of the security of ICT products and services, complemented by a European, commercially-oriented, voluntary and lightweight **labelling scheme**.
- Promoting **privacy-respecting approaches to cybersecurity within ICT standards** and promoting measures to accelerate their development and adoption.

A clear and common interpretation of 'national security' within the EU is a prerequisite here. Also, as the ITU has pointed out, the adoption of international trade agreements represents a potential barrier: it has to be made clear that restrictions on transborder data flows imposed to protect personal data shall not be regarded as 'non-tariff barriers' to trade.[38]

[36] See European Cyber Security Organisation (ECSO), www.ecs-org.eu
[37] European Commission (2016)
[38] Maintaining Trust in a Digital Connected Society, GSR-16 Discussion Paper. ITU, 2016.

6.3 Facilitate multi-stakeholder dialogues

Recommendation 3: DigEnlight should seek dialogue with relevant organisations on the ethical dimensions for digital security and privacy, focusing in particular on cross-cultural issues. This dialogue could be based on GCIG's proposal for a Social Compact for Digital Privacy and Security and should lay out a proposal for a set of rules to support designers and developers to deliver ethics-aware services and products.

In an area as complex as online security and privacy a multi-stakeholder approach is crucial. The various stakeholder groups inevitably have different perspectives on these issues and this presents an immediate obstacle to productive multi-stakeholder discussion.

Issues such as Internet governance, the development of ethical frameworks and guidelines, the role of legislation and enforcement, the promotion of data traceability and accountability, and the development of a research and innovation agenda all call for input from a wide range of stakeholder groups. Businesses, governments, civil society organisations and individuals each have their reasons for participating online, attribute different goals and success criteria, and make different ethical calculations as a result.

Often efforts are made to reach ethical conclusions through false opposition. For example, it might be argued that: "This is a matter of drawing the balance between individual privacy and national security interests", rather than trying to optimise for both, or to arrive at optimised relationships of interests/power.

These multi-stakeholder issues increase in complexity when one takes a global view of the digital environment without regard for national and cultural boundaries. Is it either desirable or achievable to aim for ethical guidelines that can be applied globally while at the same time respect differences between regional/national cultures, social aspirations and individual morals? Is this, as one commentator has asked, the twenty-first century version of the debate over moral absolutism and moral relativism?[39]

There are many examples of such cross-context issues: i.e. where data crosses contextual boundaries between industry sectors, application contexts, or domains of personal interaction. Similar issues arise if we consider data disclosure according to a number of criteria: active versus passive disclosure; disclosure with a direct, returned benefit versus asymmetric (or no) benefit; etc. The general problem is that of finding the appropriate mixture of technical, policy, regulatory

[39] Wilton (2014)

and procedural measures to achieve the best (i.e. most ethical) result. Here, too, dialogues are needed.

The playing field in digital security and privacy is inherently inter- and multi-disciplinary. We need shared conceptual frameworks that reflect technological, social, ethical and legal perspectives. This approach has proved successful in the identity and privacy domain and extending existing models to cover ethics would be a valuable exercise. We should continue to draw on Europe's long tradition of constructive technology assessment, based on dialogue between multiple stakeholders, so as to ensure that we talk *to* citizens and not *about* them.

The Global Commission on Internet Governance (GCIG), a multi-stakeholder group, has called on the global community to build a new social compact with the goal of restoring trust and enhancing confidence in the Internet.[40] This compact, it argues, "must be built on a shared commitment by all stakeholders in developed and less-developed countries to take concrete action in their own jurisdictions to build trust and confidence in the Internet. A commitment to the concept of collaborative security and to privacy must replace lengthy and over-politicized negotiations and conferences."

The DigEnlight fully endorses the GCIG's approach and commits to supporting it through the Forum's own channels and networks. In particular, it will seek to develop principles to support designers and developers to deliver ethics-aware services and products. DigEnlight has been multidisciplinary from the outset and its debates attempt to contribute to ongoing multi-stakeholder dialogues.

6.4 Promote ethical digital business models

Recommendation 4: Industry should adopt a shared ethics framework for online data security and privacy within digital business models, including principles of responsibility, accountability and traceability, through self-regulation. The EU and Member States should encourage these approaches and complement them by appropriate regulation if and as needed.

For ethical principles to take hold they must be embedded into the business models of both commercial businesses and government agencies (including NSAs). This means developing a wide range of tools, from guidelines and codes of conduct, to corporate mechanisms and policies that make systems more transparent and accountable.

[40] GCIG (2016)

Guidelines and codes of conduct can be useful in translating principles into day-to-day business practice. Examples include the video games industry and, more recently, initiatives by European cloud suppliers. Experience shows the value of an iterative approach: experimental guidelines framing early interactions between technologists and users, which in turn leads to robust and practical guidelines as solutions come to market.

Two principles that are likely to feature prominently are traceability and accountability. Data traceability – enabling people to find out what information is available and how it is derived – will help users to feel more empowered. We need to enforce data traceability in big data, by finding new ways to hold data controllers to account. This includes principles such as transferable consent, where data is only able to be bought and used if its previous origin and purpose are known and consent is explicitly transferred.

For traceability to work, new accountability mechanisms are needed at corporate level and the ethical dimension needs to be integrated into the work of data protection authorities (DPAs). All of this should be articulated in policies on data ethics by businesses and governments.

An example from the corporate world is Philips, which has established a Data Governance Review Board as a review and decision-making body for data analytics initiatives.[41] The Board reviews, approves and provides guidance on data analytics (and storage) initiatives. It is the authorised body tasked with ensuring responsible data stewardship and effective management of ethical and legal risk for data initiatives. The company has also adopted the Philips Data Analytics Code of Conduct to promote good practice and deter wrongdoing. This vigilance extends across the supply chain, where the company undertakes due diligence and ensures appropriate governance and liability arrangements are in place.

With a longer term perspective, business will need to respond to and support the shift towards human-centred personal data management and processing. This means working alongside regulators, citizens and civil society organisations in the development of i) personal data stores with data security built-in and ii) near real-time audit frameworks for the transactions that are undertaken. The systems that emerge will entail a balance between personal data stored with providers (low acceptance threshold) and data stored centrally with the users (ecosystems).

The challenge here has a strong practical orientation and holds significant potential. Building on its established networks, DigEnlight should collate and spread best practice on relevant approaches and frameworks and lead the debate on their future development.

[41] Trusted Data Management in Health Care, DigEnlight Conference Report, Jun 2016

6.5 Raise awareness and mobilise citizens

Recommendation 5: Industry and Governments should cooperate to systematically promote EU-wide awareness of the exploding business value of personal data as well as privacy rights and security risks online and mobilise citizens in the search for acceptable, ethics consistent solutions. DigEnlight will contribute to the development of awareness and the creation of required skills.

The digital environment is still in its infancy and in our enthusiasm to embrace the opportunities of the new technologies we have lost sight of the risks. In many ways the situation reflects previous experiences: the risks from traffic accidents, smoking, and environmental pollution all took many years to be recognised and for appropriate – and proportionate – safeguards to be put in place. Cyber risks are, arguably, more challenging because digital technologies are growing faster and their reach is global. We have to mobilise citizens and make them part of the search for acceptable, ethically-based solutions.

At the most basic level, we need to raise awareness of the potential risks and disbenefits of online activities. What gets rewarded gets repeated. But habitual behaviour is not necessarily ethical behaviour and increasingly we are being encouraged to develop behaviours that could potentially cause us harm. Ethical dilution means that often users do not know what the costs/risks are nor even understand that there are costs/risks at all, and so are unable to make an informed choice. We need to consider how we reinforce and encourage ethical habits online.

Governments should be encouraged to allocate funding for education about the value of privacy and the risks posed by surveillance, identity theft and fraud. Campaigns should also raise awareness of means of increasing personal privacy protection, including support for privacy-enhancing technologies such as privacy-by-design.

The use of open technologies (including open hardware) – which are tried, reviewed and reported on by open communities – should also be encouraged. Certification and labelling by trusted parties can help people to modify their behaviour. And incentives (similar to those provided for green energy) by governments might be an extra support.

Citizen empowerment can also be addressed through other means – such as ethical IT innovation, business models that emphasize accountability and traceability, and smart regulation – which are the subject of separate Recommendations here.

Again, DigEnlight can play a role through its networks by helping to ensure citizens are represented in the debate and promoting exchanges of best practices between stakeholders, including NGOs, civil society organisations and policy-makers.

6.6 Develop a multidisciplinary research and innovation agenda for a human digital world

Recommendation 6: Develop a multidisciplinary research and innovation agenda for a sustainable, ethical and human-centred digital world with attention to mastering complex techno-socio-economic systems and the effects of ever more data, processing power and connectivity.

Research and innovation have crucial contributions to make to the effects of the fast technological developments in a global world with more data, processing power and connectivity. The automation of society leads to unprecedented complexity problems, which our current scientific knowledge is insufficient to deal with adequately, let alone master. Multidisciplinary research, involving experts from science and technology, sociology, law, politics and ethics can show the way towards rebalancing the asymmetry in power between those who have the data and those who provide or even constitute the data. We have to find innovative ways for enabling a participatory democracy for our digital world. Value-based approaches, such as the digitally assisted self-organisation that has been proposed by Helbing,[42] need further study and development to help provide new solutions based on ethical principles and approaches.

DigEnlight proposes to direct its energy and resources to stimulate such multi-disciplinary research aimed at addressing the hard core problems of the digital revolution, towards a secure and humane future society, based on ethics and democracy. The tasks are multi-dimensional. They include:

- Re-architecting the Internet infrastructure for a participatory democracy in a global context.
- Understanding the development of complexity in our world based on techno-socio-economic systems and finding ways of mastering complexity to the benefit of creating a sustainable, humane society.
- Developing a trusted environment for individuals based on digitally assisted, ethically responsible self-organisation.

[42] Helbing (2015)

- Understanding information cultures and the role of ethics globally.
- *Future-proofing policies, technologies and systems* for the enormous challenges arising from Big Data, the Internet of Things, greater processing power and more connectivity, so as to ensure a digital evolution that supports the individual in a secure and ethically responsible digital society.

It is clear that new research is needed that should not be confined to today's framework. It has to be open enough to encompass new and disruptive ideas, technologies and societal and systems architectures. Many technologies such as Internet of Things, graphene, quantum computers and spintronics are progressing very rapidly. As all of these find their way into research agendas in both the public and private sectors, we must re-establish their connection to personal and societal needs so as to ensure that the resulting products and services will support the individual and society.

6.7 Build bridges for policy cooperation

Recommendation 7: Promote the exchange of views and best practices on ethical principles and approaches both within the EU and internationally. Seek models for useful cooperation, and policy instruments and institutions to enable bridge building and common standards development.

Given the current weaknesses and overlap in Internet governance, cooperation – both within the EU and internationally – to strengthen the ethical dimension in security and privacy online is essential. Globalisation and technological advances pose common challenges to providing a progressive, sustainable model for protecting privacy in the global Internet environment. Yet too often tensions between different legal systems, such as the EU and the US, result in loss of confidence on the part of users and confusion by commercial entities.

Conciliatory, rather than confrontational, approaches are called for, recognising the differences and rights for democratic states to follow their own laws but also that common approaches are in everyone's interests. There can be no digital nirvana: this will always be a messy field but we should at least try to collaborate. The dialogues advocated under Recommendation 3 and research and innovation agendas described under Recommendation 6 will play important roles.

The United States will be a particularly important partner for the EU in this respect. Recent work by the International Privacy Conference has outlined approaches designed to advance strong privacy values in a manner that respects the

substantive and procedural differences between the two jurisdictions.[43] The IPC identifies a series of ten 'privacy bridges' that will both foster stronger transatlantic collaboration and advance privacy protection for individuals. They range from cooperation on policy development (e.g. deepening the working relationship between the EU's Article 29 Working Party and the Federal Trade Commission); through to the exchange of best practices (on issues such as de-identification of personal data and security breach notifications); harmonising regulatory approaches (in areas such as accountability and use of drones); and joint technology development (e.g. easy-to-use mechanisms for user controls and collaborative research programmes).

Further work is needed to make this type of policy cooperation a reality. Much more should be done, including by DigEnlight, to facilitate such exchanges across the full spectrum of issues addressed in this White Book.

[43] IPC (2015)

Bibliography

Brown I. (2014), *Designing Internet technologies for the public good,* The Policy and Internet blog, Oxford Internet Institute, http://blogs.oii.ox.ac.uk

Cate F.H., Cullen P., Mayer-Schönberger V. (2014), Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines.

Council of Europe (CoE) Commissioner for Human Rights (2014), *The rule of law on the Internet and in the wider digital world*, Council of Europe. www.commissioner.coe.int

Crawford K., Miltner K., Gray M.L. (2014), *Critiquing Big Data: Politics, Ethics, Epistemology: Special Section Introduction*, International Journal of Communication 8 (2014), pp. 1663–1672.

EGE (2014), Ethics of Security and Surveillance Technologies, Opinion No. 28 of The European Group on Ethics in Science and New Technologies, Luxembourg, Publications Office.

European Commission (2016), Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final

European Data Protection Supervisor (EDPS, 2015), Towards a New Digital Ethics, Opinion 4/2015.

Floridi L. (2013), *The Ethics of Information* (Oxford Univ Press)

Floridi L. (2014), *The Future of Europe is Science – and ethical foresight should be a priority.* The Policy and Internet blog, Oxford Internet Institute, http://blogs.oii.ox.ac.uk

FRA - European Union Agency for Fundamental Rights (2015), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union*, Luxembourg, Publications Office. http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

GCIG (2015), *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance*, Centre for International Governance Innovation and The Royal Institute for International Affairs. Available at: www.ourinternet.org

Helbing D. (2015), The Automation of Society is Next: How to Survive the Digital Revolution. (North Charleston, SC: Createspace)

International Privacy Conference (2015), *Privacy Bridges: EU and US privacy experts in search of transatlantic privacy solutions*, 37th International Privacy Conference Amsterdam 2015, https://privacybridges.mit.edu/

ITU (2016), Maintaining Trust in a Digital Connected Society, GSR-16 Discussion Paper, International Telecommunications Union.

Hoepman J.H. (2015), *The demise of society threatens our privacy*, DigEnlight blog post, https://digitalenlightenmentforum.com

Johnson J.A. (2014) *From open data to information justice*, in Ethics Inf Technol. DOI 10.1007/s10676-014-9351-8

Kamphorst B. (2012), *The primacy of human autonomy: understanding agent rights through the human rights framework,* Rights and Duties of Autonomous Agents, Proceedings of the 1st Workshop on Rights and Duties of Autonomous Agents. http://ceur-ws.org/Vol-885/

Korff D., *Coppers and Spooks in cyberspace: une liaison dangereuse*, on the DigEnlight blog, http://digitalenlightenmentforum.com

Millar L. (2015), *The post-digital social contract (part 2 of 3)*. DigEnlight blog post, https://digitalenlightenmentforum.com

Poikola A., Kuikkaniemi K., Honko H., MyData - A Nordic Model for human-centered personal data management and processing www.lvm.fi

Preneel B, Rogaway P., Ryan M.D., Ryan P.Y.A (eds.) (2014), Privacy and Security in an Age of Surveillance, *Dagstuhl Manifestos*, Vol. 5, Issue 1, pp. 25–37

Riguidel M., Bus J. (2015), *Digital ethics,* DigEnlight blog post, https://digitalenlightenmentforum.com

Spiekermann S (2015), *Ethical IT Innovation: A Value-Based System Design Approach*, Auerbach Publications. ISBN 9781482226355

Wilton R. (2014), Four Ethical Issues in Online Trust: Topics for a moderated workshop, CREDS 2014 – Position Paper, CREDS-PP-2.0

Wilton R. (2015), Can a Machine Care About Privacy, Tech Matters blog post, www.Internetsociety.org/blog/tech-matters

Wilton R. (2016), Thoughts from the Ethical Data-handling Panel at CPDP2016, Public Policy blog post, www.Internetsociety.org/blog/public-policy

DigEnlight Publications and Reports

All available at http://digitalenlightenment.org

Digital Enlightenment Forum Yearbook 2013: The Value of Personal Data

Digital Enlightenment Forum Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment

DigEnlight Forum 2015 (25-26 March, Kilkenny, IRL): The Citizen – Negotiating Life in the Digital World.

Security, Surveillance and Civil Liberties in Cyberspace (Brussels, 13 Nov 2015). DigEnlight Workshop Report

The Future of the Internet of Things (Brussels, 26 Nov 2015). DigEnlight Conference Report

Digital Ethics (Brussels, 1 Mar 2016). DigEnlight Workshop Report

Trusted Data Management in Health Care (Amsterdam, 7 Jun 2016). DigEnlight Conference Report.