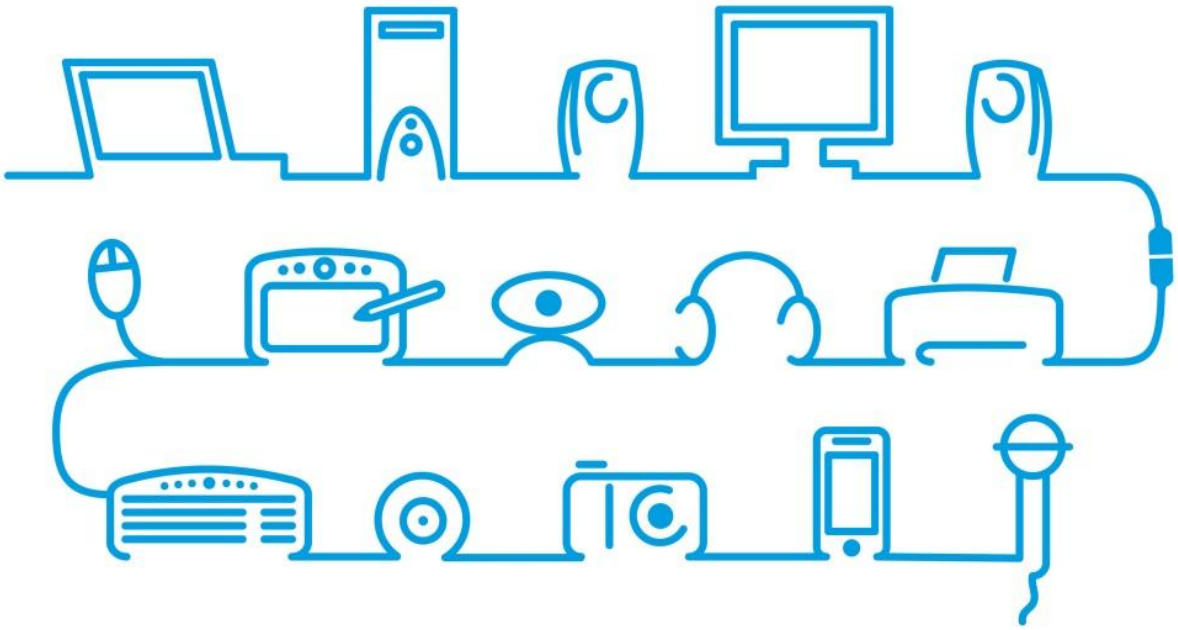
TO L0G OR NOT TO L0G?



Risks and benefits of emerging life-logging applications

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is a European Union (EU) agency which acts as a centre of expertise for the EU Member States and European institutions. It gives advice and recommendations on good practice, and acts as a "switchboard" for exchanging knowledge and information. The agency also facilitates contacts between the European institutions, the Member States, and private business and industry.

Contact details

The report has been edited by Barbara Daskala.

For questions related to this study or to the Emerging Risks Framework, please use the following details:

e-mail: RiskManagement@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

LIST OF EXPERTS AND CONTRIBUTORS

This report was produced by the ENISA editor using input and comments from a group selected for their expertise in the subject area and in the areas of assessment (security, privacy, social, legal) including industry and academic experts. It should be noted that group members participate as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and individual group members may not agree with all of the observations and recommendations made in the report.

The contributors are listed below in alphabetical order:

Ioannis Askoxylakis, Foundation for Research and Technology (FORTH), Greece

Ian Brown, Oxford Internet Institute, UK

Peter Dickman, Google Switzerland

Michael Friedewald, ISI, Fraunhofer Institute for Systems and Innovation Research (Fraunhofer ISI), Germany

Kristina Irion, Central European University, Hungary

Eleni Kosta, KU Leuven, Belgium

Marc Langheinrich, University of Lugano (USI), Switzerland

Paul McCarthy, Lancaster University, UK

David Osimo, Tech4i2, Belgium

Sotiris Papiotis, Ernst & Young Advisory Services, Greece[1]

Aljosa Pasic, ATOS, Spain

Milan Petkovic, Eindhoven University of Technology & Philips Research, The Netherlands

Blaine Price, Open University, UK

Sarah Spiekermann, Vienna University of Economics and Business, Austria

David Wright, Trilateral Research & Consulting LLP, UK

[1] Assisted in the implementation of the technical risk assessment procedure.

ACKNOWLEDGEMENTS

We would also like to acknowledge the following for their useful input at certain phases of our work:

Rosa Barceló, European Data Protection Supervisor, Brussels

Danah Boyd, Social Media Researcher at Microsoft Research New England, Fellow at Harvard University's Berkman Center for Internet and Society, US

Serge Gutwirth, Vrije Universiteit Brussel (VUB), Belgium

Nicola Jentzsch, DIW Berlin, Germany

Gwendal LeGrand, Commission Nationale de l'Informatique et des Libertés (CNIL), France

EXECUTIVE SUMMARY

ENISA undertook the task of developing a scenario identifying the risks, threats and vulnerabilities particularly regarding privacy and trust issues of a set of technologies grouped around the trend known as 'Life-logging'. This was done under the broader remit of ENISA's role in assessing new and emerging technologies[2].

Life-logging is not a new concept: however, the way we do it, is…

Recording aspects of one's life, or life-logging, has a long established history in human society, but it is undergoing transformational change in terms of depth, volume and type of data. Before the 20th century, life-logging was restricted to recordings on paper media and involved written accounts, such as books, diaries, or collections of letters between people as well as person-constructed images such as drawings or paintings. By the 20th century, the media had broadened to include still photographic images, sound and moving images and most families kept at least an image life-log in the form of a photo album. By the end of the 20th century, most of these life-log data were digitally recorded with both the resolution and frequency of recording dramatically increasing year on year. Paper diaries and letters gave way to blogs, e-mail, and social networking status updates with the significant difference that the latter were potentially recorded forever and with a vastly more complete history than the episodic fragments of days gone by.

Information security related risks may have serious connotations on privacy, economy and society, or even on people's psychology…

It is has become quite a profitable market and it is increasingly popular among citizens alongside social networking applications, in some cases also used by the governments. It has also started to gather much attention from analysts, considering various aspects of its development. It thus presented an interesting case for ENISA to explore how information security related risks regarding the life-logging environment actually have serious connotations on privacy, economy and society, or even on people's psychology. Our analysis goes to show how all these aspects are highly interrelated, and should be examined together. The approach we used, as in other similar ENISA studies, was adapted according to the nature of the assessment, aiming at an informative analysis, considering as many aspects as possible (e.g. privacy, social, legal, economic, etc.), and identify risks for all three stakeholder groups (individuals, industry, state / government) and making recommendations based on the risk assessment results. At ENISA we think that it is precisely through this knowledge and understanding that we could be better prepared to mitigate the risks and maximise the benefits of these technologies.

[2] The scenario and topic of life-logging was selected by ENISA based on various topic proposals received from external stakeholders and experts in early 2010.

SUMMARY OF THE SCENARIO

The scenario can briefly be summarised a day in the life of a family, 3-5 years from now, with 2 adults (Annika and Bennie), 2 young people (Christer and Dana) who to greater and lesser degrees make use of different life-logging and related services during the course of their respective daily routines. It captures all four and other individuals interacting with them in a variety of settings performing a number of everyday activities, including work, commuting, being at school and relaxing at home. During the course of their daily activities all of them also come into contact with other individuals, commercial providers as well as government agencies. In these various interactions as well as through the activities of the family, it is clear that life-logging is embedded within their daily routines and through illustrating these, the scenario illuminates the wide variety of risks that this report considers.

TOP BENEFITS

The following benefits have been identified per stakeholder.

Individuals

Individuals can benefit from life-logging, both on a personal level and on a societal level. Life-logging can bring families and friends closer and for a longer period of time, thus **reducing individuals' sense of isolation** and enhancing the **building of social bonds** among people and **enhance communication**.

Individuals can also be more aware of their colleagues' and professional contacts' activities, which may make it easier to contact the right people from their networks when they need advice on a specific problem; they can also **benefit professionally by building their reputation online**, e.g. getting a better job etc. (consider for example the existing case of many artists and other individuals, that got a job through exposing their work in social networking sites, such as YouTube, LinkedIn etc.)

Life-logging offers the advantage that it **occurs automatically**; it offers a continuous stream of data compared to occasional bursts of information that one keys into a social network. Finally, the ability to automatically and effortlessly log a huge range of data about one's daily life, combined with the right tools to analyse the data, could allow people to better understand why certain things happen (e.g. sleeping patterns correlated with noise/light levels).

Commercial and economic interests

The data generated by individuals will underpin new business and charging models. For example, commercial real estate may be valued against the background of real consumer flows or traffic in front of a building. In addition, the decreasing cost of sensor and storage technologies provides commercial opportunities for companies to embed or **combine life-logging services in almost any product or "thing"**, ranging from personal items such as clothes to public infrastructure elements, such as traffic signs or buildings. Data generated by "life-logging services" will contribute to higher degree of context-

awareness and **personalisation of services**, which in its turn, would mean **competitive advantage** for those who have control over this data.

State / government and society

Generally speaking, existence of large sets of data and access to this data would improve understanding of different actions, relationship, causes etc. One of the main uses is therefore **decision support** and there are many ways that government and society can profit from it. For example, access to the health related life-logging data of groups across a country could help medical investigations or help national health infrastructure promotion campaigns as well as get early warnings of disease outbreaks.

Moreover, we are already experiencing the impact of social networking and social media on the public affairs; life-logging activities can potentially provide to governments some good **indications of public opinion** and to a certain extent **influence policy-making**, since they can be an additional source of citizens' input to various political issues.

TOP RISKS

Given the scope of the activities, services and devices that are depicted in this scenario on life-logging it is unsurprising that the report identifies a broad and large number of possible risks. We have selected some of the key risks identified in the report and summarised them here, grouped per stakeholder that the risk primarily affects. We see these as very important and ones which we follow by suggesting a number of top recommendations.

Individuals

The top risk for individuals utilising life-logging devices and scenarios is **the threat to privacy** [**R2**] that accompany using them. **Loss of control over this data** [**R8**] might result in individuals being subjected to **financial fraud** or unauthorised access might result in reputational harm or discrimination and exclusion [**R5**]. This risk is compounded by the nature of life-logging in that apart from privacy threat to individuals coming from commercial entities and governmental agencies, there is also a **threat of deliberate or accidental data collection** about one person by other individuals.

Dependency on the availability of certain devices or services is also increasing the risks for individuals, as the mobile devices, sensors or services become more attractive targets for attackers. In this direction, it is particularly important the link between tangible and intangible assets, as we can also see in Future Internet scenarios; a related risk is the **loss of autonomy**.

Finally, we should consider risks such as **psychological damage**, related to discrimination, exclusion, harassing, cyberstalking, child grooming, feeling of being continuously under surveillance (paranoid behaviour), pressures related to work performance, peering into other peoples life etc.

Commercial and economic Interests

The top risk for commercial and economic interests is likewise related to the failure of the companies to comply with data protection and privacy regulations (especially of social networking providers) [**R4**]. The risk is not solely about possible **sanctions** (financial or other forms) that might be imposed but also a **loss of trust and decrease of reputation** in the face of the multitude of things that can go wrong when data is compromised, lost, stolen or erroneous.

There are specific risks related to legal issues, from the ambiguity of certain regulatory requirements to the **incoherence and fragmentations of national legislations** that apply in this scenario. In addition, the life-logging scenario exemplifies a situation where multiple data controllers and data processors might be involved to that the roles and responsibilities, as well as risk allocation are not clearly defined.

State/ government and society

The top risk for government is **not ensuring a balanced regulatory environment** which guarantees fundamental rights and protects citizens and society, while at the same time does not constrain or have negative consequences on the growth and competitiveness of European industry [**R4** , **R11**]. While a regulatory lag is often present in relation to the development of new technologies and services, life-logging presents **particular risks due to the pervasiveness of data collection** and the **persistence of data in various forms**. Risk of **abuse of information** is inherent both to private and public sector, however in the case of government (e.g. data manipulation in statistics), issues that are at risk are even more important (e.g. liberty, dignity).

Since data storage or processing is often done outside of national borders, there is a risk **of legal gaps or a loss of sovereignty**, as well potential conflicts as a consequence of incoherence in legislations or legal gaps. This "delocalisation" has also economic consequences for a state, in addition to other economic risks, such as a **loss of productivity due to excessive life-logging.**

Creation of "market dynamics loop" where the consent on providing additional personal data is needed for better service experience poses an obvious risk on societal norms. There is an additional risk that **society will accept these "default behaviours"** even when no service improvement is involved (e.g. postcode or boarding pass are frequently requested at cash desks). Commoditisation of such information is shifting borders of what is considered acceptable and in which context.

Finally, there is **a risk of erosion of social values and change of behaviour norms**: for example, individuals deliberately placing online personal data of another person (or refusing to erase it afterwards).

TOP RECOMMENDATIONS

Addressing the risks identified is neither a one-way street nor something which is associated with only one category of stakeholder within a life-logging environment. This report makes a number of recommendations; here we present the top ones per stakeholder that they are addressed to.

Individuals

We believe that **an informed user is the first step: the right to be forgotten, right to be let alone etc, are probably best enforced if the user is in control over his/her personal data**. Specifically, we recommend that individuals:

- although the industry and the state /government and EU institutions have the most important role to play in this, **be alert for protecting their own privacy** (for example by making use of available tools) **and be aware of** the potential impacts on others, accidentally or deliberately affected by their own use of these services, as well as the impacts on themselves by the use of such services by others.

- **make use of privacy friendly tools** and consider factors and variables that reflect the trade-offs they have to make between the benefits (e.g. gain of comfort, increased functionality, discounts) and risks (e.g. mistrust, disadvantages, risk of misuse or manipulation).

Life-logging industry and service providers

ENISA recommends that industry and service providers:

- design life-logging services with privacy-friendly default configurations and settings, intelligible to a wide range of customers.

- perform impact assessments and use risk management approaches with regard to privacy and information security, so as to be better prepared.

- provide direct online access to users, showing them when and with whom data is being shared, including an audit trail of accesses, and to explain decisions being made using data elements

- make individuals aware of and control the privacy risks associated with use of life-logging services

- use of encryption for data stored on user devices (e.g. smart phones), as well as use stronger multiple factor authentication mechanisms where available, i.e. two or three-factor authentication methods.

- should consider following a distributed model of data storage, allowing users to store and process their data on their own equipment, with strict access controls, and the provision of interoperable services by separate companies rather than integrated large-scale data processors

- need to obtain and consider detailed information about the functionality and configuration options of the life-logging tools they provide to employees, with a view to balance the need to use life-logging applications with productivity issues.

State / government, EU Institutions and regulators

It is recommended that:

- The European Commission utilise the consultation on revisions to the data protection directive as a mechanism to anticipate the regulatory frameworks required as a result of increasing use of life-logging devices and services. We believe that the risks identified in this report, as well as the recommendations, **can inform on-going discussions** as to what changes to the data protection directive can anticipate the technologies and services described herein.

- Governments and other statutory agencies seek to create a **regulatory environment that provides incentives for privacy-aware or privacy friendly devices** and services while supporting competition through promotion of interoperability and interconnection between devices, services as well as providers.

- the approach of **privacy and information security impact assessment** and **risk management** should be also followed by the public sector, which should promote it and also develop generic frameworks that could assist the industry towards this direction.

- state/governments as well as EU institutions should focus on making people aware both of the benefits and of the risks of using the life-logging services; more importantly, they should also aim to **educate the individuals** of the risks and ways to protect them (e.g. the inclusion of privacy training in computer science education).

- **Competition regulators** consider privacy issues in their broader work to ensure competitive marketplaces.

- **the EU and its member states** strive for regional agreements that would apply throughout the European Union, therefore consolidating and harmonising to the best possible extent the compliant treatment of life-logging data.

- **state/ governments** consider introducing real sanctions for personal data breaches.

- **regulators** in general create **strong incentives** for companies to include user interface "nudges" towards safer behaviour by customers, as well as to consider privacy requirements in early stages of product development.

RESIDUAL RISKS

Utilising a very important risk management concept, that of "residual risk", i.e. the risk that will remain after the implementation of the controls, we have identified certain risk areas that we consider will not be fully mitigated by the proposed recommendations; this may come to pass either because the risk cannot be fully mitigated, or because by addressing this risk, other risks may surface, and would thus require further analysis.

Those risk areas regard encryption, architectures (large scale and centralised systems versus small scale and distributed with external access to data repositories), informed consent implementation challenges, as well as maintaining open-ness in applications and data sharing while respecting and safeguarding individuals' privacy rights.

CONTENTS

1 INTRODUCTION

In the context of ENISA's Work Package 3.1 "*Identifying emerging and future risks for creating trust and confidence*"[3] and in continuation of last year's work[4], we have launched a scenario assessment based on a selection process, focusing on privacy and trust issues of life-logging and continuous instant activity sharing (e.g. nano-feeds, life-tracks).

While the term 'Life-logging' might be new, the practices and activities it represents are well-known, well established and pervasive historically and currently in societies. The keeping of a diary, the writing of a biography or autobiography, personal accounts of historical moments (sporting, war) and news stories capturing moments of celebrities' lives can all be represented in life-logging. Before the 20th century, life-logging was restricted to recordings on paper media and involved written accounts, such as books, diaries, or collections of letters between people as well as person-constructed images such as drawings or paintings. By the end of the 20th century, most of these life-log data were digitally recorded with both the resolution and frequency of recording dramatically increasing year on year; the media had broadened to include still photographic images, sound and moving images and most families kept at least an image life-log in the form of a photo album. Other life-log data types, such as performance results in a sporting event or medical history related data were recorded for very small numbers of people, but the main life-log data for most was the photograph at infrequent intervals.

That the public has an interest in these is central to the appeal and the risks inherent for individuals and society in the expanding use of life-logging devices and services. Indeed in most of the world, these media forms dominate sales and continue to be a profitable market in an age of declining sales for other traditional print media. Some self-narratives are also important cultural and historical documents, such as the Diary of Anne Frank. Other sources of historical accounts are also important as are the growing phenomena of individuals, present at newsworthy current events, recording, transmitting, sharing a persistent digital account of events.

The development of new ICT technologies, the internet and the explosion in terms of popularity of new forms of social media have transformed these activities. They have allowed for individuals to create their own content (Web 2.0 and other technologies) and expanded dramatically the range and number of who we can tell our stories to (or who can know our stories without us even knowing them). Diaries have become blogs, biographies have become Facebook pages and digitalisation and the proliferation of inexpensive portable video and photo capture devices have revolutionised where

[3] You can access the complete ENISA Work Programme at www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010

[4] See the 2010 ENISA study on an Internet of Things / RFID air travel scenario, available at www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2.

we can record, what we can record and how it can be shared with others. While there are legitimate questions often about the quality of this new content (in terms of depth and details) there is little doubt over the quantity of such content now existing in cyberspace.

1.1 MOTIVATION, SCOPE AND OBJECTIVES OF THE STUDY

Based on the above, a scenario was created to illustrate potential risks posed by new life-logging and social networking services, affecting citizens, the private and public sector, but at the same time to explore potential benefits. What risks are raised by these new life-logging services when people are intentionally sharing lots of personal information? There may be security and privacy issues, risks to the individuals, but are there risks to any other stakeholders? Would it be possible for a malicious user or an attacker, to glean personal information uploaded by individuals that could be used as a way to hack into or attack a company or government department or a network?[5]

How is our conceptualisation of privacy and trust affected by (a) individuals who intentionally share personal information on the Internet, (b) companies, such as social network providers, which may intentionally repurpose users' personal data (possibly due to insufficient or not user-friendly information provided to the users during sign-up or inadequate consent mechanisms) and/or encourage users to "share" their data (often using trivial inducements as supermarkets have done with loyalty cards), and (c) the state, who might be using such services to get more information on citizens and to enable better profiling?

Clearly, there are many aspects to be considered vis-à-vis the expected development of such technologies and applications. This study aims to provide an informative analysis, considering as many aspects as possible, and identify risks for all three stakeholder groups. The study highlights the benefits of such services, and offers recommendations to address the risks and challenges identified.

1.2 SUMMARY OF THE SCENARIO

The scenario presented in this report represents the next step in the evolution (or revolution) in technologies enabling and supporting these human activities. It has some common characteristics with previous scenarios developed by ENISA, such as Flying 2.0[6], which also included technologies seamlessly integrated into human living and working environments. Where it diverges from these is the emphasis, demonstrated in the flow of the scenario, of the range of potential human activities,

[5] Langheinrich, M., and Karjoth, G., 'Social Networking and the Risk to Companies and Institutions', *Information Security Technical Report, Special Issue: Identity Reconstruction and Theft*, Vol. 15, Elsevier, 2011, pp. 51–56.

[6] Daskala, B. (ed.), *Flying 2.0 – Enabling automated air travel by identifying and addressing the challenges of IoT/RFID technology*, European Network and Information Security Agency (ENISA), 2010.

locations, relationships as well as types of devices, network infrastructures, storage and interfaces that are potentially brought into play.

The scenario can briefly be summarised as a day in the life of a family, 2 adults (Annika and Bennie), 2 young people (Christer and Dana) who to greater and lesser degrees make use of different Life-logging and related services during the course of their respective daily routines. These are familiar to them and are integrated into their routines and daily activities.

The scenario takes place over the course of a day, and captures all four and other individuals interacting with them in a variety of settings performing a number of everyday activities, including work, commuting, being at school and relaxing at home. All four might appear to be technologically savvy but a feature of the scenario is the assumption that interfaces have developed in such a manner as to make many of the technologies unobtrusive and easy to use. As such they represent a typical family for the timeframe considered in the scenario.

The scenario also depicts the benefits expected to flow from the use of proliferation of life-logging devices as well as the drawbacks. During the course of their daily activities all four individuals also come into contact with other individuals, commercial providers as well as government agencies. In these various interactions as well as through the activities of the family it is clear that life-logging is embedded within their daily routines and through illustrating these the scenario illuminates the wide variety of risks that this report considers.

1.3 STRUCTURE OF THE REPORT

ENISA convened a group of independent experts to develop and analyse a scenario, part of which is presented in **Chapter 2** of this report. Once the scenario was reasonably stable (it went through several iterations), the group then analysed it using ENISA's methodology, which is presented in detail in **Chapter 4**, in particular to identify and assess the assets, vulnerabilities, threats and finally the risks in the life-logging scenario: all these results are presented in **Chapter 5** of the report. The benefits of life-logging technologies were also identified in parallel, and those are discussed in **Chapter 3**. Based on the analysis and the risks identified, the group came up with some remedial actions to mitigate the risks; these recommendations are presented in **Chapter 6**. Finally, in order to provide for a more complete picture of the issues identified and for a more holistic analysis, in **Chapter 7**, some residual risks are highlighted, namely more ambiguous areas which we considered may not be fully addressed by the recommendations and which may merit from further consideration.

2 CAUTIONARY TALE

This section presents the scenario, the cautionary tale, based on the somewhat longer scenario script, which you may find in Appendix I. The scenario is the foundation on which everything else is built.

The cautionary tales are in two parts. The text in the right-hand column presents a streamlined scenario script, while the left-hand column provides some commentary, notably on possible risks arising from the actions taking place in the scenario script. Also in the left-hand column, the potential risks are indicated, with direct reference to the specific risks identified in section 5.3 of this report.

Annika, a professional mum, and Bennie, a self-employed dad, live together with their 12-year old son Christer and their 14-year old daughter Dana in Malmö, Sweden.

Morning at home

Automatic life-logging combined with social networks can unobtrusively "connect" people and their activities, providing shared virtual experiences. They can also offer playful motivations for healthier living.

As the alarm goes off in the morning, Bennie grudgingly makes his way into the bathroom. The smart mirror that also allows his son Christer to play his favourite "Brushy" game (in which he competes with his friends on who brushes the teeth best) detects his composure using image recognition and gets ready to auto-blog his ritual "morning riser" message to his social network. A glance to his "friend stream", which is projected to the side of the bathroom mirror, shows him that Dan, his best friend, is also already up – though his night must have been short: Dan's icons say "grumpy" and his message is "Don't Ask!"

Annika detects a change in Dana's behaviour which somehow is related to or reflected in the latter's not posting status updates on her life-logging system, which makes her suspicious [R6 R7]

When Bennie comes downstairs, Dana and Annika are already at the breakfast table, seemingly in a heated discussion. "She hasn't posted any status updates for more than two weeks now," Annika says to Bennie. "There must be some reason, I'm sure, but she won't tell me." Dana quickly mumbles "I have to get ready for school" and slips upstairs. "Bennie, I'm also worried about her working late at Krista's house so often, supposedly on some school project. How do we know she is actually there working and not going out or something?" "Relax Annika, I remember checking her life-log last week and she was definitely at Krista's all of these days," Bennie replies.

Bennie accessed his daughter's location data to check her whereabouts: how about Dana's privacy? [R1

Dana exchanges some of her privacy in order to have more freedom to go out on her own [R1

"But how do you know she didn't just leave her phone behind at Krista's and go out the whole night?" Annika retorts. A good point indeed, Bennie must admit to himself. "Hmm, I guess you're right. A few days ago, I would have said there's no way that Dana would move more than a few meters away from her phone, not being able to update her social network on her activities minute by minute. She would have sooner walked out of the house naked than without her phone! But if she stopped her updates as well…" Earlier that year, Dana agreed that she would give her parents access to her location data in exchange for having more freedom to go out on her own. As Dana reappears a few minutes later with her school bag in hand, Bennie quickly finishes his coffee and offers to walk with her to the bus stop.

Travel to work/school

Infatuated with Freia, Christer has been "stalking" her [R4 . In this case, it is innocent. In other cases, use of a social network may not be so. There's also a risk here since Freia, like many other users, didn't change the default settings of the social networking app [R1].

Meanwhile, son Christer is munching on his cereal and scanning his friendship streams. Suddenly his mood rises rapidly: it seems that Freia is taking the bus today! Her avatar is currently aboard the 983 from Staffanstorp! This is his chance to "accidentally" meet her on the bus! Since Christer had been keeping tabs on Freia for a few weeks now, he knows that her parents usually drive her to school. While they aren't friends yet and thus Christer shouldn't know her location, it turns out that Freia didn't yet change the default settings in their school's social networking app! Christer simply befriended Gitte, one of Freia's friends, in order to get access to all of Freia's details, too!

Annika benefits from a networked system that saves her wasting time in a traffic jam.

Annika faces a risk in giving her service provider access to her whereabouts [R1 R2]. While the opt-out option exists, her choices are limited – opting-out would cost her 39 kronor per month, which she is not prepared to pay [R11]

Annika does not know what data is being uploaded

Annika starts her drive into town, however, her mobile phone provider sends a traffic alert to her car's navigation system: Seems as if there are a lot of non-moving phones up on the Sallerupsvägen onramp. "Probably an accident," she thinks as she accepts the alternative route suggestion. As she prepares to turn at the next signal, her new route plan is automatically shared with her mobile phone provider, which uses this information to improve its already excellent traffic forecasting system. Usage is free for Annika, as long as she agrees to share all of her travel information. She could, of course, opt out at any time, though she always felt that paying 39 kronor per month for this was a bit steep. While Annika is driving down Toftanäsvägen, her car monitoring systems detects first signs of wear and tear in the two front brakes and makes an entry on the myCar diary that Annika signed up for in order to keep up with the car's maintenance. It supposedly also helps with selling the car later, Annika had been told, as prospective buyers could get a first-hand impression on how the car was handled by the previous owner. Annika usually never bothers to check that diary, and has set the car to never bother her with what information it is uploading. However, as Annika enabled the "CareFreeCar" app inside her diary, any safety-relevant entries are directly copied through to her preferred

about her car [R8 , R7]	garage, allowing it to contact Annika for scheduling a check-up.
Peer-group pressure (or aspirations) can lead to risks [R7 R8], e.g., grooming or malicious attacks [R3 R6], although we don't know that it happens here	As Dana is walking to the bus stop with her dad, she decides not to tell him about Leif having invited her to join a peer-to-peer social darknet, where she's been doing all her postings. She's still quite psyched about that invitation: Leif's already 16 and has a motorcycle! Plus: being in a decentralised and thus unregulated network means completely different kinds of postings. No parents or teachers watching!!
Posting some personal data or preferences can lead to victimisation or psychological harm or discrimination from one's peers [R5 R9 R7]	As she puts on her headphones, she consciously disables the music sharing feature on her MP3 player. She can't imagine what would happen if her ABBA playlist would find its way into her online music profile! She still remembers when her friend Marit's profile had suddenly shown the complete Pippi Longstocking episodes as her favourite "songs"! Some of her friends still have her listed as "Marit Longstocking" in their Instant Messengers. Poor Marit!
Bennie faces the risk that his private information, including that of his home, will be misappropriated [R2]. ***In some instances, life-logging offers benefits to the whole community.*** ***Bennie's personal data is "shared" or distributed with others. The repurposing of data can hold risks when it is used for purposes other than originally specified [R1 R2]***	While Bennie enjoys seeing the occasional update from his friends, he hardly bothers to manually post anything himself. Though with all the auto-posting scripts embedded in many of his devices and appliances, there's still plenty of updating going on, as far as he is concerned. Take, for example, his bike. As Bennie is cycling to a first meeting with a new client, he relies on his mobile phone to direct him (using voice commands through his wireless headset). He is part of the CycleMalmö online community. Its members can mount a small sensor module directly on their bicycles and thus update city-wide pollution and traffic maps in real-time. In turn, they get to use CycleMalmö's own navigation service that takes both traffic situations (including bike lanes!) and air quality into account. As Bennie has asthma, he also always wears a small sensor patch under his shirt that correlates his bike's air quality measurements with a number of his vital signs, and records this in his HealthStore profile at his local health county council. This way, he and his doctor can inspect his health record periodically to better understand both short-term and long-term irregularities. The aggregated data is also automatically shared with local urban planners. And all this without Bennie having to post anything himself! Talk about convenient…
	Daytime at work/school
Life-logging devices and applications are dropping in cost and offer a way of	When Annika arrives at work, she quickly checks her e-mail. One is a new contact request in her social network from "Helena" down in Purchasing. While the face looks vaguely familiar, Annika cannot really remember

recording personal history for later recall, which has benefits for many people, who can't quite remember certain details

meeting her – Helena's message says something about last week's company midsummer fest. Annika quickly opens her lifelog app and browses through the images from the event. Bennie had given her some really nifty lifelog jewellery last Christmas: a pendant with an integrated camera and Bluetooth module, which takes a picture every minute and sends it wirelessly to her phone, from where her "CloudNote" app then regularly archives it into her life-log cloud. And indeed, there she is: Helena from Purchasing, in what seems to have been an extended discussion with her and Larson, the IT guy. She realises that the photo also caught Nils, her colleague, while he was engaged in nasal mining! Yuck! She'll have to forward this to him later – maybe he'll treat her for coffee if she promises not to share! She moves on to the message from Ingemar in HR, who has asked everybody to check if they imported old data to a new portal all right. Annika quickly clicks on the link and enters her login credentials at a nicely designed new portal page. Unfortunately, the system keeps rejecting her password. As she is about to close her e-mail window, a message from IT security comes in: "Warning: Phishing attack posing as an e-mail from HR! Do not follow the login link!" Oops!!

Unbeknownst to him (as yet), Annika's work colleague Nils has been caught on a life-logging device which captures an unflattering image of him [R1 R2

Social networks can increase the social attack vector significantly, making impersonating a colleague much easier [R3 .

Life-logging may offer many benefits, including convenience in paying bills and providing data to tax authorities automatically, but there is a risk of discrimination against those who are not so computer literate or can't afford more advanced technologies *[Error! Reference source not ound.* ***. "Free" versions of some services often come with a price – e.g., personal data going to advertisers [R2]***

Bennie has since finished his meeting at a nice bistro over coffee and pastries. Using his phone to pay, Bennie automatically set it to upload the transaction to his MyFinances online service. By tagging it with the client's name, not only can he easily keep track of his various client accounts but also he can easily file his tax return, including a scanned copy of the receipt (which he snaps with his phone's camera). Incidentally, the rise of such personal finance services has allowed tax authorities to vastly streamline their operations: as Bennie has opted for the DirectTaxLink feature, he enjoys a 1% tax break in exchange for the instant sharing of all tax-relevant receipts with the national revenue services. As his receipt also shows the bistro's tax identification number, authorities at the same time cross-correlate his purchase with the bistro's tax record, thus improving accounting reliability. While Bennie is using the paid version of MyFinances, there is also a free version that offers much of the same functionality yet also shares personal consumption data with advertisers.

Dana is "manipulated" by the darknet – wanting to protect her image in

Dana's school day is uneventful, apart from that moment when Lena and Marit ask her to go down to the roundabout with them during lunch break. She almost agrees to come, but luckily remembers that her location profile

darknet, she feels she can't go with her friends, otherwise her tracker will expose her being off school grounds [R11]

already streams into the social darknet, and she would thus be logged as being outside the school grounds. She quickly mumbles an excuse and as Lena and Marit take off without her, she briefly regrets not knowing how to reconfigure her tracker so that she could still safely venture outside the school grounds.

Attacks can burn time and resource on the part of victims [R3]

Annika is simplifying her life, but she still may be exposed to risks subverting essential protections [R1 R2 , R3]

New life-logging applications have benefits such as a (human) memory back-up

As Annika is finishing up, she quickly reviews her day. Due to that false e-mail from HR, she spent all morning on the phone with the company IT helpdesk resetting all her various passwords. Oh well, she should have updated those passwords a long time ago, anyway. Good thing she had that "CloudNote" app installed on her phone: she simply recorded her voice as she was repeating all those changed passwords to herself. The CloudNote app streamed this directly into her lifelog account, indexing them in the process so she will be able to look them up in case she forgets them later.

While life-logging can make it easier to record and thus manage actual use of time, excessive use may also decrease productivity [R8

While Annika consents to the provision of her data, there's a risk that her employer (or any organisation) does not fully comply with data protection legislation [R4

Data can easily be aggregated from different sources [R2 R11 , and her activities could be "steered" by the system ("advisors") [R7 R8]

Any organisation processing personal data will be

Annika checks her work logs to review how she spent her work time last week. When they announced the availability of the "Getting Work Done" app last September, she was at first highly sceptical, just like all of her colleagues: who would want all of their e-mail and other work habits to be monitored?! However, participation is completely voluntary, and management is apparently only seeing aggregated data. So after she tried it for a few weeks, she quickly got hooked. Using a combination of software and devices, the system is able to track her work activities on her laptop, her company smart phone, during meetings using the AV system in place for videoconferencing, and even her personal sensor patch she is wearing to track her health levels. All of the various devices and software monitors feed into a single "work log" in her company portal, allowing her to inspect her own performance and accomplishments. Optional software "advisors" suggest improvements to daily routines. By now, almost all of her colleagues are using the system, even after their initial reservations. And it does feel good to see her efficiency steadily rising, she has to confess. A recently released add-on now supports collaborative inspection of these profiles, which allows them to be used

tempted by function creep [R2]. Here supposedly anonymised data comes back for use in yearly performance reviews. Supposedly such use is voluntary, but employees may not be able to resist the pressures, especially if they think the employer might hold it against them if they don't "cooperate" [R7 , R8].

This could also result in subtle pressure among colleagues to make their profiles available for performance reviews; this peer-pressure creates a tendency and a sizable risk to abide to conformity [R7 R1].

during the yearly performance review – only on a voluntary basis, of course!

Leisure evening

Life logging may also be used in collaborative work settings – "two heads are better than one" – which has benefits for users

Such community systems, like this school logging network, may allow people to "spy" on each other through functions designed for collaboration [R6

Also, there is potential for discrimination based on life-logging data [R5]

Life-logging leisure activities can increase the fun of competing, but may risk disclosure of otherwise

Back home, Christer logs into their school's media system and begins his homework, only to notice that Freia is logged in as well! He nonchalantly acknowledges her on the chat channel and sets out to do the assigned research: they are supposed to create a set of Web pages on deforestation. He quickly checks the log of Freia's action that the system automatically keeps of each student, in order to allow the teacher to understand each student's contribution. In quite a cool fashion (Christer thinks!), he contacts Freia over the chat channel to co-ordinate. Time flies by, and by the time Freia has to leave, as her mom is calling for dinner, Christer realises that he has spent the last half hour chatting! Then he realises that all of this is now archived in the school's media system, accessible to all class members! Ugh!

Christer fires up his "Nebula" gaming centre app. Joe from Atlanta is online, and they quickly battle it out on a small map, against two guys from Belarus. Soon their two opponents fold, and Joe and Christer earn a badge for such a quick victory! Of course, it is precisely at the medal presentation ceremony clip that his mom has to enter, calling him for dinner. "Another medal, young man?" she dryly remarks. "I thought you'd be doing your homework, but instead you are spending all your time online again! You better enjoy the sight, because I'll be locking down your game account for the rest of the

private information [R1 R2]

week!"

Life-logging and other social media can be used to convey false or misleading data [R3 R2]

Being a parent does not mean you don't need to respect your child's need of privacy: where do we draw the line? [R6]

After the kids have gone to bed, Annika checks on Dana's updates: "Good, she posted something again today. Maybe having Bennie talk to her really helped." A quick cross-check shows that Dana is still mostly spending time with her long-time friends Lena and Marit. No boys yet for her, so one less thing to worry about! She really is amazed at that data-mining pack that she subscribed to for use on her mashup page – it really does find some interesting correlations!

Social networking connects us to otherwise unknown persons – can they be trusted? [R4 R3

She then calls up Christer's various blogs and school media records. Thirty-nine new medals in the last two weeks alone?! Incredible! "Good thing I decided to cut off gaming for this week," she thinks. Then, she notices that total playing time was only 146 minutes, i.e., only some 10 minutes per day. Hmm, maybe I was too harsh? But really: who are all these people? Joe from Atlanta?! I really should be watching his friends a bit more. But school activity is up, and it seems a girl is involved! Interesting: his activity records seem to increase whenever that Freia is in his class.

Although the easy, affordable presence of electronic devices might be seen as taking over our lives [, they do offer the benefit of greater community collaboration and activism. However, it's not always known to whom our tweets and other "digital" messages are being conveyed or even how others have obtained information about us [R8]. There's also the possibility that our (choice of) lifelogs can misrepresent us [R5

Before she goes to bed, she checks her e-mail one last time, only to find a new message from the Riseberga neighbourhood council: since her public driving record indicates that she takes the Toftanäsvägen road regularly, they are inviting her to join a planned online referendum on the city's plans of widening it into a four-lane road. She briefly wonders if her tweets against last year's highway extension made them target her specifically, hoping that she would join them. In fact, widening that road should make her morning commute easier. Maybe she should talk to Bennie about this – he must have gotten a similar invitation, given his activity at CycleMalmö. In any case, she really should check again who is on her follower's list – it sure looks as if a few bots are automatically interpreting her postings.

The ubiquity of life-logging technologies results in a loss of solitude or contemplation time [R7 R12]

Another trade-off between "free" services in exchange

Before going to bed, Bennie logs into his asthma community web for a last check. He still remembers when his health insurer had given out free sensors a year ago, allowing participants to upload vital data to the insurer in exchange for discounts on the monthly premium. Bennie was the first to sign up, expecting some significant savings due to his daily bike commute. He was thus quite surprised when, after three months of use, he received an "invitation" for a medical check-up to "reassess his insurance protection" and

for personal data [R7 R8]

Faulty equipment and thus the uploading of inaccurate data can lead to higher insurance premiums [R7 .

some pamphlets on how to deal with obesity. It took him several weeks and many phone calls with the insurer's hotline until he realised that the sensor had reported faulty blood pressure levels ever since he installed it, resulting in his profile matching that of a highly obese person.

Young people (or anyone) can put themselves at risk by not understanding how they can be manipulated by social media [R1 R2 R8 R6]

Before she goes to sleep, Dana sets her phone to post two additional status messages before midnight, so that Leif does not notice that she had to be in bed by 10:30 pm! While things have certainly got more complicated ever since she moved networks, she really is thrilled by the fact that no adult [most importantly of course her parents!] will see her messages anymore. Tomorrow, she will ask Leif for some help with setting up that fake updater – that sure sounds like a great excuse for contacting him again!

3 BENEFITS OF LIFE-LOGGING TECHNOLOGIES AND APPLICATIONS

We have already noted how the concept of logging one's life, memories etc is not entirely new. However, the fundamental differences between new and emerging life-logging technology and earlier forms from the previous centuries are effortlessness, cost-effectiveness, improved resolution, breadth, and persistence. Previously one had to expend quite a lot of effort in recording the events of one's life; before the digital camera became ubiquitous the cost of media to record anything but a handwritten account was prohibitive. The continuously decreasing cost of computer memory means that it is now practical to make daily records of one's life using audio, video, and still images, among a huge array of other data including e-mail, calendar and personal performance measurements. The decreasing cost of storage also means that this data can be easily copied, shared, and kept forever.

Life-logging technologies may take many forms. Perhaps the most obvious currently popular technologies are the digital camera and social networking websites supporting multimedia such as Flickr, Facebook, and YouTube. Many new devices now support fully automated logging of activities and uploading to websites, such as the FitBit which monitors activity or sleep, the ViconRevue camera which automatically takes images constantly throughout the day, or the various smartphone applications which automatically track users or monitor their activities, such as Google Latitude. Office productivity software on desktop computers, tablets and smartphones can track diary information, and email activity as well as browser and other Internet activities. Smart homes can adjust heating and energy use automatically according to the occupancy pattern.

With adequate privacy controls so that it is only shared with those who should see it, life-logging has the potential for significant benefits across the spectrum of society. These benefits are conceivable for economic players and governments as well as individuals and the social environment in which they are embedded. For example, individuals may adopt a particular life-logging technology for their own benefit, such as location-tracking or health monitoring. They may then agree to allow their anonymised data to be shared with the traffic or health authorities to help plan infrastructure, allow others to avoid vehicle traffic congestion, or predict how diseases are spread. They may choose to trade[7] their life-logging data to businesses to use for marketing purposes: although this business model is not yet fully established, nor have its impacts been fully determined as yet, in principle business are supposed to benefit from collecting very valuable and accurate data, while citizens could be provided in return for handling out their data with the option of "free" services or reduced service charges.

In the following sections we discuss some of the areas where life-logging may benefit individuals, commercial /economic interests, government, and society in general.

[7] This could also mean "selling" their data, as it already provided by some on-line services e.g. www.i-allow.com, www.myid.com, www.mint.com.

Individuals

Individuals can benefit from life-logging, both on a personal level and on a societal level. Life-logging allows friends and family to stay in closer contact with what each other is doing and how they are feeling regardless of physical distance. This may reduce their sense of isolation and help them enjoy social bonds with others in the virtual world. One can build up a personal archive of personal milestones, important moments and memories etc. (in a way replacing the old family photo album) that is richer and timelier. In doing so, people are able to construct separate online existences and personas if they so wish. Online, they may have more control over how they want to represent themselves. Depending on the logs they release they can publicise socially-approved aspects of their lives (this assumes of course that security and privacy controls are adequate).

Life-logging can help support bonds and friendships for a longer period of time than would have been possible without the tools' support – although these may be "weak ties" that are less psychologically beneficial than physical-world relationships. Private social life in the physical world may get richer through the online transparency of events happening in the physical sphere. In addition, people can keep in touch and build relationships with online friends in other regions of the world.

From a professional perspective, individuals can be more aware of their colleagues' and professional contacts' activities, which may make it easier to contact the right people from their networks when they need advice on a specific problem; they can also benefit professionally by building their reputation online, e.g. getting a better job etc (consider for example the existing case of many artists and other individuals, that got a job through exposing their work in social networking sites, such as YouTube etc.]

But also on a private level, one is more aware of what others are up to, what events they will visit and thus private social life in the physical world may get richer through the online transparency of events happening in the physical sphere. In addition, people can keep in touch and build on online friends in other regions of the world. Life-logging offers the advantage that it occurs automatically, whereas with other popular social networks such as Facebook or Twitter, one must make a conscious effort to record something. Life-logging offers a continuous stream of data compared to occasional bursts of information that one keys into a social network.

Finally, the ability to automatically and effortlessly log a huge range of data about one's daily life, combined with the right tools to analyse the data, could allow people to better understand themselves along with their habits and behaviour. Achieving a personal goal, such as losing weight or eating more healthily, could be aided by having data about one's actual behaviour. Being able to compare an objective measure of a person's activity with their previous history or with a desired group norm can help "nudge" them toward desired behaviour. One valuable domain of life-logging in this context may include health-related data, which can also be used by medical practitioners to more easily track symptoms and help diagnose or treat conditions. To some extent, these tools can also support older

people to live independently, while providing reassurance to the rest of their family that they are well and healthy.

Commercial and economic interests

The data generated by individuals will underpin new business and charging models. For example, commercial real estate may be valued against the background of real consumer flows or traffic in front of a building. Advertisements may be paid for on the basis of whether people see and discuss them, purchase the advertised products, or pass by them at the right moment. Individuals or groups may elect to trade parts of their life-logging data with "free" services, so as to help marketers better understand a certain demographic or in order to receive better targeted offers. By better understanding the needs of the individuals to whom they are selling, companies can more easily implement first-degree price differentiation: the most efficient form of pricing from a company perspective, although not that popular with consumers.

The decreasing cost of sensor and storage technologies provides commercial opportunities for companies to embed life-logging technologies in traditional physical goods. Network-enabled smart domestic appliances and vehicles are becoming the norm and the range of services that can be sold to consumers increases with each new smart device. These devices in turn can have an economic benefit both to individuals and society as less power is used by devices which regulate their own energy usage based on data from the environment and the life-logs of individuals.

State / government and society

Logging movements of individuals and vehicles also promises to help organise infrastructure, such as roads and traffic, more efficiently. Urban planners can use data from people rather than relying on models and sampling techniques in order to decide where to improve roads or provide better public transportation. Road traffic queuing may be reduced if bottlenecks can be predicted in real-time before they become serious and traffic management can react with immediate countermeasures. The number of accidents may be reduced in the same way. Generally, infrastructure load can be more carefully planned and balanced, extending its lifetime. People can be notified of alternative routes in real-time, such as taking another road than one that is currently congested.

Access to the health life-logging data of groups across a country could help target national health infrastructure promotion campaigns as well as get early warnings of disease outbreaks. Areas with more sedentary individuals can be targeted so as to encourage a more active lifestyle, and other health choices can be tailored at an individual level.

Last but not least, society at large and semi-public or public institutions could potentially benefit from life-logging, because the data generated from life-logging services can provide useful input for the state to consider. As we already experience, social networking and social media have an impact on public affairs; in this light and considering its nature, life-logging and continuous activity sharing activities are likely to provide an additional source of citizens' input to various political issues, for

example, either in the form of explicit feedback (a "Like" button for policy) or as a "voting with your feet" observational feedback of citizen activities and preferences. The concept is not new: "participatory or urban sensing" with the use of mobile phones and online social networking has been already advocated to offer many benefits[8]. It may also offer important statistical feedback, potentially instantaneous, on certain policy decisions (e.g., how does the new smoking ban affect restaurant patronage?); in this respect, life-logging activities can provide to governments some good indications of public opinion and to a certain extent influence policy-making[9]. By this we do not mean to say that it will change the way politics works or shape, but rather that there is some potential in this area, that may be worth exploring, provided that the state considers carefully the risks life-logging may pose (some of which are analysed below). Whether life-logging and continuous online activity sharing can even act as a tool a government can use to foster citizens' participation in public affairs, and thus improve the public services, is something that remains to be seen.

And finally, the persistence and completeness of life-logging data could be invaluable to future historians as they will have not only our written records and images but detailed data about our behaviour and personal interactions.

---

[8] Estrin, D., 'Participatory sensing: applications and architecture [Internet Predictions]'. *IEEE Internet Computing*, Vol. 14, No. 1, 2010, pp. 12–42.

Ganti, R.K., Pham, N., Tsai,Y.E., and Abdelzaher, T.F., 'PoolView: stream privacy for grassroots participatory sensing', *Proceedings of the 6th ACM conference on Embedded network sensor systems*, ACM, New York, 2008, pp. 281–294.

Goldman, J., Shilton, K., Burke, J., Estrin, D., Hansen, M., Ramanathan, N., Reddy, S., Samanta, V., Srivastava, M., and West, R., Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world, *Woodrow Wilson International Center for Scholars*, 2008, pp. 1–15.

Lane, N.D., Eisenman, S.B., Musolesi, M., Miluzzo, E., and Campbell, A.T., 'Urban sensing systems: opportunistic or participatory?' *Proceedings of the 9th workshop on Mobile computing systems and applications*, ACM, New York, 2008, pp. 11–16.

Osimo, D., Szkuta, K., Armenia, S., Lampathaki, F., Koussouris, S., Mouzakitis, S., Charalabidis, Y. et al. *The crossroad roadmap on ICT for Governance and Policy Modeling*, 2010.

[9] A nice example is that of the EU FP7 funded research project "+Spaces" ["Positive Spaces"] which focuses exactly on this: it aims to "provide tools that will allow the exploitation of virtual worlds for assessing public reaction […]" .http://www.positivespaces.eu/

4 ENISA EFR FRAMEWORK AND RISK ASSESSMENT METHODOLOGY

The European Network Information Security Agency (ENISA), has undertaken the development of a framework for the analysis and reporting of emerging and future risks in the area of information security. ENISA defines emerging risks as those that may have an impact between one and five years in the future; and future risks as those that may have an impact more than five years in the future.

4.1 THE EFR FRAMEWORK: CONCEPT AND PURPOSE

The EFR Framework is based around the use of predictive, narrative "scenarios". The concept behind scenario planning is essentially simple: it facilitates the telling of realistic stories about possible (or probable) future events, based on extrapolation from present trends.

In the EFR Framework , the use of scenarios, rather than any other form of analysis, is intended to ensure that the extrapolations are both realistic and can be understood and appreciated by the decision makers. When building the scenario, a single technology, or prospective use of that technology, is selected for consideration. This is then built into a unique scenario that describes a situation in the future; in which that technology, or its functionality, has been deployed.

Once an area of EFR interest has been selected; a narrative story or "scenario" is written. The concepts underlying the story are then subjected to a risk assessment process, more information on which you may find in the next section. This looks at the technology and its use, as described in the narrative, in order to identify possible threats and vulnerabilities. From these, the assessment deduces the potential risk to the assets mentioned by the narrative.

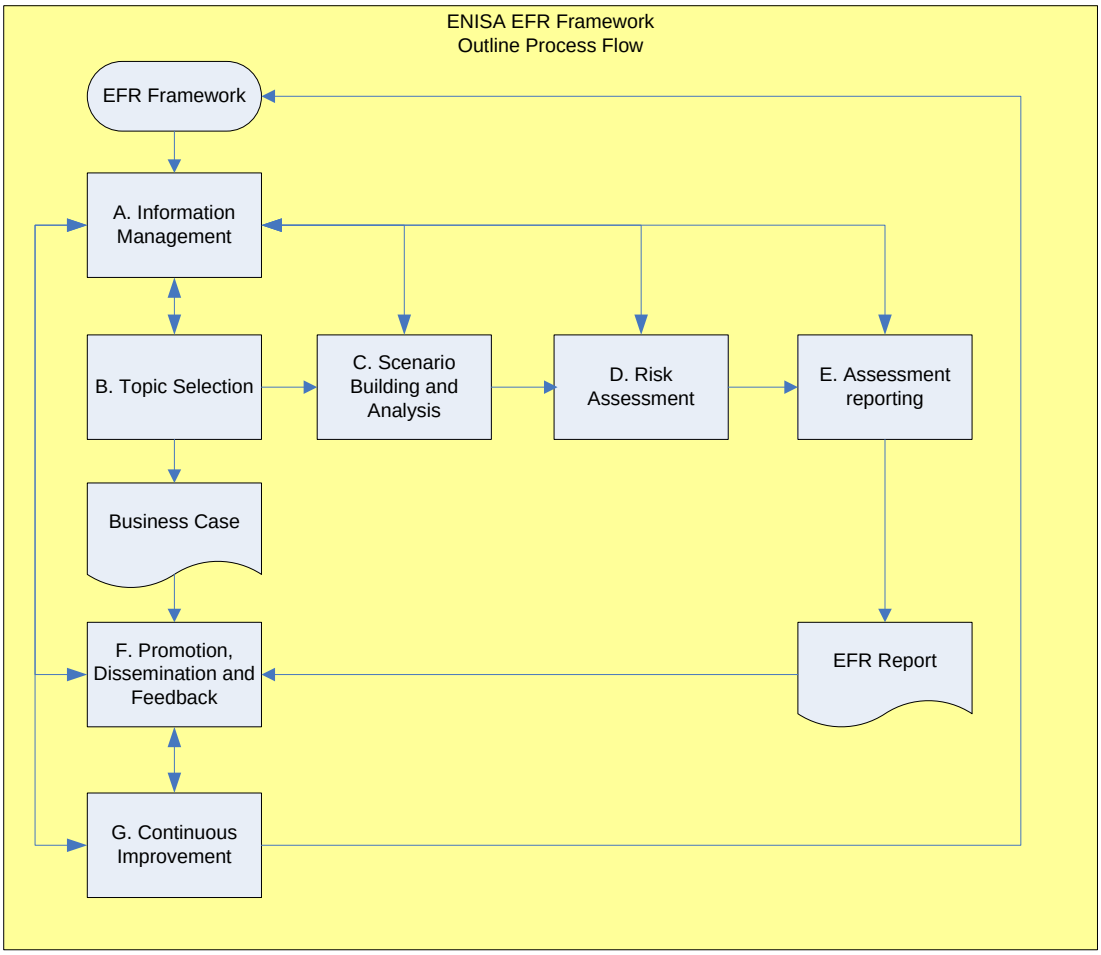
The purpose of the ENISA EFR Framework is similar to that of classical scenario planning; in that it alerts those reading the report to possible future outcomes of current trends. However, the EFR Framework is both more narrowly targeted and more structured; in that it delivers a reasoned assessment of the risks inherent in the technology and its use.

EFR assessment reports should be read by appropriate target audiences in order to ensure that the risks (both positive and negative) inherent in a technology and its use are recognised and understood. If considered necessary and appropriate, comprehension of the risks will enable decision makers to take appropriate steps to manage and mitigate them, where possible.

At figure 1, below, is a simplified, outline flow diagram showing the processes of the EFR Framework. These are as follows:

A. Information Management
B. Topic Selection
C. Scenario Building and Analysis
D. Risk Assessment

E. Assessment Reporting
F. Promotion, Dissemination and Feed-back
G. Continuous Improvement.



For more information on the EFR Framework, please refer to the *ENISA EFR Framework – Introductory Manual* [10].

[10] *Emerging and Future Risks Framework – An Introductory Manual, European Network and Information Security Agency (ENISA)*, 2010. Available at: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/emerging-and-future-risks-framework-introductory-manual

4.2 RISK ASSESSMENT METHODOLOGY

The methodological approach used in this project to identify and assess emerging and future risks was based on the standard **ISO/ IEC 27005:2008 Information technology — Security techniques — Information Security Risk Management**[11].

The evaluation scales and metrics have been customised to fit the project's requirements.

The following major steps were performed in the process of assessing the emerging and future risks:

- Assets identification and valuation
- Vulnerabilities identification and assessment
- Threats identification and assessment
- Identification of existing / implemented controls
- Identification of final risks

4.2.1 IDENTIFICATION AND VALUATION OF ASSETS

In this step, we identified the major assets to be protected in the scenario and we estimated their value.

For the purposes of our analysis, asset identification was performed at the composite asset level, meaning that personal and other type of data was identified as part of a physical asset (e.g. a smart device, a health monitoring device, a database etc.) and not as a separate asset. As such, the estimation of the value of the physical asset considered also the value of the data that resides on this asset.

To estimate the asset value, we identified and considered the certain impact areas. Using a scale from 1 to 5 (Very Low to Very High), we estimated the impact in each area for each asset. The final asset value was the maximum of these values.

4.2.2 IDENTIFICATION AND ASSESSMENT OF VULNERABILITIES

The purpose of this stage was to identify and assess vulnerabilities of the assets. A "vulnerability" refers to an aspect of an system / process (the assets) that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that

[11] International Organization for Standardization (ISO), Information technology — Security techniques — Information security risk management, International Standard, ISO/IEC 27005:2008(E), First edition, 15 June 2008, p. 1.

are likely to be threatened. These vulnerabilities are independent of any particular threat instance or attack.

In the evaluation of the vulnerabilities, a scale from 1 to 5 (Very Low to Very High) was used and the following attributes were considered:

- **Severity**: The severity of impact that will be incurred if the particular vulnerability is exploited. This includes the scope of the impact and the escalation potential (e.g.: where the exploitation of the particular vulnerability would subsequently lead).
- **Exposure**: The ease of exploiting the particular vulnerability through physical or electronic means (required know-how, required resources).

It should also be noted that the vulnerability value was assigned when related to a specific asset, since the same vulnerability had different value in different assets. The vulnerability assessment also considered possible existing / implemented controls identified or assumed in our scenario.

4.2.3 IDENTIFICATION AND ASSESSMENT OF THREATS

This stage involved the identification and assessment of possible threats that could exploit the vulnerabilities of the assets identified. It should be noted that threats exist regardless of the vulnerabilities, and there are two major categories of threats to be considered: **man-made** and **natural** threats, namely threats due to humans (either accidentally or intentionally) and threats due to natural events (e.g. adverse weather conditions).

Using the same scale of 1 to 5 (very low to very high), the threats are evaluated, considering the following parameters, especially for man-made threats:

- **Capability**: The amount of information available to the threat agent (knowledge, training, technological sophistication etc.) and the availability of the required resources.
- **Motivation**: The threat agent's perception of attractiveness of the assets, danger of apprehension, and in general motive to violate standards and procedures

Please note that the function of these two parameters provides the **likelihood** of this threat to occur.

4.2.4 IDENTIFICATION AND ASSESSMENT OF IMPLEMENTED CONTROLS

As controls we identified measures for protection and effective operation of the assets such as: policies, procedures, organizational and technological manual or automated mechanisms.

As our scenario is plausible, existing (implemented) controls have been identified in the form of assumptions in the scenario development.

The expert group considered existing controls in the evaluation of vulnerabilities and threats. The values of which have been decreased in some cases due to the existence of these controls.

4.2.5 Risk identification and Assessment

According to ENISA's risk analysis methodology, the final risk and its value are a function of the three elements namely:

Risk = f(Asset, Vulnerability, Threat)

In practice, after identifying and assessing the vulnerabilities for every asset, the group followed these steps:

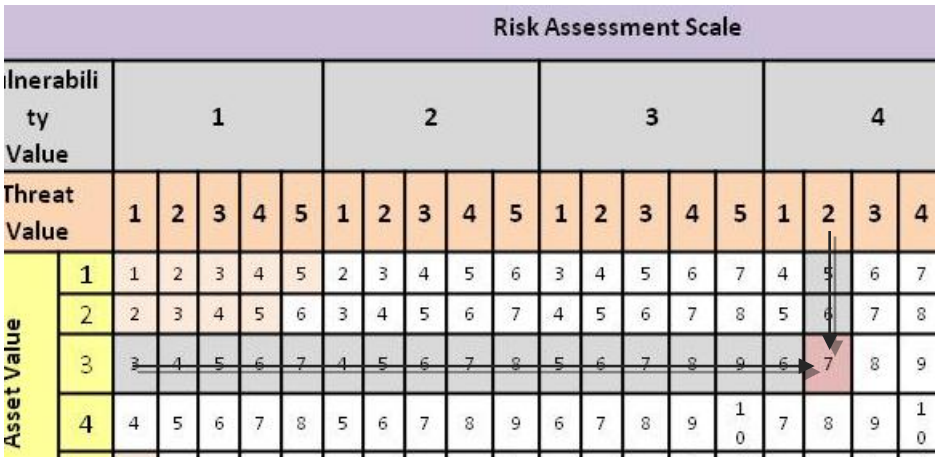
- **Mapping threats to vulnerabilities**: In this step, the group identified possible threats that could exploit each vulnerability of each asset. It is the unique pairs of vulnerability and threat for a certain asset that produces a risk for this asset.

- **Risk value**: As mentioned above, the value of the risk is a function of the asset, vulnerability and threat values. The asset values, and the threat and vulnerability levels, relevant to each type of consequence, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 1 to 13. The values are placed in the matrix in a structured manner[12].

[12] Id.

Risk Assessment Scale																									
Vulnerability Value		1					2					3					4					5				
Threat Value		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Asset Value	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
	2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
	3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
	4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
	5	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13

According to the standard, for each asset, the relevant vulnerabilities and their corresponding threats are considered. In principle, if there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk[13]. Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the vulnerability value and the threat value. For example, for an asset with a value of 3, with a vulnerability valued at 4, which can be exploited by a threat valued at 2, the final risk produced is estimated at the value of 7, as shown in the figure below:



All of the steps presented above have been performed and are documented in an Excel file, which can be found in the attached Annex III of this report. The results for each step are presented in the relevant worksheet tab.

[13] Id.

4.2.6 Risk mitigation – Identification of controls and recommendations

Following the identification and assessment of risks, the group ranked the risks from very high to very low. Therefore, as the next step, the group identified possible controls and safeguards that could reduce those risks. For the purposes of this analysis, the risk mitigation step has been limited to the recommendation of potential controls to mitigate the risks identified: these are presented in the form of recommendations, in Chapter 6.

4.2.7 Residual risks

For making our analysis more complete, we have identified certain risk areas that would still need to be further considered even after the implementation of the proposed solutions, as well as other open issues (Chapter 7). This by no means was an exhaustive analysis of the residual risks, especially given the nature of our assessment (prospective scenario).

5 RISK ASSESSMENT RESULTS

This chapter describes the results of our analysis, namely the assumptions we had to make during our scenario development and assessment, as well as the identification of assets and risks.

5.1 ASSUMPTIONS

The scenario presented in chapter 3 above draws on a number of assumptions both interdependent and those that can stand alone. For ease of, reading assumptions have been grouped into a number of different categories although these divisions and categories are not exhaustive and are not meant to be definitive. As described elsewhere, life-logging represents the (r)evolution of a potentially complex set of services and human interactions with services and devices enabling these services. This is matched in foregrounding/identifying the particular assumptions on which it is expected that such trends will capitalise and build.

TECHNICAL

Technical assumptions are a key driver for the scenario and can be roughly grouped into those assumptions which build upon currently existing and emerging technologies and infrastructures developing further and those that are newly developed. For the purpose of the risk assessment of the scenario, the expert group assumed that:

- Smart devices such as cameras and mobile phones will continue to evolve in terms of functions, e.g., increased storage and networking.
- Due to an increase of processing and storage efficiency, prices for mass-market hardware and software services continue to decline.
- Advances in network and service interoperability and integration will allow for near or total seamless interaction between an individual's devices, at home, at work and while mobile.
- There will be significant advances in battery storage, energy optimisation in devices and new micro power sources, allowing devices to operate longer, collect more data and access more services for increased durations when individuals are mobile.
- Networking devices and infrastructures are an ever present feature of modern locales and will lead to ever more blurred distinctions between being offline or online in various places.
- Powerful new mining technologies for massive collection of data, video and image files will emerge that make it easy for organisations and individuals to shift through oceans of data to find the details or patterns they want.

- Location-based services and position determination capabilities will be an integral part of an ever-increasing range of devices and applications, so much so that the precise location of data subjects will be continuously tracked. For example, the development of next generation wireless networks (trends towards micro, pico etc. cells) and the start of the Galileo system is expected to make the location detection even more precise than today.

- New smart devices, such as bio-sensors, will emerge and will enable the collection of more and new personal data from individuals, e.g., biometrics for identification and mood sensing, new ways of interacting with devices, etc. Data processing and communication capabilities will increasingly be built into every-day objects, such as mirrors, bicycles, automobiles which will be integrated into life-logging applications.

- Since the focus of this study is life-logging, the group didn't consider it appropriate to embark on a detailed vulnerabilities' and threats' identification of PC and home infrastructure. The group thus assumed that there are bound to be certain vulnerabilities in the PC and home infrastructure in 3-5 years, when the scenario takes place. The vulnerabilities have been estimated by the expert group as **High** [4 out of 5 in our metric scale].

POLICY

Policy assumptions are closely entwined with social, legal and economic assumptions made for the scenario. Policy assumptions include policies supporting or enabling particular facets of the scenario, such as user acceptance. The group assumed that policy-makers, organisations and other national and transnational policy actors will derive benefits from aggregated life-logging activities. The group assumed that:

- Public awareness campaigns, for particular demographics not familiar or comfortable with new life-logging services or for those who are economically unable to avail of such services and devices will be supported and promoted by the EU and national governments.

- Life-logging services and devices will allow for new forms of policy-making, in particular around local issues as well as new ways for citizens to interact with policy impacts and those making policies. Increased connectivity as a result will shape new ways of policy development, both from organisational and individual perspectives.

- Data generated by particular life-logging activities will become a tool for policy analysis and implementation, such as new, more sophisticated and responsive traffic management systems as detailed in the scenario.

- There will continue to be policy initiatives aiming to inform and educate people in relation to their rights to privacy as well as and in regard to the risks arising from use of life-logging activities.

Nevertheless, policy-making will continue to lag behind the development and use of new technologies.

SOCIAL

Social assumptions can be broadly grouped into those made in relation to individuals acting within society and societal wide assumptions affecting individuals themselves. The group assumed that:

- Family members will make use of life-logging devices and services in order to communicate and keep in contact with each other.
- The use of ICTs and networks will allow for new ways of providing social services of different kinds, such as education as described in the scenario text.
- Social acceptance of personal recording devices will increase, at work, at home, in public as well as private spaces. Legal frameworks as detailed below will emerge to offer some baseline protections. Automated profiling and data analysis about individual preferences and behaviour will gain acceptance, especially where users perceive improvements in particular services, products and device operation as a result of such analysis.
- Although the complexity of networked privacy will not decrease, it is assumed that individual and societal desires and wishes, such as the desire not to be recorded or included in others' life-logging activities will be reflected to a certain extent in parameters and settings coded in devices and software.
- Some people will continue to be careless with their privacy; there might be also people whose perception of privacy allows them to share their data more than others or who enjoy being looked at and exposed socially; and also people that consider that the benefits of publicity outweigh the costs of having less privacy.
- Peer-group pressure will also continue to play a role in some people being careless, such as Dana's joining a dark network to impress Leif, an older boy.
- Some people and companies and governments will continue to spy on others, sometimes for supposedly benign reasons (like Dana's parents who want to make sure Dana is not going "off grid").

LEGAL

In constructing the scenario, the group made certain legal assumptions linked with the risks that could arise from the scenario. Particular risks will be explicitly targeted by the implementation of legal protections, such as in relation to privacy, data protection and data collection. The group assumed that:

- A new European data protection regulatory framework will emerge to deal with the perceived new and existing risks to privacy as a result of the proliferation of life-logging devices and services, but also of other new technologies over which life-logging services can be provided. The new and updated data protection frameworks highlight the principle of privacy by design and emphasise principles of accountability in light of changes to the meaning of 'data controllers' as a result of life-logging services and devices.

- As a result of the above, some end-user controls over data collection and use of data will have been further developed; we do not however consider that the level of sophistication of this would still adequately address the requirements. A regulatory environment enforcing some privacy-enhancing technologies (PETs) will emerge. This is reflected in both devices and software in devices attempting to automate or provide settings so that individuals can more easily control privacy and offer protections outlined by European data protection regulatory framework.

- The need to have international legal frameworks related to transnational flows of data will be well established and understood as it is nowadays; but in 3-5 years we consider that there won't yet be such an appropriate framework in place, allowing for proper transnational interoperability in terms of life-logging devices and services; this issue would certainly continue to present a challenge in the coming years.

ECONOMIC / GROWTH

It is assumed that products, services and devices are produced in a commercial environment where profits can be made (although some non-profit services are described in the scenario, these draw on infrastructures developed within a commercial environment). The group assumed that:

- A number of product providers and service providers operate within the life-logging environment. Some super-providers continue to exist but it is assumed here that the wide range of potential activities enabled by technical developments will lead to a proliferation of new commercial operators and some competition among providers.

- Some commercial operators are based in countries outside the EU, where the legal frameworks assumed above remain difficult to enforce by the EU and Member State statutory regulatory authorities.

- New services and products derived from life-logging will enable increased efficiencies in existing markets (such as energy, traffic management, etc.). Commercial operators will see new market opportunities in life-logging and take advantage of these.

- Data, and new forms of data generated by life-logging activities, will increase in value as a resource and product itself. Individuals will be enticed to derive from the value of their data and that of others through, for example, participation in targeted data mining/profiling services that offer

reduced fees for services. Certain service providers will continue to make the use of their services conditional to the consumer's opt-in to the processing of personal data for secondary purposes, thus essentially bundling the supply of the desired service to the consent of the data subject.

- Life-logging data will be considered a treasure trove for companies marketing goods and services at life-loggers and others. This would increase the motivation of big companies to collect as much personal data as possible, in order to provide highly targeted and personalised services to individuals.

- Prices for computing resources continue to be at such a low level that a life-logging service infrastructure is affordable for the mass market.

5.2 ASSETS – WHAT ARE WE TRYING TO PROTECT?

This section identifies the assets that we wish to protect against potential risks that can have an impact on them. Within the life-logging and continuous instant activity sharing context, assets can be tangible or intangible as well as be owned by various stakeholders such as family members, software vendors, service providers, etc. Assets may include hardware, software, systems, data, business processes, buildings/facilities, equipment, or infrastructure.

Assets have vulnerabilities that could potentially be exploited. These vulnerabilities expose assets to various risks. For example, there is a risk associated with life-logging devices and services in that an individual cannot control the recordings of himself made by other users. In this sense one person's life-logging device may capture and broadcast unflattering data about another person without knowledge or consent.

During a meeting in London in November 2010, experts used the life-logging and continuous instant activity sharing scenario as a framework to identify assets likely to be owned by various stakeholders. After the discussions, the group agreed upon the following set of assets as significant within the continuous instant activity sharing context:[14]

INTANGIBLE ASSETS

A1 – ACTORS' DIGITAL PRESENCE NOT INCLUDING SOCIAL OR PROFESSIONAL REPUTATION: Identity, avatars, profile etc.; *Value*: MEDIUM

A2 – SOCIAL REPUTATION: Parts of digital identity relating affecting social reputation; *Value*: HIGH

A3 – PROFESSIONAL REPUTATION: Parts of digital identify affecting professional reputation; *Value*: HIGH

[14] For the detailed asset identification and impact assessment, please refer to the Appendix II: Risk assessment spreadsheet.

A4 – SENTIMENTS: Includes any subjective feeling, emotion or information. It can include personal opinions (e.g. strong rejection of an ideology), bias, attitude, tonality, affective/emotional state etc; *Value*: HIGH

A5 – IDEAS: Includes any result of creative process, reflection or in general any use of intellect with the purpose of creating a new concept or knowledge; *Value*: MEDIUM

TANGIBLE ASSETS

A6 – LIFE-LOGGING SERVICES: services provided to our scenario user for updating and storing online their activities or other data they choose from their everyday activities, e.g. CycleMalmö online community, Annika's life-log cloud; *Value*: MEDIUM

A7 – SOCIAL NETWORKING SERVICES: Blogs, photo-sharing, Christer's brushy game, "Nebula" gaming center … as they affect the user (not service provider); *Value*: MEDIUM

A8 – SMART HOME OBJECTS / APPLIANCES: Fridge, mirror, dishwasher, IP TVs; *Value*: LOW

A9 – PC AND HOME INFRASTRUCTURE; *Value*: MEDIUM

A10 – SMART PHONE / MOBILE PHONE / LIFE-LOGGING DEVICES: Including data stored; *Value*: MEDIUM

A11 – E-CARS AND E-BIKES: Including car monitoring system? Where loss of asset does not affect safety of user; *Value*: MEDIUM

A12 – HOME SECURITY SYSTEM: Home CCTVs; *Value*: MEDIUM

A13 – ENERGY MANAGEMENT SYSTEM: including energy sensors installed in the house...; *Value*: LOW

A14 – EXTERNAL RECOGNITION / MONITORING SYSTEM: Image or speech recognition [unknown to the participants]; *Value*: LOW

A15 – DATABASES OF AGGREGATED DATA: Residing in various data centres. Includes aggregated health data; *Value*: MEDIUM

A16 – DATA MINING PACK / SOFTWARE: e.g. online scripting package [in the scenario: Annika to mash-up pages pulled in all of Christer's various records]; *Value*: LOW

A17 – RECOMMENDATION SYSTEMS: Service /systems generating personalised recommendations to users; *Value*: MEDIUM

A18 – BIO-SENSORS / PERSONAL HEALTH DEVICES, SMALL SENSOR PATCHES, HEALTH DATA [USER END]: meaning, the devices themselves, not the data they collect; *Value*: HIGH

As mentioned in the methodology section above, the valuation of assets was based on the impact areas identified. The group agreed upon the following impact areas:

I1 – HEALTH / LIFE: Refers to the physical and psychological condition of an individual; his/her physical and psychological well-being and absence of disease.

I2 – HUMAN RIGHTS AND SOCIAL VALUES: include privacy, autonomy, non-discrimination, dignity, social inclusion, trusted human relationships, etc.

I3 – HUMAN AGENCY: refers to behaviour, socializing i.e. how we do things.

I4 – FINANCIAL / ECONOMICAL FACTORS: refers to cost considerations for companies and individuals

I5 – COMFORT, CONVENIENCE AND EASE OF ACCESS: refers to the extent to which services are provided and procedures followed without difficulties.

I6 – INTEROPERABILITY: refers to interoperability between networks, sensors, devices, organisations, and users that are central to the scenario.

I7 – TRUST: refers to trust established and maintained among individuals, processes, systems and stakeholders in general.

I8 – LEGAL: refers to legal considerations for companies and individuals.

The group assigned a weighting factor to the impact areas, ranging from *0.7* to *1*, depending on the importance for each impact area, we have identified. Please refer to Appendix II, the excel spread sheet for more information on the identification and assessment of the assets.

5.3 THE RISKS

Based on our detailed analysis which you can find in the excel spread sheet of Annex III (*Risk Assessment*" tab), we have identified a total of 1253 'individual' risks. We call an 'individual' risk each triplet identified, namely an Asset, Vulnerability and Threat unique association. Following the risk assessment methodology described in the previous chapter, each individual risk receives a value in the scale of 1 to 13, as presented in the table below.

Information Security Risk Measurement Scale												
Minimum Risk												Maximum Risk
1	2	3	4	5	6	7	8	9	10	11	12	13
VERY LOW		LOW			MEDIUM			HIGH			VERY HIGH	

All the individual risks identified were above 5 in this scale, and there was no risk of the maximum value of 13. The weighted average value of all individual risks is **9.25**, namely *High***.** It is noted however that there are individual risks that have been found as **Very High** [*Value 12*]; from the analysis we have performed, these individual Very High risks have been already linked with the following compound

risks that are presented in the next paragraphs, namely: **R1** , **R2** , **R5** , **R6** , **R7** , **R8** , **R9** , **R10** , **R11** , **R12** . More details on these individual "*Very High*" risks, you may find at the "*Risk Assessment*" tab of the excel spread sheet of Appendix II.

For presentation purposes as well as to provide for a better analysis, we have grouped the individual risks into 12 major risk areas that we consider the most important, namely:

R1 – Breach of privacy

R2 – Inappropriate secondary use of data

R3 – Malicious attacks on smart devices increase as their value to authenticate individuals and store personal data increases

R4 – Compliance with and enforcement of data protection legislation made more difficult

R5 – Discrimination and exclusion

R6 – Monitoring, cyber-stalking, child grooming and "friendly" surveillance

R7 – Unanticipated changes in citizens' behaviour and creation of an "obedient" citizen

R8 – Poor decision making / inability to make decisions

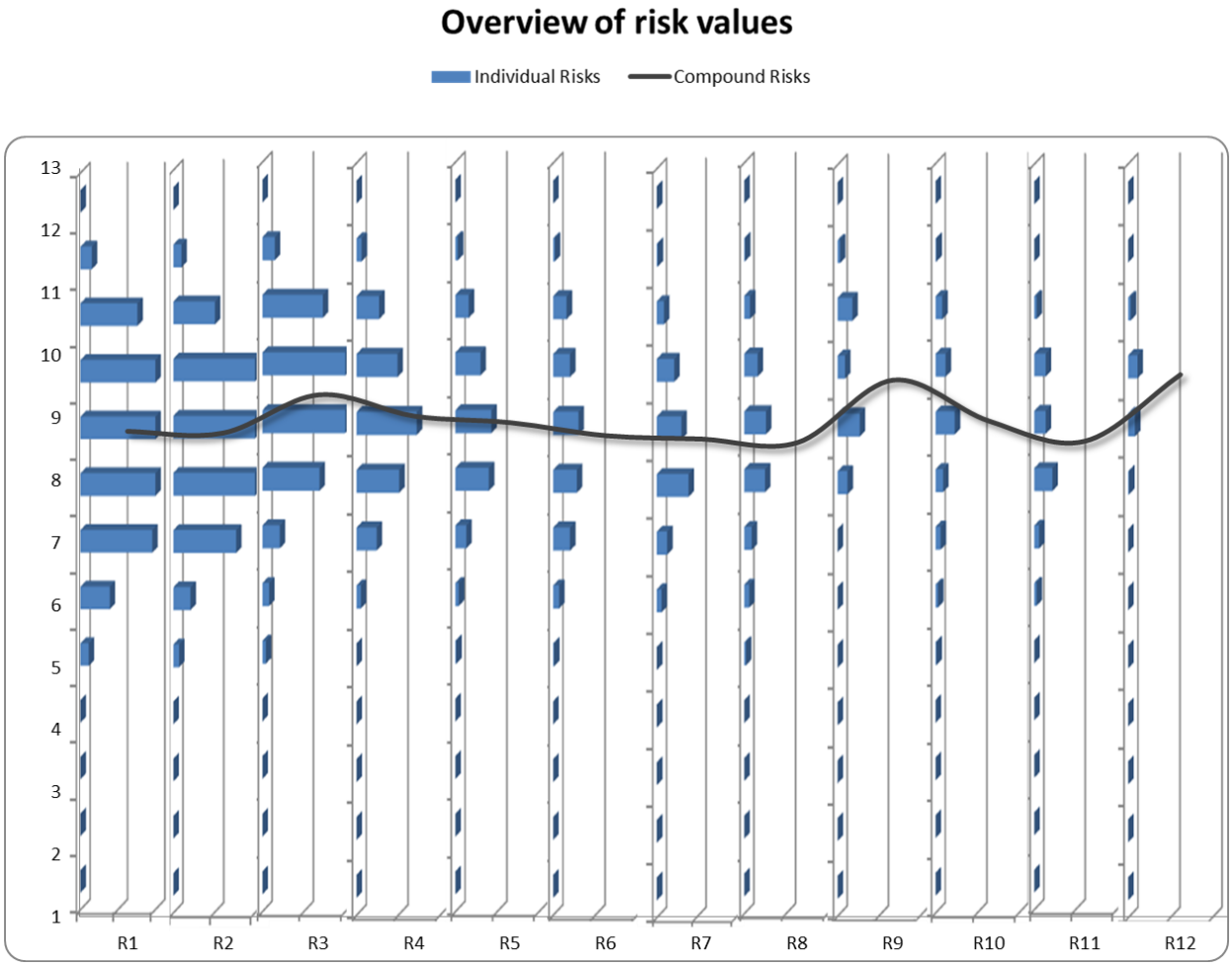
R9 – Psychological harm

R10 – Physical theft of property or private information from home environment

R11 – Reduction of choices available to individuals as consumers and user lock-in

R12 – Decrease of productivity

We call these "*compound*" risks, since they are formed by the individual risks, and we have calculated a weighted risk value for each one of these, so as to get an idea of the risk level of each one. We have seen that all these compound risks range from Medium to High, roughly within the values 8 to 10. These major risks have been then ranked according to their weighted average value and the amount of individual risks they represent, since the individual risks are not distributed evenly among the compound risks.



In the tables that follow, these risks are presented in detail and according to this ranking. In addition to a short description of the risk, the following items are identified for every risk in a table:

- **The affected assets** : as those have been identified in the previous section
- **The relative vulnerabilities and threats** the association of which generates the risk. For a detailed overview of the associations in the triplets "Asset-Vulnerability-Threat" please refer to Appendix II, the excel spreadsheet where the assessment was performed.
- **Reference to other risks**: most of the risks identified are highly inter-related, so specific reference to other relevant risks is made. Again you may click on the item to navigate to the corresponding risk inside the document.
- **Weighted risk level**: as mentioned above, since the risks identified here are a high level grouping of all the individual risks identified in our analysis (see the detailed analysis in the spreadsheet of Annex III), a weighted risk level is estimated and included in the risk description. It is noted that this weighted average risk level has been calculated for each compound risk in isolation of the

other compound risks; it is thus the case that risks with a High weighted average might be ranked lower than a compound risk of Medium, since also the amount of individual risks represented haven been considered in the ranking.

R1 – Breach of privacy

Affected assets	A1. Actors' digital presence not including social or professional reputation A2. Social reputation A3. Professional reputation A4. Sentiments A5. Ideas A6. Life-logging services A7. Social networking services A9. PC and home infrastructure A10. Smart phone / mobile phone / life-logging devices A15. Databases of aggregated data A16. Data mining pack / software
Vulnerabilities	V1 Flawed/insufficient design, implementation and/or capacity of devices and systems. Includes software bugs and design flaws. V2 Inadequate policy framework V3 Inadequate privacy/security interfaces (poor interface design) V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities V5 Inherent features of smart devices (size, material etc.) They may be easy to lose or to be stolen, oversensitivity of sensors (for example, leading to inaccuracies) V6 Lack of appropriate, common or harmonized legislation in EU Member States V8 Lack of or inadequate user identification, authentication and access controls; e.g. use of new devices as authentication tools V10 Over reliance and excessive dependency on electronic devices and systems V11 PC and home infrastructure vulnerabilities V12 Smart phone vulnerabilities [*regarding privacy legislation*] V13 Lack of revocation/correction/deletion mechanisms

	V14 Lack of (usable and appropriate) privacy controls V15 Lack of (usable) logging controls/policies/ reminders V18 Lack of noticeable (and usable) notification systems V19 Increased complexity of controls (making it difficult for users to follow) V20 Increase of (unprotected) data storage capacity in smart-devices V22 Lack of appropriate assurance procedures (e.g. third party audits) or enforcement of such, regarding the implementation of security controls, especially from the state, other regulatory and public authority V23 Lack of transparency and "social translucency" V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V27 Cognitive biases – Some people accept what they should not… V28 Data linkability / life-logging data can be aggregated with other data
Threats	T1 Accidental loss of device T2 Identity theft/ impersonation T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T4 Unintentional misuse , unauthorised disclosure, modification or destruction of individual's data T6 Malicious physical attacks (theft, vandalism, misuse, etc.) T7 Malicious (logical) attacks on devices and systems T8 Overhearing/recording logging/blogging activity T10 Spamming of users with ads and other non-solicited information; they can also use open, public information T11 Constrain consumer choices T12 Vested interests T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc T14 Individual being negligent, careless, making mistakes

	T15 Increased need for attention / social exposure T16 Changes in perception of privacy and / or privacy needs (especially from one generation to another) T17 Data mining and profiling (large-scale, excessive and/or inappropriate) T18 Monitoring and surveillance
Weighted average risk level	**MEDIUM**
Relevant Risks	**R2 R3 R5 R6 R9 R10**

A breach of privacy is a risk with several components given the nature of life-logging activities and services as set out in the scenario. The risks here are largely derived by the possible permanence of data. Privacy is a difficult and complex concept to define; in order to facilitate the analysis and presentation of this risk, we have been based on some widely accepted aspects of privacy, and examine

A traditional definition of privacy is the "**right to be let alone**"[15]. Life-logging could undermine this kind of privacy, because there may be considerable social pressure from peers to constantly mirror our personal activity. It may also be that peers (or colleagues) – while filling their own personal life-logs – indirectly share data about a person who does not want to participate.

A specific expression of privacy is **information privacy** and more specifically **"privacy as control over my personal data".**[16] Due to excessive data collection and subsequent aggregation of logs in personal profiles, as well as potentially inappropriate and uncontrollable secondary use of that data by life-logging service providers or peers, people can become victims of privacy breach. They cannot control who has access to or insight into their personal data. The "right to informational self-determination" is effectively lost. Powerful data warehouses may combine life-logging data from different sources and may be capable of profiling, which relies on accurate life-logs from various activities and capturing different aspects of life (location data, health information, purchase histories etc.). For example, ad networks are prone to develop in this direction where companies hand over life-logging data of their customers in exchange for participating in a powerful ad network which promises even better targeting.

[15] Warren, S.D., and Brandeis, L.D. 'The Right to Privacy', *Harvard Law Review*, Vol. IV, No. 5, 1890, pp. 193–220.

[16] Westin, A.F., *Privacy and Freedom*, Atheneum, New York, 1967.

There is also– as Solove points out[17]– a future **risk of abuse of information**. Such abuses can reside in false judgements that are made on the basis of the personal data collected. Behavioural targeting for marketing purposes based on probabilistically aggregated consumer profiles is a likely driver of false judgements on consumer preferences. Furthermore, the 'spill over' of personal data between life-logging services could lead to context violations [see also **R2**]. Users can hardly control these marketing practices.

Moreover, the "**two-sided market dynamics**" underlying online markets (including life-logging) drive the privacy risk: on one side, advertisers want to offer products and need to market those to the right target audience (behavioural targeting). On the other side, the target audience "logs" its interest profile. The "attention glue" between the two market sides is the personal information known to the online platform about prospective consumers. As a result, commercial operators continue to have strong incentives to collect the maximum amount of private data for unwanted secondary uses. Missing privacy controls, a lack of transparency about data use, lack of access to one's personal data and lack of change and revocation options aggravate this privacy risk.

Furthermore, the "**right to be forgotten**"[18] may be also lost: an individual might have a life-logging event on the web, which she might have deleted but it remains in some form due to its having being copied or posted elsewhere. This could have serious negative consequences for individuals: for example, an individual might apply for a position and prospective employers might have accessed their life-logging details.

Other elements in this risk include some individuals being recorded in life-logging activities without their **consent or knowledge**; however for additional information on consent, you may refer to risk **Error! Reference source not found.**.

Finally, **privacy vis-à-vis the state** is at risk. The state and the law enforcement agencies can access the vast material of personal logs. This is particularly dangerous when the information created is accessible to governments operating under different legal privacy regimes [see also **R4**].

[17] Solove, D.J., 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*, Vol. 154, No. 3, 2006, pp. 477–560.

[18] The '*right to be forgotten*' is not yet an established right; it is however an important privacy consideration and it is already explicitly mentioned in the EC Communication "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final.

R2 – Inappropriate secondary use of data

Affected assets	A2. Social reputation A3. Professional reputation A4. Sentiments A6. Life-logging services A7. Social networking services A10. Smart phone / mobile phone / life-logging devices A15. Databases of aggregated data
Vulnerabilities	V2 Inadequate policy framework V3 Inadequate privacy/security interfaces (poor interface design) V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities V6 Lack of appropriate, common or harmonized legislation in EU Member States V13 Lack of revocation/correction/deletion mechanisms V14 Lack of (usable and appropriate) privacy controls V15 Lack of (usable) logging controls/policies/ reminders. E.g. capturing some embarrassing scene of someone else or yourself V16 Lack of secure transmission and storage of data; also includes lack of (usable) transmission control (who gets the data) V17 Lack of mechanisms to validate reputation or trustworthiness of service provider V18 Lack of noticeable (and usable) notification systems V22 Lack of appropriate assurance procedures (e.g. third party audits) or enforcement of such, regarding the implementation of security controls, especially from the state, other regulatory and public authority V23 Lack of transparency and “social translucency” V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V27 Cognitive biases – Some people accept what they should not… V28 Data linkability / life-logging data can be aggregated with other data

Threats	T1 Accidental loss of device T2Identity theft/ impersonation T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T4 Unintentional misuse , unauthorised disclosure, modification or destruction of individual's data T6 Malicious physical attacks (theft, vandalism, misuse, etc.) T7 Malicious (logical) attacks on devices and systems T8 Overhearing/recording logging/blogging activity T12 Vested interests T14 Individual being negligent, careless, making mistakes T16 Changes in perception of privacy and / or privacy needs (especially from one generation to another) T17 Data mining and profiling (large-scale, excessive and/or inappropriate) T18 Monitoring and surveillance
Weighted average risk level	**MEDIUM**
Relevant Risks	**R1 R3 R6 R7 R9**

There are a number of elements to this particular risk.

- There is a risk of function creep whereby life-logging data may be used for purposes not explicitly stated in a services' terms and conditions. This may be compounded by context violations whereby information from one domain/context will "spill over" to another. The state might also engage in activities whereby it is using inappropriately aggregated databases. There is a risk of this from leakage of social data between legal jurisdictions and where data protection regulation might not be applied when national security is considered to be at stake.

- And particularly because life-logging data may be considered as a valuable commercial asset, it can contribute to the commoditisation of such information. As explained earlier in **R2 R5** , life-logging services may be also used to harvest life-logging data for secondary purposes, which they might also reveal consumption patterns and allow this to be used in unwanted ways, such as targeted marketing. The commoditisation is exemplified in the requirement to consent to the use of personal information, in order to use specific services and the consumer enticement to give up

personal information for the free use of services. In many instances offers to use life-logging services without any consent to secondary data uses are not available or on purpose not very attractive compared to the "free meal against data" option.

- Individuals might also accidentally place sensitive or highly confidential information on the Internet. This might have value in a number of illicit contexts such as criminal activities, terrorism, harassment or reputational harm, for example, when individuals have forgotten about life-logging data from past times in their lives.

R3 – Malicious attacks on smart devices (phones and home devices) increase as their value to authenticate individuals and store personal data increases

Affected assets	A1. Actors' digital presence not including social or professional reputation A2. Social reputation A3. Professional reputation A6. Life-logging services A8. Smart home objects / appliances A9. PC and home infrastructure A15. Databases of aggregated data A17. Recommendation systems
Vulnerabilities	V1 Flawed/insufficient design, implementation and/or capacity of devices and systems. Includes software bugs and design flaws V3 Inadequate privacy/security interfaces (poor interface design) V5 Inherent features of smart devices (size, material etc.) V8 Lack of or inadequate user identification, authentication and access controls V9 Lack of third party system reviews and software integrity certification V10 Over reliance and excessive dependency on electronic devices and systems V11 PC vulnerabilities V12 Smart phone vulnerabilities V15 Lack of (usable) logging controls/policies/ reminders V16 Lack of secure transmission and storage of data; also includes lack of (usable) transmission control (who gets the data) V20 Increase of (unprotected) data storage capacity in smart-devices

	V21 Reliance on legacy, un-patched systems or integration mistakes V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V28 Data linkability / life-logging data can be aggregated with other data
Threats	T1 Accidental loss of device T2 Identity theft T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T6 Malicious physical attacks (theft, vandalism, misuse, etc.) T7 Malicious (logical) attacks on devices and systems T8 Overhearing/recording logging/blogging activity T9 Exploring new 'vulnerabilities' in the new app T14 Individual being negligent, careless, making mistakes T17 Data mining and profiling (large-scale, excessive and/or inappropriate) T18 Monitoring and surveillance
Weighted average risk level	**HIGH**
Relevant Risks	**R1 R2 R3 R6 R10**

Smart devices, such as a person's smart phone or the main home computer or home server, will become more attractive targets for attackers. If these systems are not built with a view to the highest security standards, the smart devices of the future will suffer from the ubiquity of malware that we are witnessing today on most Windows PCs and beyond.

As dependability on the availability of devices is increasing, the effects of malicious attacks are increasingly serious.

ENISA has recently conducted a detailed study on information security and privacy risks of smart phones[19]. Since the focus of this study is life-logging, the group didn't consider it appropriate to drill down on the specific vulnerabilities and threats of smart phones, especially since this has already been

[19] Hogben, G., Dekker, M. (eds.), *Smartphones: Information security risks, opportunities and recommendations for users*, European Network and Information Security Agency (ENISA), 2010.

performed in the context of another ENISA study. Based on this study, in our analysis we have considered the vulnerabilities for 'smart phones' that have been identified therein [for more information please refer to "*V12 Smart phone vulnerabilities*" in Annex I.

Considering the above and the fact that the amount of data being collected and exchanged is quite high in the life-logging environments, smart phones used to life-log present an even more attractive target for attackers, thus increasing their motivation. A successful malicious attack against a smart phone would lead to the increase of various other risks, such as disclosure of personal data, impersonation and surveillance, as well as risks identified below. It is evident that all these risks are highly inter-connected, one generating another.

R4 – Compliance with and enforcement of DP legislation made more difficult

Affected assets	A2. Social reputation A3. Professional reputation A4. Sentiments A6. Life-logging services A7. Social networking services A15. Databases of aggregated data
Vulnerabilities	V2 Inadequate policy framework V3 Inadequate privacy/security interfaces (poor interface design) V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities V6 Lack of appropriate, common or harmonized legislation in EU Member States V7 Lack of interoperability between devices/ services/ technologies and/or systems V8 Lack of or inadequate user identification, authentication and access controls V9 Lack of third party system reviews and software integrity certification V10 Over reliance and excessive dependency on electronic devices and systems V13 Lack of revocation/correction/deletion mechanisms V14 Lack of (usable and appropriate) privacy controls V15 Lack of (usable) logging controls/policies/ reminders V16 Lack of secure transmission and storage of data; also includes lack of (usable) transmission control (who gets the data)

	V17 Lack of mechanisms to validate reputation or trustworthiness of service provider V22 Lack of appropriate assurance procedures (e.g. third party audits) or enforcement of such, regarding the implementation of security controls, especially from the state, other regulatory and public authority V23 Lack of transparency and "social translucency" V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V26 Psychological vulnerability (low self-esteem and confidence to self, high influence potential by others, naïve and suggestible, etc ; weak perception of self V28 Data linkability / life-logging data can be aggregated with other data
Threats	T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T4 Unintentional misuse , unauthorised disclosure, modification or destruction of individual's data T8 Overhearing/recording logging/blogging activity T9 Exploring new 'vulnerabilities' in the new applications T12 Vested interests T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc T14 Individual being negligent, careless, making mistakes; e.g. does not follow procedures appropriately, e.g. clicks through T17 Data mining and profiling (large-scale, excessive and/or inappropriate) T18 Monitoring and surveillance
Weighted average risk level	**HIGH**
Relevant Risks	**R1 R2 R7**

Although a new European data protection legal framework has been adopted at the time when the scenario is taking place, which aims at coping with technological challenges (among which life-logging), [see assumption …] specific issues raised by logging render the compliance with this framework, as well as its efficient enforcement difficult at specific instances.

The application of the European data protection is challenged as regards the specification of the person who serves as 'data controller' for life-logging activities. The determination of the data controller is of great importance as she exercises the decision making both on the purposes for which personal data are collected and processed, as well as on the means to be used for a specific processing. Life-logging facilitates interactive information sharing and collaboration between various actors over social networking sites, who do not always fit in the traditional communications models.

Life-logging activities are based on the instant processing and sharing of information. The scenario clearly demonstrates the risk of being recorded in life-logging activities without one's consent or knowledge (for example, where an individual is life-logging within public spaces), as occurs when Annika's colleague is caught picking his nose. Although, it could be feasible to require consent from individuals before information related to them is shared, it still may be rather challenging; it may be in contrast with the very nature of life-logging applications[20].

Moreover, difficulties in the enforcement of the European data protection legal framework arise in relation to international services, which do not offer standard data protection control interfaces that would allow for a similar level of privacy protection worldwide and for a level of protection that is consistent with all the regional legislations. European governments have in practice limited power to enforce their citizens' rights vis-à-vis such foreign data processors.

Compliance with regional legislation is a costly challenge for globally active platform operators that many do not want to address. A risk of lack of compliance at the country level is increased with the lack of privacy audits and sanctions for breach of data protection. The staff required to investigate a companies' privacy practices is costly and rare. As a result, most privacy breaches today already go unnoticed. At the same time, sanctions for privacy breach are so low that companies can risk their revelation in many cases.

[20] Some references on this challenge:
O'Hara, K., Tuffield, M.M., Shadbolt, N., 'Lifelogging: Privacy and Empowerment with Memories for Life', *Identity in the Information Society*, Vol. 1, pp. 155–172, Springer, 2009.
Allen, A.L., 'Dredging up the past: Life-logging, Memory, and Surveillance', *The University of Chicago Law Review*, Vol. 75, No. 1, 2008, pp. 47–75.

R5 – Discrimination and exclusion

Affected assets	A1. Actors' digital presence not including social or professional reputation A2. Social reputation A3. Professional reputation A4. Sentiments A5. Ideas A6. Life-logging services A7. Social networking services A8. Smart home objects / appliances A9. PC and home infrastructure A10. Smart phone / mobile phone / life-logging devices
Vulnerabilities	V2 Inadequate policy framework V3 Inadequate privacy/security interfaces (poor interface design) V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities V14 Lack of (usable and appropriate) privacy controls V15 Lack of (usable) logging controls/policies/ reminders V19 Increased complexity of controls (making it difficult for users to follow) V23 Lack of transparency and "social translucency" V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness, i.e. in which context the data should be used V26 Psychological vulnerability (low self-esteem and confidence to self, high influence potential by others, naïve and suggestible, etc ; weak perception of self V28 Data linkability / lifelogging data can be aggregated with other data
Threats	T11 Constrain consumer choices T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc; T14 Individual being negligent, careless, making mistakes; e.g. does not follow

	procedures appropriately, e.g. clicks through T17 Data mining and profiling (large-scale, excessive and/or inappropriate)
Weighted average risk level	**MEDIUM**
Relevant Risks	**R1 R2 R6 R7 R9 R11**

As life-logging data can reveal sensitive and personal information, and through various services can be made accessible to a wide range of individuals or organizations, there is a significant risk that individuals might be subjected to discrimination and exclusion as a result of the content of their life-logging data. Specific risks here might, for example, include disclosure of sexuality, particular preferences or political affiliations. It may create a risk associated with the review of an individual's past that could be used unfairly, especially if the individual no longer engages in particular behaviour or activity.

Several forms of discrimination can result from life-logging services. One is that people who do not participate in life-logging may be sanctioned offline. For example, participation in online traffic services could allow for free service delivery of traffic news in the real world. If the individual is reluctant to share location data, she may be forced to pay for the traffic news that others get for free. Thus, financial loss or even service exclusion could result from a reluctance to share personal data logs.

Furthermore, one could encounter direct discrimination from peers who are annoyed that he/she won't share personal life-logging data with them. Another aspect of social discrimination may occur as a result of profiling; life-logging might provide more opportunity to public and private sector to profile the citizens / customers, something which we see already with the use of social networking applications, but which with the use of life-logging will be further intensified. There is thus a risk that citizens are discriminated based on these profiles that may present financial status, various preferences, sexual orientation[21] and behaviour. In the insurance sector, life-logging data may also result in discriminations against people who carry a health risk and slowly undermine the collective risk insurance approach to an individual risk insurance system.

Moreover, as mentioned as a benefit in section 3 of this report, price-discrimination presents a major incentive for companies enabled by life-logging information. At the same time, however, it poses the

[21] For example, the "Gaydar" study conducted at MIT that resulted in a method for accurately predicting the sexual orientation of Facebook users by analyzing friendship associations [Jernigan, C., and Mistree, B. F.T., 'Gaydar: Facebook friendships expose sexual orientation', *First Monday*, Vol. 14, No. 10, 2009]. In addition, there have been reports about series of suicides of teenage homosexuals who had been outed against their will (by posting videos to youtube): http://www.thefirstpost.co.uk/69352,people,news,gay-student-suicide-after-sex-video-posted-on-web-tyler-clementi-dharun-ravi-molly-wei

risk that individuals may not get the same offer for exactly the same product or service, just because their personal profile, derived inter alia from life-logging data, suggests that price discrimination strategies are successful. Some consumers may not receive an offer at all because they are considered unworthy or bad customers judged solely from their personal profiles, and be thus discriminated.

Another aspect of discrimination and exclusion has to do with victimisation. There is a risk that wide-spread proliferation of life-logging devices might be harmful in some settings for those who do not wish to participate in the sharing of life-logging data. For example, within organizations, use of life-logging devices might be seen as being important in relation to benefiting from particular corporate procedures, as shown in the scenario where Annika uses the corporate "*Getting Work Done*" application. Individuals who do not participate in these types of life-logging activities might be excluded due to distrust by other members of the organisation. In order to avoid this stigmatisation, this may result in a subtle pressure to conform; thus, life-logging data applications in certain sectors, even if implemented on a voluntary basis, may become pervasive and difficult to evade (see also **R7**).

In addition victimisation may result in situations where life-logging is seen as being part and parcel of membership of particular peer groups. Individuals who do not participate in life-logging activities in this instance might be excluded and viewed in a negative light by other members of the peer group. Furthermore, as the creation of digital traces become mainstream, non-participation may be regarded with suspicion. Life-logging may be used as a means to prove one's whereabouts which might cast a shadow on those who do not wish to share information about where they are or were.

R6 – Monitoring, cyber-stalking, child grooming and "friendly" surveillance

Affected assets	A1 Actors' digital presence not including social or professional reputation A4 Sentiments
Vulnerabilities	V3 Inadequate privacy/security interfaces (poor interface design) V14 Lack of (usable and appropriate) privacy controls V15 Lack of (usable) logging controls/policies/ reminders V16 Lack of secure transmission and storage of data; also includes lack of (usable) transmission control (who gets the data) V19 Increased complexity of controls (making it difficult for users to follow) V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V26 Psychological vulnerability (low self-esteem and confidence to self, high influence potential by others, naïve and suggestible, etc ; weak perception of self)
Threats	T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T8 Overhearing/recording logging/blogging activity T12 Vested interests T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc; T14 Individual being negligent, careless, making mistakes; e.g. does not follow procedures appropriately, e.g. clicks through T16 Changes in perception of privacy and / or privacy needs (especially from one generation to another) T17 Data mining and profiling (large-scale, excessive and/or inappropriate) T18 Monitoring and surveillance
Weighted average risk level	**MEDIUM**
Relevant Risks	**R1 R2 R3 R5 R7 R9 R12**

Risks posed by excessive surveillance and monitoring are not new: it certainly holds true for today's society as well. However, in a life-logging environment the abundance and the nature of the data shared and exchanged increases of this risk.

As identified in the respective threat, monitoring and surveillance can be performed by three different threat agents / stakeholders (individuals, companies / private sector, state) assuming thus different aspects[22]:

- **The state / Governments** need to collect, process and store citizens' personal data in order to provide better public services or tackle tax evasion, and for national security purposes. Indeed, "the risk society requires surveillance as a way of managing risk"[23]; however, it does pose great risks for individuals [see also **R1** and **R7**]

- **Private sector** may use life-logging data, in order to be able to provide more personalised services to customers, as well as to deal with customer churn. However, consistent monitoring of their clients activities does present a risk for individuals. The same as with the case of monitoring one's employees: in our scenario, Annika's professional life-logging activities are recorded by her employer. Workplace surveillance is a serious issue for individuals.

- **Individuals**, such as peers, friends or family (for the case of monitoring and surveying minors please look below) may monitor an individual's activity constantly out of interest that may develop into an obsession and generate problems for the individual [see also **R12**]. Moreover, malicious users may be after our identity information to perform various fraudulent activities.

In addition, as the digital presence on life-logging service platforms becomes a permanent mirror of one's personal life, a "digital garden" is created where one can find instances of tracking, persecution and stalking like those sometimes found in the offline world. Stalkers from the offline world could intrude in one's online world (e.g., by publicly commenting or just following over a longer period of time, thereby breaching the "right to be [digitally] let alone"). Anonymous stalkers could secretly follow one's activities (depending on available privacy settings). Advertisers could continuously survey and analyse one's preferences.

Cyberstalking is the graver variation of online harassment which describes an extreme form of online pursuit involving repeated harassment, malicious threats online and can cumulate in compromising the victim's personal details in order to cause psychological and physical distress. In many EU countries it is punishable as a criminal offence either by meeting the definition of harassment or by making reference to electronic communications as a way of committing the crime. Perpetrators who may have

[22] Daskala, B, Maghiros, I., *D1gital Territ0ries - Towards the protection of public and private space in a digital and Ambient Intelligence environment*, JRC Technical and Scientific Report, EUR 22765 EN, 2007.

[23] Regan, P. M., 'Privacy as a common good in the digital world', *Information, Communication & Society*, Vol. 5, No. 3, pp. 382–405.

access to their victim's life-logging data because they belong to their social sphere or gain unauthorised access can abuse the information for their threats. In the worst case scenario the stalking moves offline and the victim will be physically harassed which may be aided by intimate knowledge about the routines, whereabouts and movements of the victim.

CHILD GROOMING

We would like to focus a bit more on this risk in the case when data is generated by children. There are risks associated with individuals being able to pretend to be someone who they are not through manipulation of data and there is a risk that individuals might be able to manipulate minors or other vulnerable persons into recording life-logging data which is wholly inappropriate (an example of which is the emergence of "sexting"[24]).

Life-logging data if accessible to a malicious individual can be abused to commit criminal offences against the linked individuals with potentially severe consequences, notably child grooming and cyber-stalking. Such crimes are especially concerning where the threat moves offline facilitated by the particular knowledge certain life-logging data sets may convey about the whereabouts, movements and routines of the victims.

Child grooming involves gaining the victim's trust through contact and interaction online which may be aided by certain information which are automatically shared or voluntarily posted and inform about the child's interests and whereabouts.[25] Perpetrators may be able to access school networks, social networks or simply certain data feeds which are not adequately secured and shielded from unauthorised access. Child grooming is a crime against minors and in a number of EU Member States (*e.g.* Denmark, France, Netherlands, Spain and UK) already made punishable as sexual solicitation in line with the Convention of the Council of Europe on the Protection of Children against Sexual Exploitation (CETS 201).[26] A recent OECD report summarises available empirical data about the risks for children, which shows that the reality of online sexual solicitation is complex and that real world

[24] Sexting can be described as "*the sending or forwarding nude, sexually suggestive, or explicit pictures on a cell phone or online*": Siegle, D., 'Cyberbullying and Sexting: Technology abuses of the 21st Century', *Gifted Child Today*, Vol. 33, No. 2, 2010, p. 14 (15); Richards, R. and Calvert, C., 'When sex and cell phones collide: inside the prosecution of a teen sexting case', *32 Hastings Comm. & Ent, L.J. 1*, 2009, pp. 1–3. See also Lenhart, A., 'Teens and Sexting. How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging', *Pew Internet & American Life Project*, 2009.

[25] According to the risk scenario Freia who can be tracked via her avatar on the school network's social site which is accessible to other pupils, parents and teachers, which makes it semi-public already.

[26] Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.: 201, Lanzarote, 25.10.2007, Art. 23.

physical sexual encounters as a consequence are rare.[27] Notwithstanding, the risk where it materialises is very grave.[2829]

It is worth noted here that the same risks can be identified for vulnerable persons at large, not only kids. Plenty of adults groom one another for malicious intentions (usually involving sex and/or money). This is one of the problems when online dating sites are abused. It finally boils down to an abuse of power and attempt to assert power over a vulnerable person.

"FRIENDLY" SURVEILLANCE

On the other side of the spectrum is the risk of disproportionate and excessive "friendly surveillance" relying on life-logging data which may nevertheless infringe children's own right to privacy[30]. In the family context, parents may wish to monitor their children's whereabouts[31], which is already possible today via "track your kids" functions of the mobile phone; and the technology will mature further powered by life-logging. Existing parental control technologies can already produce detailed reports on children's online activities[32] which is likely to expand across platforms (mobile phones and other Internet enabled devices) and linked to additional data sources (school network, social networks, etc.). Besides, life-logging data may enable even further analytics where various data feeds are correlated and analysed, which parents may want to use in order to monitor the performance and social environment of their children.[33] In addition, schools or libraries embark on monitoring children to maintain attendance records[34] or as part of a cyber-safety strategy. Children's privacy is at risk under

---

[27] 'The Protection of Children Online: Risks faced by children online and policies to protect them', *OECD Digital Economy Papers*, OECD, No. 179, Para 72.

[28] In the scenario, Freia can be tracked via her avatar on the school network's social site which is accessible to other pupils, parents and teachers, which makes it semi-public already.

[29] For an additional more detailed study on the risks regarding cyber-bullying and online grooming, as a result of excessive data mining and profiling, you can also refer to: Marinos, L. (ed.), *Cyber-bullying and online grooming: helping to protect against the risks – A scenario on data mining / profiling of data available on the internet*, European Network and Information Security Agency (ENISA), 2011 [forthcoming].

[30] Marwick, A., Murgia-Diaz, D. and Palfrey, J. (2010), Youth, Privacy and Reputation (Literature Review), Berkman Center Research Publication No. 2010-5, pp. 14, 16.

[31] In the scenario, Annika and Bennie have access to their 14-year-old daughter Dana's location data with her consent.

[32] In the scenario, Annika, the mother, monitors Christer's online playing time.

[33] In the scenario, Annika uses a convenient online scripting package to create a small set of mash-up pages which pull in all of her children's various records into a convenient two-page report.

[34] In the scenario, Dana and Christer's school requires class check-in, a service that they have to use in order to comply with attendance

this "privacy protection paradox"[35] posed by "friendly surveillance", and this trend may well spill over to "assist" the elderly and seriously ill persons, to monitor spouses and partners[36], and finally in the employment relationship. The challenge is threefold: (1) technology must be designed to cater for the essential functionalities provided that monitoring and surveillance are justified, proportionate and kept to the minimum as well as that (2) such schemes comply with statutory privacy protection frameworks and guidance issued, notably that there is positive knowledge and consent by the individual concerned. (3) There should be certainly realms where the use of life-logging data is strictly limited or even prohibited (e.g. for certain insurance in employment relationships).

R7 – Unanticipated changes in citizens' behaviour and creation of an "obedient" citizen

Affected assets	A1. Actors' digital presence not including social or professional reputation A4. Sentiments A5. Ideas A6. Life-logging services A10. Smart phone / mobile phone / life-logging devices A15. Databases of aggregated data
Vulnerabilities	V2 Inadequate policy framework V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities V6 Lack of appropriate, common or harmonized legislation in EU Member States V17 Lack of mechanisms to validate reputation or trustworthiness of service provider V19 Increased complexity of controls (making it difficult for users to follow) V23 Lack of transparency and "social translucency" V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness

[35] 'The Protection of Children Online: Risks faced by children online and policies to protect them', *OECD Digital Economy Papers*, OECD, No. 179, Para 72.

[36] See The Social Graph: "Facebook Is Now Leading Source of Evidence in Divorce Cases". Thursday, March 10, 2011. Available at http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=146421&nid=124595

	V27 Cognitive biases – Some people accept what they should not… V28 Data linkability / lifelogging data can be aggregated with other data
Threats	T10 Spamming of users with ads and other non-solicited information; they can also use open, public information T11 Constrain consumer choices T12 Vested interests T13 Peer-pressure and social pressure to conform and constantly share data; fear of violent response / or ridicule from peers, friends etc T14 Individual being negligent, careless, making mistakes; e.g. does not follow procedures appropriately, e.g. clicks through T15 Increased attention deficit disorder T16 Changes in perception of privacy and / or privacy needs (especially from one generation to another) T17 Data mining and profiling (large-scale, excessive and/or inappropriate) T18 Monitoring and surveillance
Weighted average risk level	**MEDIUM**
Relevant Risks	**R1 R2 R5 R6 R8 R9 R5 R11 R12**

There is a risk that a proliferation of life-logging activities and data generated from these will lead to too much monitoring and surveillance (see also **R6**). There is also the risk of a loss of autonomy for individuals through the creation of an "obedient" citizen, including the conformity stemming from social pressure in the use and sharing of life-logging data. There are risks also to changes in perception of privacy, addiction to life-logging, individuals being dependent on carrying life-logging devices, fears of data leakage which may lead to psychological and social harms for individuals, both those using life-logging devices, as well as services and those who do not use such services.

There are thus several ways in which citizens' behaviour could change in a negative way. One is that people may feel a need to be "obedient". In order to best understand this, it is helpful to draw upon the example of the Panopticon, an envisaged prison building, designed by Jeremy Bentham, a philosopher and social theorist, in the late 18th century.[37] Through a central observing tower in the middle of the prison, this architecture aimed to create the notion among prisoners that they were

[37] Bentham J. , Bozovic M (ed), *The Panopticon writings*, Verso, London, 1995, pp. 29–95.

being constantly observed. And this notion persisted regardless of whether guards were really observing them from the tower or not. Life-logging applications and services risk creating an analogous effect: because there is the notion that "others" are constantly observing one's own life-logging activity, people may feel forced to participate in the service(s) on a regular basis. In order to please, they may be driven into mimicking a specific image or display an opportunistic public image. Feared publicity of abnormal behaviour could lead to increased obedience and a perceived lack of autonomy. This may turn into a variation of the so-called "chilling effect", which refers to the concern that constitutionally protected freedom of information will be inhibited by the potential of individuals and authorities to engage in forms of post hoc surveillance of search data and may deter users from searching, receiving and imparting information.[38]

A very different change in behavior could reside in service addiction. Already today, studies suggest that many users become addicted to the use of their mobile devices and show withdrawal symptoms when asked to put their devices aside. As life-logging becomes an ever more integral part of our activities, there exists a risk of an unknown degree of dependability and addiction to the services.

There is a risk that widespread use and proliferation of life-logging devices in public, as well as private spaces might result in loss of solitude and contemplation time of individuals; individuals may have less time to be alone or to engage in certain activities if they fear that some device or someone might be recording them without their consent.

R8 – Poor decision-making / inability to make decisions

Affected assets	A4. Sentiments A6. Life-logging services A8. Smart home objects / appliances A17. Recommendation systems
Vulnerabilities	V1 Flawed/insufficient design, implementation and/or capacity of devices and systems. V2 Inadequate policy framework V3 Inadequate privacy/security interfaces (poor interface design) V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities

[38] Wood D.M. (ed.), *A report on the surveillance society for the (UK) Information Commissioner*. Surveillance Studies Network, 2006.
Kosta, E., Kalloniatis, Chr., Mitrou L., Kavakli E., 'The "Panopticon" of Search Engines: The Response of the European Data Protection Framework', *Requirements Engineering*, Vol.16, 2011, pp. 47–54.

	V6 Lack of appropriate, common or harmonized legislation in EU Member States V17 Lack of mechanisms to validate reputation or trustworthiness of service provider V19 Increased complexity of controls (making it difficult for users to follow) V23 Lack of transparency and "social translucency" V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V27 Cognitive biases – Some people accept what they should not…
Threats	T10 Spamming of users with ads and other non-solicited information; they can also use open, public information T11 Constrain consumer choices T12 Vested interests T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc T14 Individual being negligent, careless, making mistakes; e.g. does not follow procedures appropriately, e.g. clicks through T16 Changes in perception of privacy and / or privacy needs (especially from one generation to another) T17 Data mining and profiling (large-scale, excessive and/or inappropriate)
Weighted average risk level	**MEDIUM**
Relevant Risks	**R2 R4 R5 R11**

Data gained through life-logging devices may be used in decision support systems. For example, people already today get driving instructions through their navigation systems based on their movement data. In the long run, a ubiquitous use of such services could lead to a lack of personal skill development as people get used to rely on the availability of services and are not used to make their own judgements. This risk is therefore related to a strong degree of personal dependence.

There is even a debate that such decision support systems that originally have the goal to broaden the consumer's decision possibilities could – in the end – result in less choices because any decision can be tagged with the related cost. For instance, to pick up the car navigation examples, traffic streams could

be manipulated top-down in order to optimise the traffic flow and the option to use a specific road could be made highly unattractive, thus limiting the choice of the car driver[39] [see also **R11**].

There is also a risk that the judgements made by machines are not optimal or are biased. Simplistic routines and algorithms, i.e., for the personalisation of life-logging services, may lead to suboptimal information search and information display as well as less good decision-making as a result. Early examples of personalisation mechanisms, such as Amazon's book suggestions, Google's 'Social Search' functionality [where you can see recommendations from your contacts using the same functionality], YouTube's recommended videos or Facebook's news feed prioritisation– despite their virtues – show how easy it is for people to be trapped into 'personalised information silos' that they cannot or do not control. The concern is basically that people might not realise that all recommenders provide filtered information, and they may fail to explore alternative sources. This impacts their choices and decisions and may seriously affect their ability to make informed decisions.

[39] Weyer, J., 'Die Zukunft des Autos – das Auto der Zukunft. Wird der Computer den Menschen ersetzen?', Soziologische Arbeitspapiere 14, *Wirtschafts- und Sozialwissenschaftliche Fakultät*, Universität Dortmund, Dortmund, 2006

R9 – Psychological harm

Affected assets	A2 Social reputation A3 Professional reputation A4 Sentiments
Vulnerabilities	V15 Lack of (usable) logging controls/policies/ reminders V23 Lack of transparency and "social translucency" V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V26 Psychological vulnerability (low self-esteem and confidence to self, high influence potential by others, naïve and suggestible, etc ; weak perception of self
Threats	T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T8 Overhearing/recording logging/blogging activity T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc; T14 Individual being negligent, careless, making mistakes; e.g. does not follow procedures appropriately, e.g. clicks through T15 Increased attention deficit disorder T16 Changes in perception of privacy and / or privacy needs T18 Monitoring and surveillance
Weighted average risk level	**HIGH**
Relevant Risks	**R2 R5 R6 R7 R8**

There are a number of elements to the risk of psychological harm to individuals as a consequence of the use and proliferation of life-logging devices and services in different contexts. For example within organisational settings linking performance data life-logging services might lead to pressures on individuals in respect of work performance which in turn might lead to feelings of inadequacy especially where life-logging data might be shared across the workplace and viewable by peers other employees or the employer. Psychological harm might also be the result of inappropriate sharing of life-logging data or inappropriate accessing of life-logging data that might involve a loss of reputation in both social and professional settings.

The risk of psychological harm can stem from several sources:

- One is that online peers may post undesirable information about oneself. Today, this phenomenon already exists on Facebook where images of one's being drunk at a party can not only cause negative perceptions among third parties seeing them, but also result in a personal perception of harm.

- Another source of personal harm may be one's own personality development and mental health. It may be that the identity of a person being consciously logged today is viewed with regret in the future. If a data subject cannot delete life-logging data, then "looking back" may become an exercise of great personal annoyance. A very characteristic example of this is the recent film project "The Marina experience", in which Marina Lutz expresses in her own way her traumatic experience by having all her moments, even the most intimate, filmed for the first 16 years of her life, exposing her father's "voyeurism, his latent paedophilia, his bullying, coercive nature, his pathological narcissism"[40]. There is a risk that social media and the way it is used would often "require and invite an almost compulsive photographic capturing of the self"[41].

- Life-logging data may create a high degree of transparency for offline activity; it may enable the benchmarking of performance or competitive actions. However, such information could cause intensified competitiveness in groups within society. Equally, "voluntary" routine monitoring by employers could be aimed at improving group performance, but also lead to psychological harm among those who do not meet peer expectations.

- Besides, watching other people's life-logs may develop into an obsession, to be envious of someone else's life and to feel lacking and not accomplished enough in comparison: "peering into the lives of your peers is making people look at themselves, and some aren't happy with what they see"[42].

---

[40] "Marina Lutz interview: The sins of my father", Louise Carpenter, The Observer, 17 April 2011. Available at: http://www.guardian.co.uk/artanddesign/2011/apr/17/photography-children. Also see: http://www.themarinaexperiment.com/category/the-marina-experiment/

[41] Id.

[42] "Study shows some suffer from 'Facebook envy'", February 3, 2011 http://news.cnet.com/8301-1023_3-20030550-93.html#ixzz1KxrC2GdE

R10 – Physical theft of property or private information from home environment

Affected assets	A4. Sentiments A8. Smart home objects / appliances A11. e-cars and e-bikes A12. Home security system A13. Energy management system
Vulnerabilities	V2 Inadequate policy framework V3 Inadequate privacy/security interfaces (poor interface design) V5 Inherent features of smart devices (size, material etc.) V8 Lack of or inadequate user identification, authentication and access controls V10 Over reliance and excessive dependency on electronic devices and systems V13 Lack of revocation/correction/deletion mechanisms V15 Lack of (usable) logging controls/policies/ reminders V20 Increase of (unprotected) data storage capacity in smart-devices V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness V28 Data linkability / life-logging data can be aggregated with other data
Threats	T1 Accidental loss of device T2 Identity theft/ impersonation T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data T5 Intermittent or no connectivity T6 Malicious physical attacks (theft, vandalism, misuse, etc.) T10 Spamming of users with ads and other non-solicited information; they can also use open, public information T11 Constrain consumer choices T12 Vested interests

	T14 Individual being negligent, careless, making mistakes
Weighted average risk level	**MEDIUM**
Relevant Risks	**R1 R3 R4**

While the scenario assumes that a large amount of data is stored online and remotely, there remains a risk that life-logging data might be compromised in particular where devices are stored in the home environment. Simple physical theft of these devices might have a number of impacts on individuals depending on the specific nature of data stored on devices and how secure this data is made by individuals in utilising security features in their devices. Loss of data might result in individual's identities being stolen, individuals being subject to financial fraud or blackmail, as well as other risks from loss of personal or sensitive data stored on devices. An obvious related risk is that of goods being stolen from home because the burglars find out that the owners are not at home, based on their compromised life-logs or wrongly set access control policies for their life-logs and location information.[43]

R11 – Reduction of choices available to individuals as consumers and user lock-in

Affected assets	A1. Actors' digital presence not including social or professional reputation A5. Ideas A6. Life-logging services A7. Social networking services
Vulnerabilities	V2 Inadequate policy framework V6 Lack of appropriate, common or harmonized legislation in EU Member States V7 Lack of interoperability between devices/ services/ technologies and/or systems V17 Lack of mechanisms to validate reputation or trustworthiness of service provider V24 Social reliance/over-confidence and trust on individual's digital identity V25 Inadequate user education, lack of awareness and training particularly in security

[43] See for example: http://pleaserobme.com/ and "*Social networking: Are you advertising your home to burglars?*" http://www.telegraph.co.uk/finance/personalfinance/insurance/8331387/Social-networking-Are-you-advertising-your-home-to-burglars.html or "*Burglars used social network status updates to select victims*" http://www.theregister.co.uk/2010/09/13/social_network_burglary_gang/

	and privacy; lack of context awareness V27 Cognitive biases – Some people accept what they should not…
Threats	T10 Spamming of users with ads and other non-solicited information; they can also use open, public information T11 Constrain consumer choices T12 Vested interests
Weighted average risk level	**MEDIUM**
Relevant Risks	**R4 R5 R7 R8**

The scenario assumes new automations in how people might conduct everyday activities such as shopping or new ways of purchasing services; it also assumes situations where targeted advertisements have reached new levels of sophistication due to advertisers being able to take advantage of life-logging data, often with the users' consent in order to take advantage of discounts or to access certain services. There is a risk, however, that those individuals might become locked into services; automated decision-aiding services might restrict user choice by tying them to particular service providers or sponsors associated with these service providers.

The economics of the Internet with its inherent "Winner-takes-all" tendency (at any given time, except during transitions in popularity), as well as life-logging services' reliance on positive network effects make likely an oligopolistic market structure among those firms that offer life-logging services. Thus, one or a few globally active platform providers may become hubs for life-logging activity in general. A good early example is today's Facebook, with an impressive amount of 600 million active users.

In such a market structure, the platform provider of choice exercises considerable power, because users of the service are de facto "locked in": They cannot switch easily to another network without incurring considerable transaction cost or leaving out completely on service participation. Moreover, not being able to transfer the contacts or the personal data (photos, etc.) from one life-logging service to another, makes the barrier even higher.

Consequently, the risk exists that the leading life-logging service provider abuses their market power. For economic reasons, they can strategically reduce available choices in terms of service access, applications offered, information made available and social control options. More specifically, they could

- artificially control the service richness offered on his platform to users, i.e., impede the publication of potentially competitive application offerings, limiting the innovation opportunities around life-logging

- hinder the spread of information if that information is not commercially or politically desired
- lever out net neutrality by introducing different service levels at the application layer
- dictate the social rules around the life-logging service, such as privacy rules, rules around the confidentiality of user data, the copyrights to posted content, etc.

R12 – Decrease of productivity

Affected assets	A2. Social reputation A3. Professional reputation A5. Ideas A6. Life-logging services A7. Social networking services A8. Smart home objects / appliances A9. PC and home infrastructure A10. Smart phone / mobile phone / life-logging devices
Vulnerabilities	V10 Over reliance and excessive dependency on electronic devices and systems V25 Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness, i.e. in which context the data should be used V26 Psychological vulnerability (low self-esteem and confidence to self, high influence potential by others, naïve and suggestible, etc ; weak perception of self)
Threats	T13 Peer-pressure and social pressure to constantly share data; fear of violent response / or ridicule from peers, friends etc T14 Individual being negligent, careless, making mistakes T15 Increased attention deficit disorder
Risk level	**HIGH**
Relevant Risks	**R7 R8**

Life-logging takes time. Even if life-logging applications could reach a high degree of automation, individuals will pay attention to their monitoring status (“Am I online?” “Is he/she online yet?”), to the personal image presented (“How do I look?” “Shall I erase some of the posting before publishing it?”)

and to the feedback coming from the applications (e.g., performance feedback, watching others, peer responses). These activities can be very disturbing and distracting, adversely affecting individual's concentration. Furthermore, during work hours this time for the life-logging activity will be effectively shared with work-related activities, directly reducing work time input, potentially decreasing productivity. It is also important to note the effort and time individuals have to invest to protect their social and professional reputation by frequently controlling the virtual self and remedying unwanted development, such as the publication of an unfavourable image.

Furthermore and although life-logging is envisaged to also increase productivity (as also highlighted in the benefits section,) life-logging activities can be also rather emotionally involving. Messages posted or seen can lead to on-going cognitive reflections among individuals that become more important to them than work- related subjects.

6 RECOMMENDATIONS

Because life-logging is still an emerging set of technologies, there are a number of opportunities for policy makers, regulators and research funders to influence its evolution in a way that minimises the risks identified in this report without stifling innovation and the potential for beneficial uses. In particular, the current review of the Data Protection Directive provides an ideal opportunity to ensure EU legislation will be ready for the mainstream deployment of life-logging across European society. Device manufacturers, software vendors and service providers also have a number of options to reduce risks associated with consumer use of their products.

Individuals should use privacy-friendly tools and make cost-benefit analyses!

Specifically, the European Commission and European Parliament in conjunction with relevant stakeholders and regulatory authorities are in a key position to determine the future regulatory landscape in relation to data protection. The scenario presented in this report aligns with a number of challenges identified by the Commission and stakeholders in the response to the consultation on proposed changes to the data protection directive. We believe that the risks identified in this report and most importantly the recommendations presented below, **can inform on-going discussions** as to what changes to the data protection directive can anticipate the technologies and services described herein.

These recommendations can inform on-going discussions on the DP directive.

We have identified three main areas where life-logging can be improved: transparency and user control in data collection and use; security and privacy by default; and strengthened competition between service providers. These areas are also identified by the European Commission in their 2010 Communication "*A comprehensive approach on personal data protection in the European Union*". [44] In each one of these areas, we make recommendations addressed to each one of these stakeholders: **individuals**, **industry and service providers**, **consumer organisations and associations and government / state** and **EU institutions, regulators and decision makers**.

6.1 TRANSPARENCY AND USER CONTROL

European companies are already required to obtain user consent for the processing of personal data, which must be explicit and informed where that data relates to "sensitive" information such as health, religious or philosophical beliefs, political opinions, sex life, racial or ethnic origin and trade-union

[44] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010.

membership. In practice, this will include a wide range of life-logging data, particularly when linked to location or body sensors. It is also noted that although it could be feasible to require consent from individuals before information related to them is shared, such consent should be enhanced by additional safeguards in order to ensure the protection of the privacy of individuals. For instance, the entity that carries out the life-logging activity should be able to demonstrate that the processing is realised respecting the essence of fundamental rights and freedoms, in accordance with the EU Charter of fundamental rights[45] and in respect of the proportionality principle.

Service providers should give direct online access to users.

To make these decisions, **individuals** need to be able to understand how life-logging devices and services collect and share their data, and the potential consequences, both risks and benefits, of that data use; they should also be fully aware of their rights vis-à-vis the protection of their personal data and be encouraged to exercise them as appropriate. **Individuals** should make use of privacy friendly tools and consider factors and variables that reflect the trade-offs they have to make between the benefits (e.g. gain of comfort, increased functionality, discounts) and risks (e.g. mistrust, disadvantages, risk of misuse or manipulation). More detailed analysis takes into account costs (financial, effort), convenience, usability, security, transparency of the use of data to the data subject, trust in a particular organization, trust in the way the organization handles persona data, trust in the technology, mechanisms that enable provision of services by a third (external) trusted party, the amount of control over one's data, perceived risk of loss of individuality, dignity, autonomy, integrity etc.

…and they should also ensure that their interfaces are user-friendly!

Individuals need to know about the benefits and risks in the use of life-logging and their rights

Companies providing life-logging services can do this by giving consumers clear and comprehensive information, while broader educational materials can be developed by **industry associations, consumer protection groups and data protection regulators** [**R1** , **R5** , **R6** , **R7** , **R8** , **R12**]. It is also important to note that in this information also the benefits should be outlined. More **research** is needed into how end users can most effectively be made aware of the social and psychological consequences that might be associated with life logging data, including how persistence of data can lead to a longer term risk. Without all of this information, individuals cannot effectively protect their autonomy [**R1** , **R7** , **R8**].

Many European countries already require companies to provide information about their personal data processing activities to a national regulator, including the recipients to whom data might be disclosed. Individuals also have a right under EU data protection law to see what personal data a company holds

[45] EU Charter of Fundamental Rights, 2000/C 364/01, Article 52.

about them, and to correct errors. We would thus recommend that **service providers** give direct online access to users, so that they could best realise the quantity and detail of information processed by life-logging services [**R1** , **R8**]; that would mean of course that appropriate information security measures to safeguard external access to these data would need to be in place. Moreover, direct online access could also be complemented with an optional[46] service detecting erroneous data [**R1** , **R2**]; and also to show when and with whom data is being shared, including an audit trail of accesses, and to explain decisions being made using data elements. But most importantly and in order to build consumer trust, **companies** need to ensure that their security and privacy-related user interfaces are intelligible to a wide range of customers – not just to those with the patience and education to understand long-winded and legalistic privacy policies.

Companies also need to obtain and consider detailed information about the functionality and configuration options of the life-logging tools they provide to employees, and then also share it with them, so as to ensure that their staff can carefully balance the need to use life-logging applications with productivity issues [**R9** , **R12** , **R7**].

6.2 SECURITY AND PRIVACY BY DEFAULT

While individuals need intelligible information on life-logging services to exercise effective choice in their use, service providers must also recognise that humans often find it difficult to make decisions about highly uncertain future risks. Many users will simply accept services' default settings. **Service providers** should therefore design their products with a view to protect privacy by default, without preventing users from sharing life-logging data more widely when they are aware of the potential risks that entails. Since these services involve different technologies and devices, as well as architectures, it might be difficult to define recommendations on privacy-by-design, but in any case life-logging **service provider companies** should at least consider privacy and security features of products and applications they select for the implementation of these services. Privacy as a selection criterion imposed by service providers would in its turn increase pressure on device manufacturers and application providers.

Designing the services on a privacy -by-default basis.

This could also include **state / government** providing incentives for companies to include user interface "nudges" [47] towards safer behaviour by customers, and the inclusion of privacy training in computer science education. In mobile and

[46] Optional because we need to consider that the users may deliberately insert "erroneous data" into their life-logged stream in order to protect their privacy, e.g. to lie about one's location; in which case they would probably be unwilling to accept such an error detection service.

[47] The "Power of the default" is an important element of a choice architecture described by Thaler, R.H., and Sunstein, C.R., *Nudge: Improving Decisions about Health, Wealth and Happiness*, Yale University Press, New Haven, 2008. See also: http://nudges.org/tag/default-rules/

ubiquitous computing context changes rapidly and often and privacy and security settings vary by context. More **research** into intelligent automatic systems that learn one's privacy requirements and automatically adjust accordingly would be worthwhile [**R1** , **R3** , **R10**].

Service providers to ensure no personal data leaks; state/governments to consider sanctions on personal data breaches…

Regulators should in general create strong incentives for companies to consider privacy requirements in early stages of product development; a good example of such a practice, which has already been established for RFID applications[48], is the performance of privacy impact assessments before building and deploying services, with input from external stakeholders as appropriate [**R5** , **R6** , **R7**]. **Service providers** and the industry should conduct **security and privacy risk assessments and management** both for new distinct services and in cases where new services have operational interdependencies with existing ones, following a holistic approach for the latter. This will enable organisations to make privacy-supportive design choices and to minimise the quantity of personal data collected to that required by the specific services requested by customers, meeting data protection requirements and reducing the risk of function creep [**R3** , **R10** , **R7** , **R5** , **R9** , **R7**].

Security and privacy risk management: an important tool to be promoted in view of such a rapidly evolving landscape.

We also recommend that the approach of **privacy and information security impact assessment** and **risk management** should be also followed by the public sector, which should promote it and also develop generic frameworks that could assist the industry towards this direction. Such assessments and risk management approaches would need to take into account for example, a cost structure analysis (e.g. costs for data controller versus data processor), consequences of privacy breach incidents, multi-criteria decision making (MCDM), effectiveness and efficiency analysis of proposed privacy related measures and options, social costs of and public reaction to it, legal and ethical costs of implementing or not implementing particular privacy solutions etc.

Service providers should ensure individuals have a "right to be forgotten" through deleting their entire stored data and providing maximum default limits on the time for which detailed data are stored [**R10** , **R2** , **R6**]. As is already the case[49], we would like to note that where life-logging services require personal data storage, **service providers** would still need to ensure that no data is leaked and would

[48] The "Privacy Impact Assessment Framework for RFID applications" prepared by the industry has been endorsed by the Article 29 Working Party on 11 February 2011: http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

[49] Obligation to secure the data processing, provisioned in Article 17 "Security of processing" in Directive 95/46/EC and obligation to define the data retention period, provisioned in Article 15 in Directive 2002/58/EC and in Directive 2006/24/EC.

be liable if any such leakage occurs as a result of their lack of taking appropriate measures, while the period of storage of personal data should be fully justified. Moreover, it could be considered for the **state/ governments** to introduce real sanctions for personal data breaches (which may be related to the market value of personal data), as well as personal responsibility of management, including reversal of the burden of proof, wherever this is possible, depending also on the system design.

Privacy regulator's role increased: prior checks and compliance audits.

For **service providers**, technical measures can ensure stronger protection of life-logging data, particularly the use of encryption for data stored on user devices, such as smart phones [**R3**] and online servers[50]. Moreover, the **service providers** should also consider following a distributed model reduces the risk of compromise of centralised database systems. This could include allowing users to store and process their data on their own equipment, with strict access controls, and the provision of interoperable services by separate companies rather than integrated large-scale data processors [**R10** , **R11**].

Distributed models in data storage & processing versus large-scale centralised databases.

When large quantities of potentially sensitive information are stored by a life-logging service, restricting access solely via easily guessed or forgotten passwords may not provide adequate user protection. Knowledge of specific facts about individuals (such as place of birth or mother's maiden name) is also less valuable when such information is increasingly shared online. In this context, **service providers** should consider using stronger multiple factor authentication mechanisms where available, i.e. two or three-factor authentication methods: "*something you know*" (e.g. password) and "*something you have*" (e.g. smart card, One Time Password) or "*something you are*" (biometrics) [**R1** , **R2** , **R3** , **R6**]. Further research is needed into more sophisticated context-aware and user friendly authentication models.

Encryption and multiple factor authentication.

Privacy regulators can play an important role in ensuring that life-logging systems are operated with sufficient regard to security and privacy issues. In many European countries they can conduct prior checks of large systems before deployment, and later compliance audits to ensure company compliance with data protection law [**R1, R3**]. They can take enforcement action on behalf of citizens – something that could be made more effective by the revision of the Data Protection Directive [**R2** , **R4** , **R6** , **R8**], alongside increased accountability requirements for companies processing personal data [**R3** , **R7** , **R8** , **R10**].

[50] Hogben, G., Dekker, M. (eds.), *Smartphones: Information security risks, opportunities and recommendations for users*, European Network and Information Security Agency (ENISA), 2010.

6.3 REGULATORY ISSUES AND INDUSTRY BEST PRACTICES

As a general remark, we consider that the EU should aim to adequately protect the flow of personal data of its citizens at an international level also through regulation [**R3**]. In the following paragraphs we provide two aspects related to regulatory aspects, one on competition issues and the second one on co-regulation principles and promoting industry best practices.

COMPETITION

An important mechanism to ensure life-logging companies meet high security and privacy standards is to ensure customers can easily switch to competitor providers. This requires interoperability among different services and providers, ideally with the use of open standards and interfaces [**R11**]. Where this interoperability does not come about through market pressures, there may be a case for intervention by **consumer protection and competition regulators**, with guidance from **consumer groups**. The European Commission has suggested that the revised Data Protection Directive include "data portability" requirements [**R11**]. This could be further strengthened with interoperability and interconnection requirements for dominant services, as already found in the EU electronic communications regulatory framework.

Promoting public-private cooperation and co-regulation towards enhancing compliance with security and privacy requirements and provision of better services!

Competition regulators should also consider privacy issues in their broader work to ensure competitive marketplaces [**R2** , **R8** , **R11**].

PROMOTING CO-REGULATION AND INDUSTRY BEST PRACTICES

Competition regulation: promoting healthy competition and avoiding lock-in. Inclusion of "data portability" and enhance interoperability

The promotion of co-regulation pertaining to life-logging services and resulting life-logging data can contribute to the objective of establishing a secure and compliant industry.

Complementary to the regulatory framework in place, **industry** commitments can specify and detail the collection and use of life-logging data for certain segments, for example how to treat location data stemming from traffic navigation services. Agreeing on certain standards in partnership with the public sector and other stakeholders, **industry and service providers** can remove uncertainties as to how to interpret regulation, help compliance and assist that best practices are followed in the life-logging industry. However, in order to be effective, voluntary commitments need to adhere to procedural best practices in co-regulation such as providing for accountability, enforceability and independent evaluation.

This recommendation might entail **governmental support** and co-operation in self-regulatory agreements and public-private initiatives, as well as direct intervention in order to ensure healthy, competitive and choice friendly markets. The main recommendation, however, is to make voluntarily compliance of the industry and self-assurance more attractive in terms of cost. We think that there is a need for the **state/governments** to develop a transparent methodology to evaluate the value function, the monetary (cost), as well as the non-monetary effects of measures taken to comply with privacy legislation and aggregate these effects into information for decision support about deployment of privacy enhancement technologies, privacy by design, auditing support etc.

Herein, **cooperation between private and public sector** (e.g. in the form of public private partnerships) can play an important role in steering industry-wide self-regulation, as well as the quest for inclusiveness and effectiveness of such industry commitments. **Public-private initiative** in this domain could for example work on definition of specific privacy-related decision contexts in several dimensions: duration of privacy measures (single-time, periodical, constant), privacy threat signals (sudden, escalating, anticipated etc), derived consequences (e.g. societal, political), privacy policy monitoring level (international, national), decision time frame (real-time/operational, long-time/strategic), decision model (top-down, peer-to-peer/forum based etc).

Moreover, in this context of cooperation between public and private sector, **the EU and its member states** could strive for regional agreements that would apply throughout the European Union therefore consolidating and harmonising to the best possible extent the compliant treatment of life-logging data [**R4**]. Joining forces among Members States with the **European Commission** provides further a fruitful avenue to broker voluntary commitments with dominant corporations or market leaders even if they are not established within the European Union: they can for example join forces and strike agreements with very large international operators in order to improve the privacy protection on a regional level.[51]

Finally, in certain cases self-regulation can be also promoted as a solution, especially where companies outside the jurisdiction of the EU member states offer services which involve the processing of personal data stemming from EU citizens, e.g. a popular social network site or life-logging application. Self-regulation can be an improvement where there is no adequate level of statutory data protection and the EU and its member states could broker such agreements [**R4**]. If they are adhering to good self-regulatory practices (accountability and enforcement, independent evaluation), it could prove to be an effective solution.

[51] A successful precedent is for example the Safer Social Networking Principles for the EU (http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm), which were adopted by Europe's major social networks, including global players such Facebook, Google, MySpace and Microsoft, in February 2009. Periodical independent evaluations help to trace implementation and review progress and the need for revisions in regard to the relevant objective of improving child online safety.

7 CONCLUSION – *THE RESIDUAL RISKS*

We have seen how emerging life-logging technologies can be used in 3-5 years in the future from now; we have identified benefits in the use of these technologies and also certain important risks, using a structured risk assessment methodology, and made recommendations.

One of the benefits of following such a risk assessment and management methodology is that it allows different levels of abstraction and granularity in an analysis, depending also on the variables you set. It also makes it clear how the management of risks has to do mostly with decisions and the level of risks we are willing to accept. A very important concept in risk management is that of the "*residual risk*": it is defined as the remaining risk after the implementation of controls. In an organisation and enterprise environment, the residual risk might be easier to identify since the whole risk assessment exercise is more concrete and usually performed on a given environment and system. In our scenario assessment however this is definitely not the case; our analysis deals with a prospective situation, identifying potential risks and recommendations, with a view to be better prepared (as a society) to address these risks.

The recommendations made here aim at mitigating the risks identified by the preceding analysis, while taking stock of the benefits; however, this does not mean that the risks identified will be fully mitigated or that the solutions proposed are not free of challenges. There are also cases where vulnerabilities are inherent, and some level of risk should be identified and accepted or further mitigated. In this context, and as a conclusion to our analysis, we have identified certain risk areas that we consider may still remain even after the implementation of the recommendations we make in the previous chapter, and other open issues that cannot be entirely addressed or need further analysis. Specifically:

- **Encryption is not a 'panacea'** – we have recommended that encryption be used to appropriately protect data stored on personal devices, such as smart phone etc; although we realise its importance, we however recognise the limitations of encryption, in the sense that it may offer a false sense of security, especially if it is not appropriately complemented with other information security controls, such as access controls and user awareness. For example, if a person shares their data with an unauthorised individual, it really doesn't matter whether the data is encrypted; also encryption offers little or no protection if the attacker is successfully impersonating the user.

- **Large scale and centralised systems versus small scale and distributed and external access to data repositories –** we have recommended that users store and process their data on their own equipment and underlined the risk of storing data on centralised large scale systems. However, we are also aware that the solution we propose is not fully free of risks: actually, we recognise that both options have advantages and disadvantages. A decentralized design with many small systems

may decrease the potential scale of a breach[52] and it may increase the resilience of the system to component failure; while a centralized model is more likely to become a single point of failure. On the other hand, having multiple systems actually means there's more surface area for the attackers to try and break in, so it may increase the risk of compromise. We understand that this an open issue, part of which has been discussed more extensively elsewhere, and also in other ENISA reports on cloud computing.[53] However, given the analysis performed for the life-logging scenario, we still maintain that a decentralised model will at least mitigate some serious risks, while we need to be aware of its residual risks.

- **Informed consent may still remain an open issue** – We have highlighted that user consent obtained for the processing of personal data should be freely given and informed. However, we understand that, in practice, relying solely on consent for the processing of personal data, especially in the case of life-logging, would not always be sufficient to safeguard the protection of the citizens. The validity of consent will depend on a number of objective and subjective criteria, ranging from the types of personal data and the purposes pursued to the maturity of the data subject and the degree to which he is technology-savvy. Safeguarding individuals' privacy should be complemented with following proportionality principles: i.e. maintaining a balance between the legitimate interests of the data controller that he wishes to serve via the obtaining of the user consent, on the one hand and the privacy of the users on the other[54].

- **Maintaining open-ness while respecting privacy rights –** Our recommendations are heavily geared towards protecting privacy rights and enhancing information security and personal data protection. This does not mean that we do not recognise the benefits of public sites or of sharing information or that we advocate completely against it; however, people need to be aware of the risks entailed and some adequate level of protection for citizens should be provided.

It is thus important to highlight at this point and this is actually the real value of such an assessment as ours: to better identify the real issues and the problem in advance, along with possible solutions, but

[52] Notably, it has been also argued that authentication using a personal device is more secure, because it does not leave that rich personal data trails: see for instance Petersen, S., *Grenzen des Verrechtlichungsgebotes im Datenschutz*, Lit-Verlag, Münster, Hamburg u.a., 2000.

[53] See for example ENISA study on "Cloud Computing Risk Assessment", available here: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment and also "Security and Resilience in Governmental Clouds", available here: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

[54] Notably under the EU Data Protection law, "informed consent" and the "legitimate interest of the controller" mentioned here are only two out of the six possible legal grounds of personal data processing (Article 7 of the *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*). But the focus of this paragraph is on informed consent given the results of the preceding analysis.

most importantly to determine the limitations and the choices that one can make. It all boils down to a risk assessment mentality: few things come risk-free; the question is to choose the level of the risk which is more acceptable or will have a less important impact. We believe that if we can reach that level of understanding now, our society can be better prepared to address the risks lying ahead.

8 REFERENCES

Allen, A.L., 'Dredging up the past: Lifelogging, Memory, and Surveillance', *The University of Chicago Law Review*, Vol. 75, No. 1, 2008, pp. 47–75.

Bentham J. , Bozovic M (ed.), *The Panopticon writings*, Verso, London, 1995, pp. 29–95.

Catteddu, D., Hogben, G. (eds.), *Cloud Computing Risk Assessment*, European Network and Information Security Agency (ENISA), 2009. Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Catteddu, D., Hogben, G. (eds.), *Security and Resilience in Governmental Clouds*, European Network and Information Security Agency (ENISA), 2010. Available at: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.: 201, Lanzarote, 25.10.2007, Art. 23. Available at: *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=1&DF=&CL=ENG*

Daskala, B, Maghiros, I., *D1gital Territ0ries - Towards the protection of public and private space in a digital and Ambient Intelligence environment*, JRC Technical and Scientific Report, EUR 22765 EN, 2007. Available at: http://ftp.jrc.es/EURdoc/eur22765en.pdf

Daskala, B. (ed.), *Flying 2.0 – Enabling automated air travel by identifying and addressing the challenges of IoT/RFID technology*, European Network and Information Security Agency (ENISA), 2010. Available at: www.enisa.europa.eu/act/ rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105 , 13/04/2006 P. 0054 – 0063. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 –

0047. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

Emerging and Future Risks Framework – An Introductory Manual, European Network and Information Security Agency (ENISA), 2010. Available at: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/emerging-and-future-risks-framework-introductory-manual

Estrin, D., 'Participatory sensing: applications and architecture [Internet Predictions]'. IEEE Internet Computing, Vol. 14, No. 1, 2010, pp. 12–42.

EU Charter of Fundamental Rights, 2000/C 364/01, Article 52. Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009. Available at: *http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf*

Ganti, R.K., Pham, N., Tsai,Y.E., and Abdelzaher, T.F., 'PoolView: stream privacy for grassroots participatory sensing', *Proceedings of the 6th ACM conference on Embedded network sensor systems*, ACM, New York, 2008, pp. 281–294.

Goldman, J., Shilton, K., Burke, J., Estrin, D., Hansen, M., Ramanathan, N., Reddy, S., Samanta, V., Srivastava, M., and West, R., *Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world*, Woodrow Wilson International Center for Scholars, 2008, pp. 1–15. Available at: http://lecs.cs.ucla.edu/~nithya/publications/ParticipatorySensingScenarios 9-19-08.pdf

Hogben, G., Dekker, M. (eds.), *Smartphones: Information security risks, opportunities and recommendations for users*, European Network and Information Security Agency (ENISA), 2010. Available at: http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users

International Organization for Standardization (ISO), Information technology — Security techniques — Information security risk management, International Standard, ISO/IEC 27005:2008(E), First edition, 15 June 2008, p. 1.

Jernigan, C., and Mistree, B. F.T., 'Gaydar: Facebook friendships expose sexual orientation', *First Monday*, Vol. 14, No. 10, 2009. Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2611/2302

Kosta, E., Kalloniatis, Chr., Mitrou L., Kavakli E., 'The "Panopticon" of Search Engines: The Response of the European Data Protection Framework', *Requirements Engineering*, Vol.16, 2011, pp. 47–54.

Lane, N.D., Eisenman, S.B., Musolesi, M., Miluzzo, E., and Campbell, A.T., 'Urban sensing systems: opportunistic or participatory?' *Proceedings of the 9th workshop on Mobile computing systems and applications*, ACM, New York, 2008, pp. 11–16. Available at: http://portal.acm.org/ft_gateway.cfm?id=1411763&type=pdf

Langheinrich, M., and Karjoth, G., 'Social Networking and the Risk to Companies and Institutions', *Information Security Technical Report*, *Special Issue: Identity Reconstruction and Theft*, Vol. 15, Elsevier, 2011, pp. 51–56.

Lenhart, A., *Teens and Sexting. How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*, Pew Internet & American Life Project, 2009. Available at: http://pewInternet.org/Reports/2009/Teens-and-Sexting.aspx

Marinos, L., *Cyber-bullying and online grooming: helping to protect against the risks – A scenario on data mining / profiling of data available on the internet*, European Network and Information Security Agency (ENISA), 2011 [forthcoming].

Marwick, A., Murgia-Diaz, D. and Palfrey, J. , *Youth, Privacy and Reputation (Literature Review),* Berkman Center Research Publication, No. 2010-5, pp. 14–16

O'Hara, K., Tuffield, M.M., Shadbolt, N., 'Lifelogging: Privacy and Empowerment with Memories for Life', *Identity in the Information Society*, Vol. 1, pp. 155–172, Springer, 2009. Available at: http://dx.doi.org/10.1007/s12394-009-0008-4

OECD, 'The Protection of Children Online: Risks faced by children online and policies to protect them', *OECD Digital Economy Papers,* OECD Publishing, No. 179, Para 72. Available at: *http://dx.doi.org/10.1787/5kgcjf71pl28-en*

Osimo, D., Szkuta, K., Armenia, S., Lampathaki, F., Koussouris, S., Mouzakitis, S., Charalabidis, Y. et al. *The CROSSROAD Roadmap on ICT for Governance and Policy Modeling*, 2010. Available at: http://crossroad.epu.ntua.gr/files/2010/02/CROSSROAD_D4.3_Final_Roadmap_Report-v1.00.pdf

Petersen, S., *Grenzen des Verrechtlichungsgebotes im Datenschutz*, Lit-Verlag, Münster, Hamburg u.a., 2000.

Regan, P. M., 'Privacy as a common good in the digital world', Information, Communication & Society, Vol. 5, No. 3, pp. 382–405.

Richards, R. and Calvert, C., 'When sex and cell phones collide: inside the prosecution of a teen sexting case', *32 Hastings Comm. & Ent,* L.J. 1, 2009, pp. 1–3.

Siegle, D., 'Cyberbullying and Sexting: Technology abuses of the 21st Century', *Gifted Child Today,* Vol. 33, No. 2, 2010, pp. 14–15.

Solove, D.J., 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*, Vol. 154, No. 3, 2006, pp. 477–560.

Thaler, R.H., and Sunstein, C.R., *Nudge: Improving Decisions about Health, Wealth and Happiness*, Yale University Press, New Haven, 2008.

Warren, S.D., and Brandeis, L.D. 'The Right to Privacy', *Harvard Law Review*, Vol. IV, No. 5, 1890, pp. 193–220.

Westin, A.F., Privacy and Freedom, Atheneum, New York, 1967.

Weyer, J., *'*Die Zukunft des Autos – das Auto der Zukunft. Wird der Computer den Menschen ersetzen?*', Soziologische Arbeitspapiere 14, Wirtschafts- und Sozialwissenschaftliche Fakultät,* Universität Dortmund, Dortmund, 2006.

Wood D.M. (ed.), *A report on the surveillance society for the (UK) Information Commissioner*. Surveillance Studies Network, 2006. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

ANNEX I – VULNERABILITIES

This section presents the results of the vulnerability identification and assessment performed by the expert group, based on the scenario. Vulnerabilities become risks only when they are exploited by a threat (see next section).

Vulnerability	Vulnerability Value[55]		
	Severity *[1-3]*	*Exposure* *[1-3]*	***Value*** ***[1-5]***
V1 Flawed/insufficient design, implementation and/or capacity of devices and systems. Includes software bugs and design flaws.	2	2	**3**
V2 Inadequate policy framework (e.g. data protection, competition)[56]	1	2	**2**
V3 Inadequate privacy/security interfaces (poor interface design)	2	2	**3**
V4 Increase in centralization of data storage and processing and over-reliance on these centralised facilities	2	3	**4**
V5 Inherent features of smart devices (size, material etc.) They may be easy to lose or to be stolen, oversensitivity of sensors (for example, leading to inaccuracies)	3	3	**5**
V6 Lack of appropriate, common or harmonized	2	2	**3**

[55] The vulnerability value is estimated considering these two values: use the scale 1-3 [*Low – Medium – High*] to indicate the value for the two criteria.

[56] For more information please refer to the Legal assumptions in section 5.1 regarding the envisaged European data protection frameworks.

Vulnerability		Vulnerability Value[55]		
		Severity *[1-3]*	*Exposure* *[1-3]*	***Value*** ***[1-5]***
	legislation in EU Member States			
V7	Lack of interoperability between devices/ services/ technologies and/or systems	3	3	**5**
V8	Lack of or inadequate user identification, authentication and access controls	3	3	**5**
V9	Lack of third party system reviews and software integrity certification	2	2	**3**
V10	Over reliance and excessive dependency on electronic devices and systems	3	3	**4**
V11	PC and home infrastructure vulnerabilities[57]	3	3	**4**
V12	Smart phone vulnerabilities Based on the ENISA report, the following are some very important vulnerabilities: • Encryption weaknesses • Weak smart phone application distributor authentication mechanisms [increasing the risk of successful phishing and spyware attacks, among others] • Vulnerabilities leading to malware installation: Patching weaknesses, limited capabilities for 3rd party security	3	3	**5**

[57] See Technical assumptions (the last bullet point) for an explanation on the rationale of this vulnerability and its assessment.

Vulnerability	Vulnerability Value[55]		
	Severity *[1-3]*	*Exposure* *[1-3]*	***Value*** ***[1-5]***
solutions (centralised security management), reputation vulnerabilities, lack of code/app review processes, and difficulty in distinguishing between singed and unsigned apps, ability to unlock phones • Covert channels/weak sandboxing: In some smart phone platforms, location data is added to photo filenames or in file metadata. If these photos are made available to other apps or uploaded to social networking sites, users will be asked for permission to access the gallery, but not location data. This therefore constitutes a covert channel. For example, a user might post a photo on a public blog or micro-blogging site, without realising that the filename contains the location of the data. • User permissions fatigue: user interfaces are usually more limited, users do not have the time or commitment to evaluate permissions requests, permissions are not detailed enough to convey the risks of giving consent We have also based our assessment on the respective values of these vulnerabilities in the ENISA report (for consumers only, since this is our focus).			
V13 Lack of revocation/correction/deletion mechanisms	3	2	**3**
V14 Lack of (usable and appropriate) privacy controls, e.g., overly permissive defaults, too coarse	2	3	**4**

Vulnerability		Vulnerability Value[55]		
		Severity *[1-3]*	*Exposure* *[1-3]*	***Value*** ***[1-5]***
	granularity, lack of privacy preserving default settings...			
V15	Lack of (usable) logging controls/policies/ reminders. E.g. capturing some embarrassing scene of someone else or yourself	3	2	**3**
V16	Lack of secure transmission and storage of data; also includes lack of (usable) transmission control (who gets the data)	3	3	**5**
V17	Lack of mechanisms to validate reputation or trustworthiness of service provider	3	3	**4**
V18	Lack of noticeable (and usable) notification systems. So that you don't know when you're logged on someone else's system	2	2	**2**
V19	Increased complexity of controls (making it difficult for users to follow)	2	2	**3**
V20	Increase of (unprotected) data storage capacity in	3	3	**5**
V21	Reliance on legacy, un-patched systems or integration mistakes	2	2	**3**
V22	Lack of appropriate assurance procedures (e.g. third party audits) or enforcement of such, regarding the implementation of security controls, especially from the state, other regulatory and public authority	3	2	**4**
V23	Lack of transparency and "social translucency", i.e.,	3	3	**4**

Vulnerability		Vulnerability Value[55]		
		Severity *[1-3]*	*Exposure* *[1-3]*	***Value*** ***[1-5]***
	audit logs (who accessed my profile/data); for instance, Annika's colleague is unaware of data collection and maybe be subject of (potential) "blackmail"			
V24	Social reliance/over-confidence and trust on individual's digital identity	2	2	**3**
V25	Inadequate user education, lack of awareness and training particularly in security and privacy; lack of context awareness, i.e. in which context the data should be used	3	3	**5**
V26	Psychological vulnerability (low self-esteem and confidence to self, high influence potential by others, naïve and suggestible, etc.; weak perception of self)	2	4	**5**
V27	Cognitive biases – Some people accept what they should not…	2	3	**4**
V28	Data linkability / life-logging data can be aggregated with other data	2	2	**3**

ANNEX II – THREATS

This section presents the results of the threat identification and assessment performed by the expert group, based on the scenario. Threats become risks only when they exploit a vulnerability of an asset.

Threat Description	Threat agent[58]	Threat Value[59]		
		Capability [1-3]	*Motivation [1-3]*	*Value [1-5]*
T1 Accidental loss of device	User / individual	**3**	**n/a**	**4**
T2 Identity theft	Malicious attackers / impostors Fraudsters	**3**	**3**	**4**
T3 Intentional misuse , unauthorised disclosure, modification or destruction of individual's data	Service provider (e.g. exploits data in an unexpected, for user, manner) Malicious attacker	**2**	**3**	**5**
T4 Unintentional misuse, unauthorised disclosure, modification or destruction of individual's data	Individual's peers, friends, family	**2**	**1**	**5**
T5 Intermittent or no connectivity	Physical	**1**	**1**	**2**
T6 Malicious physical attacks (theft, vandalism, misuse,	Malicious attacker	**1**	**1**	**4**

[58] Can be: natural (e.g. fire, flood etc.), physical (e.g. hardware / equipment failure) or man-made, e.g. a scenario actor, an attacker, employer etc.

[59] The threat value is estimated considering these two values: use the scale 1-3 [Low – Medium – High] to indicate the value for the two criteria.

Threat Description		Threat agent[58]	Threat Value[59]		
			Capability [1-3]	*Motivation [1-3]*	*Value [1-5]*
	etc.)				
T7	Malicious (logical) attacks on devices and systems	Malicious attacker	**2**	**2**	**2**
T8	Overhearing/recording logging/blogging activity	Service provider Malicious attacker Individual's peers, friends, family	**1**	**3**	**3**
T9	Exploring new 'vulnerabilities' in the new applications [the importance of this threat lies in the motivation which is exceptionally high, considering what's at stake]	Malware authors Cyber-criminals	**1**	**3**	**2**
T10	Spamming of users with ads and other non-solicited information; they can also use open, public information	Companies / service providers	**2**	**3**	**3**
T11	Constrain consumer choices	Companies (e.g. those offering life-logging services)	**2**	**3**	**3**
T12	Vested interests	Service providers, providers in market sectors, public sector / state	**2**	**3**	**4**
T13	Peer-pressure and social pressure to constantly	Individual's peers, friends etc	**3**	**3**	**3**

Threat Description		Threat agent[58]	Threat Value[59]		
			Capability [1-3]	*Motivation [1-3]*	*Value [1-5]*
	share data and conform; fear of violent response / or ridicule from peers, friends etc;				
T14	Individual being negligent, careless, making mistakes; e.g. does not follow procedures appropriately, e.g. clicks through	Individual	**3**	**1**	**4**
T15	Increased need for attention / social exposure	Individual	**3**	**n/a**	**3**
T16	Changes in perception of privacy and / or privacy needs (especially from one generation to another): changes to this respect are not always negative; on the other hand, they may not be always informed or natural.	Individual State	**3**	**1**	**4**
T17	Data mining and profiling (large-scale, excessive and/or inappropriate): profiling entails the categorisation of citizens in profiles, based on their buying behaviour, financial status, habits or even health condition; this may happen for example, with a view to offer better	Companies / service providers, State Individual's peers, friends etc	**3**	**3**	**5**

Threat Description	Threat agent[58]	Threat Value[59]		
		Capability [1-3]	*Motivation [1-3]*	*Value [1-5]*
and personalised service. However, there is a threat, particular in a life-logging scenario, that heavy data mining and profiling is rather excessive and not always justified, which might lead to risks.				
T18 Monitoring and surveillance: given the nature of life-logging applications, the threat of excessive monitoring and surveillance, which is already identified as an important issue nowadays, needs to be considered as well, as it extrapolates the importance of the risks it poses even today.	Companies / service providers on citizens and their employees, State on citizens Individual's peers, friends etc for personal purposes	**2**	**3**	**4**

APPENDIX I – SCENARIO BUILDING AND ANALYSIS TEMPLATE

Please refer to accompanying document.

APPENDIX II – RISK ASSESSMENT SPREADSHEET

Please refer to accompanying document.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu