Achieving synergies between security and information-related fundamental rights (IRFR) in a digital intensive environment

Report of the Horizon 2020 Protection and Security Advisory Group (PASAG)[1]

September 2018

In a digital-intensive world, the design of cyber-security solutions needs to address the two seemingly competing fundamental rights of security and privacy. Additionally, confidentiality of information needs to be preserved and enforced in a growingly digitised world, to avoid the loss of valuable Intellectual Property Rights to individuals and businesses and the compromise of sensitive information in the area of security.

This report is intended to provide an overview of approaches on how to address these issues objectively in future programmes, in terms of IPR (Intellectual Property Rights) management, access to project information, and external communication about the projects, taking into account novel privacy-by-design and security-by-design techniques.

1. Overview

The primary focus of this report is to address the significance of ensuring that the privacy and the security characteristics and specifications of digital environments are mutually reinforcing, rather than potentially exclusive of each other, to achieve solutions that are protective of the individual's digital fundamental rights. Indeed, these two essential, complementary building blocks of a free, safe and democratic society, need to be placed into a broader context. Increasingly, this also means bringing together what happens on-line with what happens off-line. Privacy and security interact in the online space in a way which should reflect and reinforce the very same values which are cherished and respected off-line. These values are typically those recognised and protected in international legal instruments such as the UN Universal Declaration of Human Rights[2], the UN International Covenant on Civil and Political Rights[3], the European Convention on Human Rights[4], the Charter of Fundamental Rights of the European Union[5]. As people interact on the Internet, as well as off-line, fundamental human rights come into play, including:

- The right to freedom of expression
- The right to freedom of association
- The right of freedom of information

[1] More information about the PASAG can be found here: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010

[2] The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A), http://www.un.org/en/universal-declaration-human-rights/

[3] https://www.ohchr.org/en/professionalinterest/pages/CCPR.aspx

[4] https://www.echr.coe.int/Documents/Convention_ENG.pdf

[5] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

- The right of freedom of religion
- The right to private and family life
- The right to privacy and protection of reputation
- The right to property
- The right to a fair trial

Part of the global objectives and concerns of PASAG revolve around the impact on these rights of past, current and future practices on the Internet.

Technical developments impose new privacy and security risks that could be harmful to the society and the above-mentioned rights. The Internet growingly supports seamless interaction with multiple on-line devices in the Internet of Things (IoT) and increasingly with off-line technologies. Taken together, these exchanges, augmented by surveillance technologies such as CCTV (Close-circuit television), transactional data and metadata, as well as by Big Data inference analysis, may, without an appropriate policy intervention, lead to a serious dilution of privacy and the undermining of fundamental rights, without the benefit of increased security.

Human rights are universal, but they are also influenced by the dimensions of time, space and place. They should be adaptable to further development and refinement, especially in contexts such as the Internet, where personal information may be shared in ways difficult to control, and where people interact with new technologies and modify their behaviour because of them. One of the avenues of research of the social, ethical and legal aspects of the impact of any new technology is therefore the relationship between information-related fundamental rights (IRFR) and the free, unhindered development of personality. The latter is an over-arching fundamental right recognised in the constitutional law of many EU Member States as well as of many other countries worldwide. This suggests that research into privacy and security, especially in a context where much of the world is on-line and where Europe is an integral part of the on-line world, needs to be carried out consistently without losing sight of the wider context of other information-related fundamental human rights such as freedom of expression, freedom of information and the right to dignity and to the protection of reputation.

2. Framing the issues

Security (e.g., protection of citizens) and privacy (e.g., protection of personally identifiable information) are two major concerns in society.

There is a tendency to recognize these as potentially conflicting requirements of modern society, and the scope of this report is to investigate conditions and approaches where mutual satisfaction of these two concerns is achievable and, where such outcome is not feasible, suggest (socially acceptable) criteria that may justify one benefitting over the other.

The friction between security and privacy often emerges as individual/fundamental rights and freedoms become constrained by law enforcement requirements to ensure societal security. This preoccupation has become increasingly relevant over the past years, particularly as the result of terrorism and the related enforcement initiatives by government agencies. In this context, advanced surveillance practices and techniques have significantly improved the ability of LEAs (Law Enforcement Agencies) to monitor and pre-empt terrorist initiatives, but have also raised red flags with privacy advocates concerned with the lack of visibility on the processes that sanction enforcement.

Criminals have also raised their game by encroaching aggressively onto the digital sphere. In 2016, online fraud and computer crime surpassed all other crimes in the UK[6]. Online crime has the great advantage of anonymity and can be perpetrated across national boundaries, making investigations and prosecution difficult and expensive. Criminal exploitation of the internet is jeopardising the potential of the digital space and undermines the confidence in digital services by the public. It is therefore an imperative to ensure that individuals are protected when using the internet and that their digital identity is securely managed, also to protect their privacy.

In the debate on identity management, some cyber security actors press hard for traceability, while privacy advocates insist on anonymity. There is a need for both in different contexts (and sometimes in the same context). Thus, identity management protocols would need to cover both – yet this is an elusive target if left to technology alone. It is for policy makers to build a societal consensus on this issue which will require compromises to be made, since the physical world does not match the digital world when it comes to anonymity.

Another challenge is the control and protection of personal data while permitting the use of direct and derived data (correlation) for emerging new services and products. This is a hot topic, currently debated in the media and among policy makers, but a consensus approach to addressing it is unlikely to emerge any time soon. Of note is that when information is used for the initial purpose declared when acquiring it, the user would likely not argue against its declared usage. It is the uncertainty that it will be used for other activities that leads to doubts and concerns. It is this lack of confidence in the rules for digital privacy that needs addressing.

Control over personal data is complex when data provenance is difficult to determine. Regulations are often inconclusive in this area and the responsibility falls to individuals to protect their rights in this uncertain domain, often with great opposition from industry players. A holistic approach to regulating this space would be highly beneficial.

In a highly competitive and globalised world, the need to protect the information assets of businesses is also a paramount consideration. Industrial and commercial cyber-espionage is a very diffuse problem which affects businesses world-wide and is a grave risk to intellectual property and economic sovereignty. Protecting European business knowledge is key to ensuring a secure and protected society. As industry 4.0 evolves, the interplay between the digital and the physical worlds will become ever tighter, requiring significantly increased attention to appropriately secure information environments that can mitigate the risks of economic compromise.

3. The value of data

"*It is not a case of big data 'or' data protection, or big data 'versus' data protection. That would be the wrong conversation. Privacy is not an end in itself, it is an enabling right. Embedding privacy and data protection into big data analytics enables not only societal benefits such as dignity, personality and community, but also organisational benefits like creativity, innovation and trust. In short, it enables big data to do all the good things it can do*." [7]

Data collection, aggregation and interpretation/analysis of user/customer interests and behaviours is necessary to provide improved services and tailored offerings, allowing for a more effective and

[6] UK Office of National Statistics, Crime Survey for England and Wales 2016.

[7] Big data, artificial intelligence, machine learning and data protection, Report by the Information Commissioner's Office, UK - 4 September 2017 – Foreword by Elizabeth Denham, Commissioner.

efficient interaction between demand and supply. Data aggregators and advertisers highlight how the customer experience can only improve as more information is collected on individual preferences and purchasing behaviours, in a virtuous circle of analysis and profiling which focuses the marketing effort to increase the sales opportunity. The benefits are clear, as overall marketing costs reduce per unit of output sold and, importantly, product development becomes more effective as demand is more likely to meet the right supply. Overall, this reduces costs to consumers and makes businesses healthier and more resilient. And, as technologies evolve, and products become smarter, the potential for data collection, aggregation and exploitation, increases exponentially. Ultimately, but certainly not far into the future, artificial intelligence and machine learning applications will enhance these capabilities even further, likely redefining the foundations of the interaction between consumers and the marketplace.

This evolution is creating a major asymmetry between the individual and the organisations that capture and exploit the data he/she generates. Whereas, the individual might be willing to give up some level of privacy in return for a free or better service or, willingly, supply personal data in the exchange, the asymmetry lies in the lack of transparency in how this data will ultimately be used and in its value to the organisations exploiting it. To address this asymmetry, privacy legislation is attempting to create a baseline of rights available to the individual in the digital environment, forcing more compliance by organisations in disclosing how data is used, requiring prior approval for its use and imposing the obligation to protect the data from inappropriate exploitation (see the EU General Data Protection Regulation[8]). Attempts are also being made to enable individuals to screen the data they are providing and control the extent of its exploitation by third parties. However, while organisations are investing major resources to improve the quality and effectiveness of data collection and exploitation, an infinitely smaller effort is dedicated to ensuring regulatory compliance to privacy legislation.

As PWC reports, "*the role of technology in the GDPR, as both the cause of the problem and as the inevitable solution, leaves organisations in a difficult position. In many organisations, the information management and governance environment is an underdeveloped part of the technology stack. This is because these initiatives regularly lose out to business-sponsored projects with a more direct connection and visible impact on core business metrics, such as revenue, cost and customer satisfaction. In such a contest, it is unlikely that a regulatory environment alone will ever provide sufficient assurance that an individual's private information is adequately controlled and protected."*[9]

This is where technology could play a useful role. Data exploitation relies on developments in algorithmic science and machine learning, and the larger the data sets, the more refined and effective the output can be. Electronically tagging individual data sets, to enable tracking of usage, including how, where and who has access to this data, could be an option to ensure that the intended result of data privacy regulation is effectively enforced. Additionally, applying blockchain

[8] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

https://www.eugdpr.org/

[9] Technology's role in Data Protection – the Missing Link in GDPR Transformation, PWC (PricewaterhouseCoopers), October 2017.

technology[10] to these data sets could enable an indelible record of all data exchanges and modifications, with the potential to significantly enhance regulatory traceability and data security.

The weakness of enforceable data privacy and the proliferation of identity theft (representing 15% of the total number of consumer complaints as reported in the latest United States Federal Trade Commission report[11], the second highest in ranking) are some of the reasons why fake accounts are proliferating, undermining trust in the digital environment that will likely have a damaging economic impact.

As a result, organisations collecting and exploiting data legitimately can end up storing wrong, misleading or sometimes criminally acquired information, enhancing and perpetuating the problem of data reliability and security. To what extent this can be dealt through traditional cyber-security mitigation approaches is debatable. Again, indelible electronic markers could help address this problem.

4. Privacy

Privacy and big data analytics

"*Privacy by design means thinking at the outset of every data-based project what the impact on personal, sensitive data might be, planning to mitigate that impact, and only ever gathering, storing or processing data that is actually needed*."[12]

Data sets can be extremely valuable in providing understanding of behaviours that can improve everyday life. For instance, mobility patterns in modern cities can be extrapolated with considerable accuracy through mobile phone mobility applications, which could assist in predicting how a viral disease might spread in a metropolitan area. For this type of analysis, aggregated data is more appropriate to provide the necessary inference information. However, big data is the collection of a a myriad of single data points, of which just a few are sufficient to provide identification of the individual source. For this reason, data collection needs to be targeted for a specified usage and when the objective is achieved the data should be discarded. In such cases, the interest of the community can be served largely without infringing on individual data privacy. Clearly, when data is collected in bulk, appropriate anonymisation protocols need to be instituted to ensure that individual information sets cannot be subsequently extracted.

At the same time, there are some internet services like Shodan (IPv4)[13] or MrLooquer that locate, identify and provide detailed insight on the IP addresses and capabilities of IoT devices, mapping and indexing them. Unfortunately, these external and mostly free detection services are not used only for remediation purposes. They are therefore vulnerable to malicious interference, as well.

[10] Blockchain technology involves the application of a distributed ledger that tracks transactions (data exchanges and modifications) without third party involvement or verification. Once a transaction is executed and confirmed a record is made and permanently retained. The first broad usage of blockchain was initiated through Bitcoin transactions but offers great scope for far wider application.

[11] https://www.ftc.gov/node/943403

[12] Tackling Data Privacy to Unlock the Power of Big data Analytics, Research Paper by Finetxra and Privitar, June 2017.

[13] Shodan is a search engine focused on the identification of internet-connected devices, or the Internet of Things (IoT)

Privacy and crime

Communication networks and social media offer an infinite source of data and information and the law enforcement and intelligence communities world-wide have been developing increasingly sophisticated capabilities to exploit them. This involves targeted data collection, storage and query as well as bulk gathering (i.e. not connected to specific targets), a common practice in some countries, but contested by privacy advocates. The advantage of bulk data collection and its retention over time for LEAs is the opportunity it offers to trace back a specific target's past communications, behaviours and associations, which would not be possible when relying exclusively on targeted collection which can only start from the time the individual is first identified as suspect. By applying big data analytics to bulk data stored over time would allow the identification of patterns without necessarily knowing in advance what to look for. When properly applied, specially trained algorithms can identify behaviours that could prelude to criminal or terrorist action: "*It can be particularly helpful when you're looking for the lone wolf…Advanced analytics lets you flag individuals who have disturbing behaviour profiles – not just the ones who are connected to networks or groups that are already under suspicion. … Big data analytics is being used by researchers to create profiles of those who are susceptible to radicalization. Combining these profiles with bulk collected metadata could allow for closer monitoring of people identified as a recruiting target for a terrorist group. Going further, if an algorithm can cross reference those thought to be susceptible to radicalization with data about who holds pilot's licences, for example, there may be a way to predict that someone is planning an attack.*"[14]

Such data analytics capabilities leveraged for security requirements, are useful to prevent and eventually sanction criminal activities. However, privacy enhancing techniques need to be implemented to ensure privacy concerns and privacy legislation are adhered to in these operations. Finally, useful results can also be observed by using systematic and selective filtering, coupled with protected query mechanisms. In this respect, controlled and filtered data acquisition, accompanied by gated queries of large databases could significantly address privacy concerns, while enabling exploitation of big data.

Encryption technologies have become a serious concern for LEAs, in limiting access to information that could prove valuable in crime prevention or conviction. If evidence is encrypted, and there is no arrangement in place to enable "back-door" access, LEAs may ultimately achieve access only by applying brute force (using massive password cracking techniques), which may delay or impede investigations (in most situations this is still a viable option, e.g. see the iPhone debate in 2016 in the US[15]). However, this continues to be an area of open public debate, with little indication that a way forward agreeable to users, providers and law enforcement is practical. In a few countries, encryption of communications by the public is prohibited by government authorities, and providers

[14] CT Tactic: Bulk Meta-Data Collection and Use, Scott Robins (http://counterterrorismethics.com/bulk-meta-data-collection-and-use)

[15] In December 2015 Syed Rizwan Farook, supported by his wife Tashfeen Malik, killed 14 people and injured 22 in a mass shooting in San Bernardino, California. Mr. Farook and his wife were killed in the aftermath. The iPhone of the suspect was encrypted. In February 2016 the FBI filed a court case in the United States District Court for the Central District of California to enjoin Apple to create and electronically sign new software that would enable the FBI to unlock the iPhone 5C it recovered from one of the shooters. The court hearing was subsequently postponed as the FBI indicated that it had found an alternative approach to securing the iPhone data.

are therefore banned from providing this service or need to ensure special access for government authorities through backdoor decryption channels.

While end-to-end encryption of communications would be detrimental to the capabilities of LEAs in crime prevention, investigation and conviction, its impact should be mitigated by the following considerations:

- End-to-end encryption goes counter to the commercial benefits of collecting data on user preferences and therefore the extent of its broad dissemination as a standard in communications may be limited;
- There are other means of effectively tracking people and their preferences, e.g. metadata[16] (this area also has the attention of privacy advocates);
- Criminals and terrorists have been at the forefront of applying encryption technologies to their communications, whether or not encryption is available as a commoditised service. Therefore, it is unlikely that general access to these capabilities will significantly diminish enforcement effectiveness.

Privacy and IPR

Increasingly, Intellectual Property Rights are held exclusively in digital form, representing the fastest growing asset class in the world and a major contributor to economic growth. The diverse nature of IPR and its significant value to businesses in all sectors of the economy, create a unique challenge to ensure its protection.

The financial and economic implications resulting from a loss or damage to IPR are difficult to assess and recovery can be complicated by the speed and anonymity with which digital information can be transferred, masked and ultimately absconded. Privacy protocols, including information dissemination, anonymisation, pseudonymisation, can also find application with digital IPR segregation and protection to minimise the opportunities for data loss. Cyber-security solutions benchmarked to provide secure repositories for valuable corporate IPR have similar applications to the security requirements of personal data.

Privacy and physical surveillance

Over the past few years, physical surveillance, implemented through detection sensors augmented by software and hardware advances that have accelerated the speed and accuracy of recognition, are creating a new and significant challenge to the right to privacy. Physical surveillance has provided LEAs with an increasingly important deterrent and conviction tool and its proliferation in major urban centres generally and in particularly areas of high footfall is significantly improving the security profile of potential terrorist and criminal objectives. Recent important developments in facial and pattern recognition software allow for a higher level of automated surveillance that can release

[16] "Meta-data is often described as "data about data". This, at first glance appears rather unhelpful; however, it does point out the main difference between data and metadata, the fact that it is data *about* other data is what makes it *meta*-data. It is the relationship with other data that makes some piece of information meta-data. On a common description, imagine I send an email to you at 10:13 AM today. Whatever is contained in the email, the content (the subject and message), would be the primary data. However, the time it was sent (10:13 AM), who sent it (me), who it was sent to (you) etc., would be the meta-data: that is, this is data *about* the email, rather than the email itself." From: CT Tactic: Bulk Meta-Data Collection and Use, Scott Robins (http://counterterrorismethics.com/bulk-meta-data-collection-and-use)

human engagement for more specific surveillance tasks. This is generally appreciated as an important contributor to an improved security environment for the protection of the citizens.

Clearly, however, there is a growing concern that these advanced surveillance capabilities, if not subjected to appropriate privacy protocols, may become abusive of individual rights. While typical identifiers of the individual are now the subject of increased protection from misuse and abuse, important physical identifiers such as recognisable images are not necessarily afforded the same protection. While mostly held by LEAs, the proliferation of image capture capabilities by both public and private operators is creating the concern that privacy in a public space (and in some instances, in private spaces as well) cannot be protected. As a start, robust access control criteria to this information should be established with all public and private organisations that deploy such capabilities, including identifying the authorized persons that have access, the modalities for release to third parties and the length of time the information can be held for later review.

New data-minimising techniques should be developed in parallel to the improvements in pattern recognition, to focus for example, on suspicious behaviours rather than massive image capture or disclosing surveillance data only in the case of a serious breach authorised by a trusted third party or controlling the details of the image capture depending on the environmental context.

As recommended in the final report of project SurPRISE, there needs to be "*a genuine consideration of non- or less intrusive alternatives prior to the deployment of broad dragnet surveillance measures for security purposes. Develop, foster, and prioritise measures (including SOSTs)*" (security-oriented surveillance technologies) "*with a narrower scope of data collection, storage and use whenever they are suitable instead of focusing on forms of untargeted mass surveillance.*"[17]

Privacy and social factors

Complexity (as the lack of usability) is one of the main barriers for not using solutions available worldwide however several attacks come also due an unsafe behaviour online and other type of human factors like human disclosure behaviour or sloppy ways to manage devices or data.

The distance between offline and online worlds seem to be an incentive for such an unsafe behaviour by internet users. Others try to create their own avatars by reproducing their own or invented attributes.

Privacy and the social media explosion

One of the major triggers for the dissemination of private information in the form of personal identifiers is the largely unfettered access to social media domains, where information sharing is encouraged by the notion of belonging to a community. While these communities expanded exponentially with the growth of online membership, there was no apparent concern from both the users and the operators of the domains, that personal identifiers shared on the site needed to be protected. This is largely the result of the ethos that generated the communities, whereby sharing is a good thing, with no downside. In most instances, and with most participants, there has been very little awareness of the risks to uncontrolled information sharing, until exploitation of this weakness has led to serious cases of identity theft and massive financial losses. Additionally, and particularly with the more vulnerable elements of society and the younger generations, with little understanding

[17] "**SurPRISE** - Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe", FP7 project under topic: SEC-2011.6.5-2: The Relationship between Human privacy and security, 2012 - 2015.

or background in privacy protection, social media have been a successful *terroir* for exploitation by criminals, sex offenders or terrorist recruiters.

More recently, social media have come under increased pressure to enhance their data protection and strengthen their data usage protocols, as has entry into force in the EU of GDPR forced these companies to re-assess their privacy policies, certainly with regard to their European customers. These developments and the mis-steps of the recent past have created a new privacy awareness that can only be beneficial in forcing a change in how social media sites manage information and protect users from unwarranted intrusions into their privacy and safety. Here win-win solutions for individual privacy and for citizen security are clearly possible.

Social media sites take little responsibility for the information posted by their users. Generally, censure is limited to offensive postings, but little is done to verify that information is factual, accurate or true. Because of this fundamental weakness and the broad social appeal these sites have, they are the perfect conduit for manipulation of public attitudes, perceptions and behaviours. While in some cases this has innocuous consequences, such as promoting the usage of a particular product or service (similarly to traditional advertising in the past), the same is not true where manipulation is directed by foreign state actors bent on inflicting political damage to national governments or, in some extreme circumstances, undermining the societal values of competing states. Social media-based information and opinion has proven to be resilient to criticism and is often the first source of information for a significant part of the population. Uniquely, it tends to be sought by those looking for arguments to reinforce their beliefs, rather than researching different views[18]. Even when there is the interest to confirm the veracity of information, it is increasingly difficult for individual users to check the validity and the source quality of such fast flowing and seemingly credible information.

Countering the impact of social media manipulation is a growing concern in many countries, particularly in open societies where the political process is governed by democratic institutions that operate transparently. If beliefs and behaviours can be influenced undemocratically through targeted social media campaigns based on untruths and misinformation, the fundamentals of democracy are challenged. This a real threat to society that requires a strong response, which must start from social media operators and, if unsuccessful or inadequate, be subjected to regulatory scrutiny and ultimately, sanctioned with meaningful penalties. Too much is at stake to leave the resolution to market forces, self-policing or an awakening of the public.

5. Tools for a symbiotic security and privacy friendly environment

Technologies that support privacy best practices may not be funded because there is no immediate market benefit to implement them and, therefore, should be preferentially considered for access to publicly available funding streams. Highlighted below are technology development opportunities that could be further investigated:

I. Data usage monitoring and control, enabling individuals to "own" usage of their data

- Sticky policies (policies that accompany data sets, when they are transferred from one data user to another) enabling users to establish how their data is used beyond the boundaries of the first data interaction. Similar tools can also provide transparency on when data is accessed (by whom/for what) and should be considered a best practice.
- Applications that allow the disabling of data correlation to ensure that an individual's

[18] "Echo Chambers on Facebook" Walter Quattrociocchi, Antonio Scala, Cass R. Sunstein (2016).

identifier data sets cannot be correlated or subjected to subsequent scrutiny by big data analytics.

- Approaches (models, languages, techniques) for specifying and enforcing data usage restrictions.
- Privacy breach detection technologies.
- Transparency best practices about the usage of end user data e.g. Estonian government e-services[19] give citizens control over what data and when, was accessed.

II. Ethics, methodologies, processes, best practices and tools to enable privacy/security by design

- Methods and languages for specifying privacy and security requirements over data and their processing.
- Privacy Impact Assessments, based on agreed methodologies, tools and ethics standards, should be required for all (major) security enhancement projects, both public and private.
- Tools to enforce the principle of minimum-privilege, e.g. need-to-know.
- Tools to enforce and control the separation of data from the execution of associated applications.
- Tools for accountability and auditability (including watermarking technologies).
- Processes, best practices, training and methodologies for privacy engineering - e.g. a national identity card does not need to carry all the individual's identifiers, such as the complete birth date; the year alone would be sufficient, with the rest on government databases. The US is now starting to ask visitors to include their social media ID in official forms[20].
- Privacy and security assurance (certification and standards by independent organizations) of software and hardware solutions/providers.
- Incentives for secure and privacy engineering.
- Enhancing opportunities for services that report breaches (e.g. online governmental services, bug bounty programs, open source modules, etc.), similarly to incentivising whistleblowing to discourage corporate crime.
- Improve relevant regulation to ensure it is comprehensive in its approach.
- Encourage simplicity, where possible, to discourage temptation to make privacy too difficult to enforce.

III. Technologies that enable outsourcing of secure data processing to third-parties (even with untrusted providers)

- Homomorphic computing algorithms and techniques.
- Secure multiparty computational techniques.
- Approaches to selective data sharing and processing.
- Locked-in anonymisation and pseudonymisation.

[19] http://estonianworld.com/security/right-mix-estonia-ensures-privacy-access-e-services-digital-age/

[20] https://www.computerworld.com/article/3153305/security/us-collects-social-media-handles-from-select-visitors.html

IV. Technologies and methods that enforce company/organization security/privacy policy

- Flexible security and privacy policies.
- Bring-your-own-device protocols.
- Advances access and usage control detection techniques and services.
- Attribution-based identities and encryption techniques.
- Models and languages for specifying access control policies and selective data sharing restrictions.

V. Technologies that reduce the chance and impact of users giving up their privacy rights involuntarily

- Privacy by default so that the end-user does not need to be aware and familiar with the security measures as the system embeds privacy properties.
- Tangible security technologies that provide dedicated hardware solutions that people can easily recognize and understand (like classic home keys).
- Encrypted messaging, e.g. an easy-to-use system, that enables sending email and similar messages without the risk of interference and discovery.
- Usability and standardization of privacy tools to enable simple control over digital interfaces (such as cookies[21] or privacy configurations of internet services).
- Risk management technologies, formal models and techniques which allow end-users to control privacy-related data and configurations easily (privacy dashboards with recommended settings aligned with best practices).

VI. Techniques for secure and private data management and processing

- Effective and efficient techniques for providing privacy and security of data collected from, stored at, processed by or shared with third parties.
- Techniques for assessing data quality and trustworthiness (also based on provenance).
- Techniques to assess compliance with data usage and privacy policies in data management and processing.

Encouraging win-win opportunities between security and privacy helps build a more trusting society and a well-functioning and inclusive economy.

The following measures could help to strengthen both privacy and security:

a) develop non-intrusive security;
b) oversight: regulate (on-line/physical) surveillance activities;
c) transparency and accountability;
d) user centric data protection mechanisms and regulations;
e) effective digital identity management that can accommodate anonymity when needed;
f) user controls and protection of personal data that encourages trading and strengthens privacy.

The following table exemplifies selective scenarios indicating possible areas of conflicts (+/-) depending on selected domains and user types.

[21] https://www.hpe.com/h30683/ww/en/hpe-technology-now/Which-cookies-are-good_1620152.html

Pro/cons	**Digital protection techniques**	**On-line surveillance**	**Physical surveillance**	**IPR protection techniques**
IT users	accountability (-) reliability of merchant / dealer (+)			free use (-)
LEA	less control (-) increased cyber-crime prevention (+)	enforcement (+) cyber-crime prevention (+)	enforcement (+) crime prevention (+)	
Citizens	reliability on the systems (+)	cyber-crime and crime prevention (+) privacy loss (-)	crime prevention (+) privacy loss (-)	free use (-)
Employees	control reduction (-) quality assurance (+)		control of work (-) help / support (+)	
Enterprises	reduced industrial espionage (+) internal complexity of processes (-)	increased control on products / processes (-)	access control (+) quality control (+) incident early warning (+)	asset protection (+) marketing (+)
Government	reduced espionage (+)			economic advantage (+)
Remediation techniques	**a)b)c)d)e)f)**	**a)b)f)**	**a)b)d)**	**c)d)**

Table 1: Table of possibly conflict areas and remediation approaches.

6. Recommendations and conclusion

Enhancing the reciprocal benefits of security and privacy is essential to a trusting society and a well-functioning and inclusive economy. The following recommendations are intended to encourage and promote synergy:

Recommendation 1: Develop non-intrusive security and empower the user.

Security is key to privacy. Without security, privacy is impossible. Security measures, tools and systems protect personal or other valuable data from unauthorized access, tampering or loss. While there are many solutions to individual security or privacy requirements, the selection and configuration of the appropriate option overburdens users. Non-intrusive security or intrinsic privacy protection can relieve the user from direct engagement.

Recommendation 2: Implement smart and practical tools and mechanisms for the identification and enforcement of IPR.

IPR of information assets should be readily identifiable. These IPRs should be supported and enforced by identifiers to assert confidentiality or availability, for example to enable the

distribution and communication of project information.

Recommendation 3: Anonymity is an important privacy feature, which should be facilitated by systems, services and infrastructure.

Anonymous access and communication is often viewed as an obstacle to security. However, balancing anonymity and identification in the digital space, should be applied similarly to the functional equivalent in the real world.

Recommendation 4: Transparency and traceability of data transfers should prevent improper usage or correlation.

Unauthorised usage of personal or valuable data should be technically preventable. Data should be indelibly marked so that it can be verified and traced, whenever it is transferred.

Privacy dashboards or other practical control tools allowing users to implement data or privacy-related configurations across different service providers would be very desirable, especially with the expansion in connected devices envisaged by IoT and IPv6.

Recommendation 5: Improve privacy protection for surveillance activities and regulate profiling/scoring activities.

Non-privacy-infringing surveillance techniques meeting the obligations of human rights conventions in Europe should be prioritised. These approaches would focus surveillance away from indiscriminate and bulk collection of information to targeted crime or terrorism investigation.

Profiling and scoring activities are currently used to predict specific behaviours of individuals, but the rules applied to the algorithms used for the analysis are unknown to all but very few analysts charged with the activity. This becomes particularly problematic when inaccurate or inappropriate data is fed into the process. Transparency features enabling some level of understanding of the process by those whose data is being used and some level of regulation over these activities may be appropriate and should be evaluated further.

Recommendation 6: Ethics, security and privacy engineering.

Ethics, security and privacy should feature in engineering training and education given the significant vulnerabilities implicit in poor implementation or unsafe behaviour by end-users. IoT will further aggravate the situation. New incentive models to encourage take-up within the education system should be considered of high relevance.

Recommendation 7: Tools to verify credibility of information disseminated through social media.

Create tools to trace the origin and assess the credibility of social media-based information liable to affect the safety and security of citizens. Educate citizens about methods for critical assessments of social media messages and sources. Special focus on knowledge dissemination targeting younger generations.