The Privacy & Security Research Paper Series

Privacy and Security in Europe

issue #6
The Privacy & Security - Research Paper Series

Edited by Centre for Science, Society & Citizenship
Co-edited by University of Westminster – Communication and Media Research Institute
ISSN 2279-7467

Privacy and Security in Europe
Authors:
Christian Fuchs. University of Westminster, United Kingdom.

Research Paper #6
Date of Publication: May 2013

Acknowledgement: The research presented in this paper was conducted in the project “PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action”, funded by EU FP7 SECURITY, grant agreement no. 285635

This paper is an output of PACT’s Work Package 7 “Dissemination and Coordination”

All rights reserved.
No part of this publication may be reproduced, distributed or utilized in any form or by any means, electronic, mechanical, or otherwise, without the prior permission in writing from the Centre for Science, Society and Citizenship. Download and print of the electronic edition for non commercial teaching or research use is permitted on fair use grounds. Each copy should include the notice of copyright. Source should be acknowledged.
© 2013 PACT
http://www.projectpact.eu
Privacy and Security in Europe

Abstract:
The overall task of this paper is to contribute to the analysis of the relationship of privacy and security in Europe. Critical observers have pointed out that since 9/11, Europe has followed a path of increased citizens’ surveillance that puts privacy concerns at risk. The question that arises is if a trade-off between privacy and security is a necessary political option, or if alternatives exist. The paper contributes to this discussion by first presenting theoretical reflections that are then used for conducting a policy analysis of recent EU policy documents that focus on the relationship between privacy and security in Europe (European Security Strategy 2003, Report on the European Security Strategy 2008, Stockholm Programme 2010, EU Internal Security Strategy 2010-2014). The analysis shows that the relationship of privacy and security in Europe is a hot policy issue that is hotly contested within the European public sphere.

Keywords: PACT, privacy, security data protection, surveillance, Europe
1. Introduction

This paper stands in the context of “PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action” (see http://www.projectpact.eu/), which is a 36 month research project funded by the European Union’s Security Research Programme.

The multinational consortium constituting the PACT team shares the common vision that “those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety” (Benjamin Franklin). PACT believes that security, privacy and fundamental rights are not necessarily in tension, but that they may all be pursued together. The web of rich and nuanced relations between security and privacy go well beyond any simplistic formula and can be correctly understood only by considering them within the context of complex of societal and cultural interactions.

Questions about what is more important in the relationship between security and privacy, or about how much privacy citizens are willing to give up for security, have shaped the scholarly and policy debate since 9/11. This paper wants to contribute to the discussion of the following questions: How can the relationship between privacy and security be conceptualised? How shall these two concepts best be related in the political realm? What is meant by “privacy” and “security” in this context? And how does the relationship of privacy and security matter for Europe?

There have been a dramatic increase and intensification of surveillance after 9/11 (Lyon 2003b, 2007). In “the wake of the terrorist attacks on America in September 2001, the climate of political and public acceptability appears to have become more accepting of the idea of being monitored” (Jewkes 2011, 219). David Lyon (2007, 184) suggests that the welfare state is being superseded by “the safety state”. There is an increased focus on law & order politics. 9/11 has resulted legally in the definition of “states of exception”, “most notably for preemptive war, domestic surveillance, and the torture of terrorist suspects; and practically” in “the establishment of elaborate surveillance rituals for citizens (for example, airport screening) and the outsourcing of lucrative security contracts to private industries” (Monahan 2010, 6). “Capturing terrorists before they strike became an obsessive goal of many governments after 9/11” (Lyon 2003a, 52). 9/11 has resulted in “the misguided and socially disruptive attempts to identify terrorists and then predict their attacks” (Gandy 2009, 5). “In this generalized control society, governed by the managerial model, the ability to anticipate individual behaviour, identify the probability of a specific behaviour and construct categories based on statistical frequency is the common thread among the ‘styles’ of marketing specialists, the ‘scores’ of financiers and the ‘profiles’ of the police” (Mattelart 2010, 184).

Also in the European Union the belief that security, understood as “the protection of the individual, but also of the collective self, the nation state”, “is a core value threatened by ‘global terrorism’ has spread” after 9/11 (Bigo 2010, 263). The EU FP6 CHALLENGE research project (The Changing Landscape of European Liberty and Se-
Security) concluded that after 9/11 “the framings of the relationship between liberty and security” has been redefined “in favour of control, surveillance, policing, and war” (Bigo, Guild and Walker 2010, 12). European security politics have therefore “been mainly oriented towards the right for governments to strengthen coercive and surveillance security measures” (Bigo 2010, 265f). “Security is then, conceptually, reduced to technologies of surveillance, extraction of information, coercion against societal and state vulnerabilities, in brief to a kind of generalized ‘survival’ against threats coming from different sectors, but security is disconnected from human, legal and social guarantees and protection of individuals” (Bigo 2008, 12).

These concerns formulated by scholars point towards the apprehension that the relationship between privacy and security has after 9/11 in Europe and the Western world in general been increasingly defined in favour of state/military/police security, that privacy concerns have been put aside and that the more extensive and intensive use of more surveillance technologies has been traded off against less privacy. It therefore looks like privacy and security have in politics been increasingly treated based on a trade-off model, where an increase in one parameter results in a decrease of the other parameter and the other way around. But the question is if there are alternatives to these assumptions? For dealing with this question, this paper first presents theoretical reflections on the notions of privacy and security (section 2), then based on this theoretical discussion analyses recent EU policy documents that focus on privacy and security in Europe (section 3) and finally draws some conclusions (section 4).

2. The Notions of Privacy and Security

Despite that “people have cared about privacy since antiquity” (Solove 2011, 4), the legal conceptualisation of privacy has emerged quite recently, namely in the late 19th century. Indeed, the legal concept is often associated to the well-known article “The right to privacy”, written by Samuel D. Warren and Louis D. Brandeis (1890) that was published in the Harvard Law review. The two American academics strongly called for the recognition and the protection of the right to privacy. Since then, privacy has remained a complex concept, which is reflected in the circumstance that there are multiple ways for defining it and no overall consensus on how to use this notion.

While some authors attempt to reduce privacy to a narrow understanding (i.e. intimacy or secrecy), others propose a broader definition. Various scholars also developed typologies of privacy in order to insist on the plurality of practices (information gathering, processing, dissemination, etc.) that should be covered under the rubric of privacy. So for example Roger Clarke (2006) distinguishes four types of privacy: privacy of the person/bodily privacy, privacy of personal behaviour, privacy of personal communications, privacy of personal data. Herman Tavani (2008) distinguishes between restricted access theories, control theories, and restricted access/limited control theories of privacy. The restricted access theory of privacy sees privacy given if one is able to limit and restrict others from access to personal information and personal affairs. The control theory of privacy sees privacy as control and self-
determination over information about oneself and over the access to one's personal affairs. The restricted access/limited control theory (RALC) of privacy tries to combine both concepts. It distinguishes “between the concept of privacy, which it defines in terms of restricted access, and the management of privacy, which is achieved via a system of limited controls for individuals” (Tavani 2008, 144).

Privacy theory has recently further developed the privacy concept, especially by the assumption that privacy can not only benefit or harm the individual, but also society, and is therefore a social and societal concept. Thus privacy is presented as a societal value per se, contributing to enforce order in society. Consequently, privacy problems can be harmful for individuals and also for society as a whole.

Another newer development in privacy theory is the assumption that privacy is not an absolute value, but a form of contextual integrity (Helen Nissenbaum): if privacy should be protected or not depends on the situation, the type of information, the subject/group. Contexts are e.g. education, health care, psychoanalysis, voting, employment, the legal system, religion, family, and the marketplace (Nissenbaum 2010).

Daniel Solove has advanced an approach that is comparable to the one by Nissenbaum. “The value of privacy should be assessed on the basis of its contributions to society. Protecting individual privacy need not be at society’s expense – in fact, the value of safeguarding people’s privacy should be justified by its social benefits. [...] Individualism should be incorporated into the conception of the common good, not viewed as outside it” (Solove 2008, 91). Ferdinand Schoeman lists aspects of privacy, including that it is relative to individuals/groups, roles, contexts, and objectives. “A privacy attribution pertains to certain subjects (S), is about certain matters (M), is relative to certain people (P), in certain roles (R), in certain contexts (C), and typically for certain associational objectives (O)” (Schoeman 1992, 106f).

The question that arises is therefore, in which situations benefits or harms society and a general heuristic can therefore be to assess privacy in each context depending on its relation to values such as democracy, welfare, justice, equality, freedom, participation, inclusion, sustainability, or solidarity.

The state-oriented notion of security is focusing on threats to one state and its citizens that are posed by other nations or groups such as terrorists or organised crime.

The Welsh School of Security Studies (e.g. Ken Booth, Richard Wyn Jones) “challenged the definition of security purely in terms of military threats to the state” (Peoples and Vaughan-Williams 2010, 9). It rather sees five security sectors: military, environmental, economic, political, societal. It assumes that “people are threatened by a multitude of issues: yes war, but also poverty, famine, political oppression, and environmental degradation to name but a few (Peoples and Vaughan-Williams 2010, 23). Representative of Securitization Theory argue in contrast “that because ‘security’ carries a specific military connotation historically, its application to non-military issues such as migration and economics can be highly misguided” (Peoples and Vaughan-Williams 2010, 30). The Copenhagen School’s (e.g. Barry Buzan, Ole Wæver) Securitization Theory argues that “security, as a concept, is fundamentally about survival: it is when an issue is represented as posing an existential threat tot he survival of a refer-
ent object. [...] According to Securitization Theory, when an issue comes to be treated as a security issue, it is justifiable to use exceptional political measures to deal with it. In other words it is securitized: we treat it with the same degree of urgency as we would a military threat” that “justifies responses that go beyond normal political practices” (77). Referent objects can be military, environmental, economic, cultural, political (80). Security “is an outcome of a securitization process which is constructed socially and politically through the discursive practices of social agents” (Bigo 2008, 125).

At a high level of abstraction, security can be understood as “the alleviation of threats to cherished values; especially those which, if left unchecked, threaten the survival of a particular referent object in the near future” (Williams 2008, 5).

The question is, which potential relations there are between security – understood as the absence of survival threats and survival risks for individuals and society – and privacy (or other values like equality, justice, welfare, freedom, sustainability, participation, inclusion, solidarity).

Which ways are there for causally relating two entities A and B? Exactly four: 1) preference is given to A, 2) preference is given to B, 3) A and B are seen as independent, 4) A and B are seen as mutually constitutive. Wolfgang Hofkirchner (2010, 36ff) distinguishes these four worldviews and speaks of reductionism, projectivism, disjunctivism/dualism, integrativism/dialectic. The fourth view is the one that assume a dialectic between A and B. A dialectic means the simultaneity of difference, interdependence, and mutual constitution. Hegel therefore described the negative as contradiction that contains difference and connection at the same time. The “negation is at the same time a relation, is, in short, Distinction, Relativity, Mediation” (Hegel 1830, §116). “The one is made visible in the other, and is only in so far as that other is. Essential difference is therefore Opposition; according to which the different is not confronted by any other but by its other. That is, either of these two (Positive and Negative) is stamped with a characteristic of its own only in its relation to the other: the one is only reflected into itself as it is reflected into the other. And so with the other. Either in this way is the other’s own other” (Hegel 1830, §119).

| reductionism | A is explained, causally determined, dominated by A |
| projectionism | A is explained, causally determined, dominated by A |
| dualism | A and B are seen as causally independent and autonomous existsences |
| dialectic | A and B are different and connected, they depend on each other and constitute each other mutually |

Table 1: Four worldviews (based on: Hofkirchner 2010, 37)
<table>
<thead>
<tr>
<th>Type of argumentation</th>
<th>Security as a condition of society</th>
<th>Human values (privacy, equality, justice, welfare, freedom, sustainability, participation, inclusion, solidarity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reductionism</td>
<td>Nothing-to-hide argument</td>
<td>B is explained, causally determined, dominated by A</td>
</tr>
<tr>
<td></td>
<td>(Solove 2011, chapter 2):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“If you are not a criminal or terrorist, then you got nothing to fear from the application of surveillance technology and therefore nothing to hide”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All-or-nothing fallacy (Solove 2011, chapter 3):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“For protecting security, we need to reduce/abolish privacy because the latter shields criminals and terrorists”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Pendulum Argument (Solove 2011, chapter 3):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Times of exception, such as terror and war, require the curtailment of civil liberties”.</td>
<td></td>
</tr>
<tr>
<td>Projectionism</td>
<td>The privacy-first-argument:</td>
<td>A is explained, causally determined, dominated by A</td>
</tr>
<tr>
<td></td>
<td>“Privacy or other values are absolute and need to be protected even if this results in less security”.</td>
<td></td>
</tr>
<tr>
<td>Dualism</td>
<td>The privacy-security-dualism:</td>
<td>A and B are seen as causally independent and autonomous existences</td>
</tr>
<tr>
<td></td>
<td>“Privacy and security can both be achieved. They are not causally connected”.</td>
<td></td>
</tr>
<tr>
<td>Dialectic</td>
<td>Privacy-security-dialectic:</td>
<td>A and B are different and connected, they depend on each other and constitute each other mutually</td>
</tr>
<tr>
<td></td>
<td>“A society that respects privacy of the weak and bases itself on equality can enhance and secure stability and social peace, which can further enhance basic rights. Privacy enhances security and security should be understood and implemented in a way that enhances privacy”.</td>
<td>A and B are different and connected, they depend on each other and constitute each other mutually</td>
</tr>
</tbody>
</table>

Table 2: Four worldviews on the relationship between privacy and security

An example for the nothing-to-hide argument was provided by Google's CEO Eric Schmidt in December 2009, when he was reacting to privacy concerns about Google by saying: “If you have something that you do not want anyone to know, maybe you
should not be doing it in the first place”¹. The argument implies that Schmidt thinks that there can be no harm from making all private information public. The problem of the nothing-to-hide argument is that it assumes that surveillance can do no harm, such as discrimination, exclusion, a culture of suspicion, false suspicions, and injustice. Security tends to be interpreted as increase of the use of surveillance technology.

An example for the all-or-nothing-argument is that the FBI released a flyer about “Potential Indicators of Terrorist Activities Related to Internet Café”², in which it says that one should consider suspicious “people who: are overly concerned about privacy, attempts to shield the screen from view of others”. A concern for privacy is equated with a likelihood of being a terrorist, which shows that privacy is considered as shielding terrorists and is an indirect expression of the wish to curtail privacy. Another example is that after 9/11 the US government conducted surveys, asking: “Should the government take all steps necessary to prevent additional acts of terrorism in the U.S. even if it means your basic civil liberties would be violated? Or should the government take steps to prevent additional acts of terrorism but not if those steps would violate your basic civil liberties?”³. A majority disagreed to curtailing liberties (January 2002: 47% curtailment, 49% no curtailment; August 2003: 29% curtailment, 67% no curtailment) (ibid).

The problem of the all-or-nothing-fallacy is that those “defending the national-security side of the balance often view security and liberty as zero-sum tradeoff. […] The argument is that security and civil liberties such as privacy can never be reconciled. Every gain in privacy must be a loss in security. Every gain in security must be a loss in privacy. […] Sacrificing privacy doesn't automatically make us more secure. Not all security measures are invasive of privacy. […] Security and privacy need not be mutually exclusive. For example, one security response to the September 11 attacks was to lock the cockpit doors on airplanes. This prevents a terrorist from gaining control of the plane. Does it invade privacy? Hardly at all” (Solove 2011, 34).

An example for the pendulum argument can be found in a speech by then US Attorney General Alberto Gonzales: “It has long been recognized that the President's constitutional powers include the authority to conduct warrantless surveillance aimed at detecting and preventing armed attacks on the United States. Presidents have uniformly relied on their inherent power to gather foreign intelligence for reasons both diplomatic and military, and the federal courts have consistently upheld this longstanding practice. If this is the case in ordinary times, it is even more so in the present circumstances of our armed conflict with al Qaeda and its allies. The terrorist surveillance program was authorized in response to the deadliest foreign attack on American soil, and it is designed solely to prevent the next attack. After all, the goal of our enemy is to blend in with our civilian population in order to plan and carry out

---

¹ http://www.youtube.com/watch?v=A6e7wfDHzew
future attacks within America. We cannot forget that the 9/11 hijackers were in our country, living in our communities”). The pendulum argument faces the problem that sacrifices of human rights in times of crisis often sacrifices “the rights and liberties of others rather than” the ones of the majority population – “minorities and dissidents” (Solove 2011, 57). “Not only is the pendulum argument wrong in falsely assuming that sacrifices of rights and civil liberties are necessary, it also misses the point about why rights and civil liberties matter. The protection of liberty is most important in times of crisis, when it is under the greatest threat” (Solove 2011, 61). Solove warns about the argument that exceptional times require exceptional measures: If the President “felt that randomly shooting people was necessary to fight the War on Terrorism, he could so in spite of murder laws” (Solove 2011, 84).

The privacy-first-argument sees privacy as absolute value and says that a reduction in security is acceptable if privacy rights are protected. Like the all-or-nothing fallacy it assumes a trade-off-model of privacy and security, in which an increase of one side necessarily results necessarily in a decrease of the other side: more privacy is seen as being only achievable by less security. A question listed on answers.com, asks: “Should individual claims of privacy be valued above claims of societal welfare?” One possible answer listed is: “Yes personal privacy is one of the greatest gifts of the constitution. I prefer privacy over security, however due to the current feelings in the U.S. and it’s liberal leanings I doubt that there will ever be true personal privacy again”⁵. A contributor in an online discussion forum writes in the thread “What is more important? Privacy or security?”: “I value privacy over security. That doesn’t mean that I don’t think security is not important, on the contrary. However I do believe that in the past decade far too many decisions were made which sacrificed our privacy for ‘the greater good’ i.e. a sense of security. Yet true security is impossible. It’s about the feeling in your head and it’s mental that governments sometimes go Big Brother on us. They make us afraid and then try to push the boundaries further”⁶. The privacy-first argument sets privacy as absolute value that is indirectly proportionate to security. It sees privacy always as necessary, even if it has negative consequences for society. It does not take criticisms of privacy, such as that it is individualistic, patriarchal, Western-centric, shields inequality and the powerful, into account.

The privacy-security dualism argument assumes that privacy and security are independent and can be achieved at the same time without a relation to each other. An example is the concept of privacy by design. Ontario’s Information and Privacy Commissioner Ann Cavoukian argues that “adding privacy measures to surveillance systems need not weaken security or functionality but rather, could in fact enhance the

---

5 http://wiki.answers.com/Q/Should_individual_claims_of_privacy_be_valued_above_claims_of_societal_welfare
6 http://s7.zetaboards.com/Ceterum/topic/8474526/1/
overall design”. This means that “privacy protections are engineered directly into the technology. [...] The effect is to minimize the unnecessary collection and uses of personal data by the system, strengthen data security, and empower individuals to exercise greater control over their own information. The result would be a technology that achieves strong security and privacy”. “I am deeply opposed to the common view that privacy is necessarily opposed to, or an obstacle to, achieving other desirable business, technical or social objectives. For example: * Privacy versus security (which security? informational, personal or public/national?) * Privacy versus information system functionality * Privacy versus operational or programmatic efficiency * Privacy versus organizational control and accountability * Privacy versus usability. The zero-sum mentality manifests itself in the arguments of technology developers and proponents, vendors and integrators, business executives and program managers – that individual privacy must give way to more compelling social, business, or operational objectives. At the same time, defenders or advocates of privacy are often cast, variably, as Luddites, technological alarmists, or pressure groups largely out of touch with complex technological requirements and organizational imperatives”.

Privacy by design would mainly mean the creation of privacy-enhancing technologies. An example Cavoukian describes is a video surveillance system developed at the University of Toronto that distorts humans and only makes them visible if a secret key is entered. CCTV can result in anticipatory compliance and solving or preventing crimes seems not to be connected to the use of CCTV. Privacy by design and its dualistic logic (A and B) are “a technocratic approach to managing personal information” that “fails to grasp how power shapes the agenda and overall context in which struggles over technological design occur” (Winseck 2003, 188). It is based on belief in a technological fix to societal problems.

A dialectical analysis of the relationship of human values (such as privacy, equality, justice, welfare, freedom, sustainability, participation, inclusion, solidarity) and security assumes that fostering broader societal goals that respect human values is a good way for advancing security of society and that conversely, a state of peace in society, is a good condition for the realisation of human values. It is based on a realistic analysis of the relationship of society and phenomena such as crime, terrorism, surveillance, which means that it neither calls for law-and-order policies or the reliance on surveillance technologies because it considers such measures as purely reactive and not addressing existing problems societal causes nor ignores the actual existence of problems that affect common people and for which solutions are needed.

A realistic analysis of security and human values can be grounded on some basic assumptions:

- Actual problems have causes in society, the lived realities of humans and power structures.
- Existing societal problems are shaped by contemporary structures of society.

---

7 http://www.ipc.on.ca/images/Resources/trans-tech.pdf
• One should not overestimate the importance of technologies and law & order policies for solving societal problems. There are no technical and administrative fixes to societal problems:
Law and order policies see the solution of crime in tougher laws, surveillance, and control. They emphasize “deterrence and repression and voices support for more police, more prisons and a tougher criminal justice system” (Jewkes 2011, 62).

• Technological determinism inscribes power into technology; it reduces power to a technologically manageable phenomenon and thereby neglects the interaction of technology with society and power structures:
Bruce Schneier (2009) argues that security technology measures often are taken for making citizens feel safer, although they do not make society safer. There would be a security illusion or security ideology that Schneier terms security theatre: “Security theater refers to security measures that make people feel more secure without doing anything to actually improve their security”.

• The use of security technologies should always respect privacy, democracy, freedom, equality, and human rights:
One should always ask the questions like: Is a certain security technology needed? For what aims and how likely will these aims be achieved? Does the use conflict with privacy rights, democracy, freedom, equality, or other human rights? Can the technology or another method be used in a way that does not infringe rights and human values? Which potential harms for individuals, groups, organisations and society arise from the use of a security technology and how can they be avoided?

• One should also not underestimate the existence of societal problems and fears. Fears of crime and terrorism are not mere illusions, are often instrumentalized by right-wing populism, and the main victims of crime and terror are everyday people.

• One should also give attention to crimes of the powerful and the misuse of power, which requires a strong and attentive civil society.

• Overcoming problems in society requires changes that address the causes of societal problems. For addressing measures that aim at overcoming problems one should neither be naïve nor disillusioned.

The discussion shows that there is not just one possible relationship between privacy and security, but the potentials between these two phenomena form a complex field with multiple potentialities. The question that arises next is what happens when we go from theory to political reality, i.e. how does the political reality of the relationship of privacy and security look like in Europe? For attempting an answer, we will present an interpretation of EU policy documents in the next section of this paper.

3. Privacy and Security in European Policy Documents

In 2003, the European Council (2003) passed the European Security Strategy. “Security is a precondition of development. Conflict not only destroys infrastructure, including social infrastructure; it also encourages criminality, deters investment and
makes normal economic activity impossible. A number of countries and regions are caught in a cycle of conflict, insecurity and poverty” (European Council 2003). In this strategy, the European Council acknowledges and mentions that security has not just to do with military and state security, but with issues such as poverty, diseases, hunger, malnutrition, global warming, energy consumption, environmental degradation, depletion of natural resources, lack of democracy, corruption, etc. But when it comes to actually defining security threats, questions of equality, social conditions, class, distribution and the environment are not mentioned as security threats, the focus is rather purely on issues relating to state security: The European Council (2003) defines as key threats to Europe terrorism, the proliferation of weapons of mass destruction, regional conflicts, state failure and organised crime. “Taking these different elements together – terrorism committed to maximum violence, the availability of weapons of mass destruction, organised crime, the weakening of the state system and the privatisation of force – we could be confronted with a very radical threat indeed” (European Council 2003, 5).

Non-military and state issues are partly seen as causes of security problems, but are not defined as security issues themselves, as a broader notion of security would however imply. As a solution to the identified security threats, the European Council (2003) sees “effective multilateralism”, which can be read as an implicit criticism of perceived US unilateralism. The European Security Strategy therefore concludes: “Acting together, the European Union and the United States can be a formidable force for good in the world. Our aim should be an effective and balanced partnership with the USA” (European Council 2003, 13).

In 2008, the European Council (2008) reported on the implementation of the European Security Strategy. In the resulting document, one can notice a profound shift in the understanding of security from military and state security towards a broader concept of “human security”: “We have worked to build human security, by reducing poverty and inequality, promoting good governance and human rights, assisting development, and addressing the root causes of conflict and insecurity” (European Council 2008, 2). The European Council (2008) reviews the security threats formulated in 2003 - terrorism, weapons of mass destruction, organised crime, regional conflicts, state failure, but adds a number of security threats that need to be addressed. One of these issues is energy security. Here one could reduce energy to a military issue by arguing that old and other resources are contested and that a certain region or country’s (EU, USA) access to energy resources needs to be secured and defended. The European Council avoids such a securitisation strategy that turns energy into a military issue, but suggest a partnership for fostering alternative energy sources: “With our partners, including China, India, Japan and the US, we should promote renewable energy, low-carbon technologies and energy efficiency, alongside transparent and well-regulated global markets” (European Council 2008, 5). Other topics that are seen as security issues are climate change that can result in environmental disasters and degradation as well as resource conflicts, water supply, poverty, human
rights, sexual violence, and – more in line with the military and state-oriented understanding of security – piracy.

The European Council does not rule out military actions, in contrast it calls for European armament by saying that support is needed for “a competitive and robust defence industry across Europe, with greater investment in research and development” (European Council 2008, 10). At the same time, military means are not seen as the ultimate solution, but a multidimensional security strategy is recommended that also includes longer-term poverty reduction and an important role of civil society and NGOs: “Civil society and NGOs have a vital role to play as actors and partners” (European Council 2008, 9). Human security would mean a “people-based approach” (European Council 2008, 10).

Two topics that are absent from the discussion of security issues are financial/economic instability/crisis and socio-economic inequality. The global economic crisis that started in 2008 has made evident that financial speculation and deregulated financial and economic markets pose a threat to human security by increasing the volatility of the economy and the risks of increased bankrupts, unemployment, poverty (Stiglitz 2010). Connected to the issue of economic deregulation is the circumstance that the unequal distribution of wealth and income has been massively rising within countries in the past decades and is very high at a global level (Held and Kayaa 2007). Wealth and income gaps pose threats to social security of humans and society. Guy Standing (2011) has for example spoken of the rise of a preacriat as a socio-economic insecurity and a labour insecurity. Associated security risks have in the past decades in many countries been the undermining of social security in terms of education, health care, the pension system. Socio-economic issues have rather been neglected in the 2008 report of the European Council, although this was the year when the global economic crisis hit Europe and the world.

In 2010, the European Council (2010a) adopted the Internal Security Strategy. Security is in this strategy defined as “protecting people and the values of freedom and democracy, so that everyone can enjoy their daily lives without fear” (European Council 2010a, 4). It defines common threats to Europe: terrorism, serious and organised crime, cyber-crime, cross-border crime, violence (youth violence, hooligan violence), natural and man-made disasters (droughts, earthquakes, energy shortages, floods, ICT breakdowns, storms), other common phenomenea (such as road traffic accidents). This formulation of security threats has an obvious focus on crime. Besides that and the usual focus on terrorism, also technical and natural risks are mentioned. In the previous evaluation document, also poverty and human rights violations were mentioned, which are now not mentioned as security risks. So no focus is given to social security issues such as poverty, income and wealth (in)equality health care, education, retirement as well as to economic issues such as unemployment and economic crisis. The EU Internal Security Strategy mainly adopts a state institution-centred focus on how to tackle security risks. It defines a European Security Model that consists in threat prevention and anticipation, effective work of institutions such as Europol, Eurojust, Frontex and the Counter-Terrorism Coordinator, data sharing
between law enforcement institutions (Schengen information System, the “use of DNA and fingerprint data”, p. 8), cooperation and coordination of law enforcement institutions in operations, integrated border management, innovation in security technologies.

One of the main strategies defined by the EU Internal Security Strategy is the increased development and use of surveillance technologies: Prevention and anticipation of security threats should be based on “a proactive, intelligence-led approach” in order to have “a stronger focus on the prevention of criminal acts and terrorist attacks before they take place” (European Council 2010a, 11). For this purpose, “analytical tools or early-warning systems” (12) should be used. The further development of surveillance systems are also explicitly recommended in border security, where the document recommends “the continued development of the European Border Surveillance System (EUROSUR)” and argues that “[n]ew technologies play a key role in border management” (14f). In general, it is recommended that new surveillance technologies are developed, applied and used in such a way that they allow European-wide exchange of qualitatively different data: “It is necessary to work together to promote and develop new technologies through a common approach as well as cutting costs and increasing efficiency. In the field of technology, it is also important for the public and private sectors to work together. [...] The interoperability of different technology systems used by any agency or service must be a strategic objective” (15).

The foundations of the EU Internal Security Strategy were laid down in the Stockholm Programme, the European Union’s five year plan (2010-2014) in the areas of justice and internal security (European Council 2010b). Like the Internal Security Strategy, the Stockholm Programme contains a general commitment to privacy, but does not further engage with ethical issues in the suggested surveillance measures. It says that all suggested measures should respect “the right to privacy and the right to the protection of citizens’ personal data” and that the “Union must secure a comprehensive strategy to protect data within the Union and in its relations with other countries” (European Council 2010b). The Stockholm Programme introduces the basic surveillance strategy that was further laid down in the Internal Security Strategy by calling for a “proactive and intelligence-led approach” in security because in “a global world, crime knows no borders”. It also calls for upgrading „the tools for the job” because security professionals would need “the right technological infrastructure to support them” (European Council 2010b). This basically means a support for the more extensive and intensive use of surveillance technologies.

The Stockholm Programme has been criticised in the political debate. So for example the British NGO Statewatch has argued that the EU in the documents commits to privacy, freedom and democracy, but that the “problem is that while we can all can agree on the ‘everlasting values’ of freedom and privacy, the record of the EU is that it has put security before liberties and rights time and time again since 11 September 2001. If the ‘values’ of the EU are not matched by the practice, what good are values?” (Bunyan 2010, 1).
The assumption that surveillance technology can control and prevent crime and terrorism is based on the belief that there are technological fixes to societal problems. Technological determinism inscribes power into technology; it reduces power to a technologically manageable phenomenon and thereby neglects the interaction of technology with society and power structures. Technological determinism is “typified by sentences in which ‘technology,’ or a surrogate like ‘the machine,’ is made the subject of an active predicate: ‘The automobile created suburbia.’ [...] ‘The robots put the riveters out of work’” (Marx and Smith 1994, xi). These arguments are frequently accompanied by the assumption that technology drives history (Marx and Smith 1994). Technological determinism can therefore also “be taken to mean that the laws of nature determining human history do so through technology” (Bimber 1994, 87). This form of preemptive and high-technology policing looks for security by algorithms in a world of high insecurity. It advances a fetishism of technology – the belief that crime and terrorism can be controlled by technology. Technology promises an easy fix to complex societal problems.

The question that needs to be addressed is how preemptive surveillance relates to privacy. The Internal Security Strategy says in this context that one believes in the values of “justice, freedom and security policies which are mutually reinforcing whilst respecting fundamental rights, international protection, the rule of law and privacy” (European Council 2010a, 9). The document has a dualistic approach in relating privacy and security: it wants to have both the application of more surveillance technologies for preventing crime and the respect of privacy, justice and freedom. The question if and how preventive surveillance and surveillance technologies in general can violate citizens’ privacy is not further addressed.

Armand Mattelart (2010, 164) has argued that the EU’s “mission resembles that of an intelligence service: exchange and coordination, data collection and analysis, creation of files not only on persons suspected of having committed or taken part in crimes, but also individuals presumed likely to commit them. In other words, it anticipates offences in a ‘proactive’ fashion. Its mission is also to produce reports on emerging trends in organized crime”.

Preventive and anticipative surveillance works technologically based on profiling and data mining. Profiling is “a set of technologies, which share at least one common characteristic: the use of algorithms or other techniques to create, discover or construct knowledge from huge sets of data” (Hildebrandt 2010a, 17). Data mining algorithms induce/predict habits and preferences of individuals and groups and helps “to find correlations between large sets of data collected about groups of people” (Jaquet-Chiffelle 2010, 35). They create profiles of people that are assumed to have certain attributes and show certain behaviours. “The goal of any data mining exercise is the extraction of meaningful intelligence, or knowledge, from the patterns that emerge within a database after it has been cleaned, sorted and processed” (Gandy 2003, 28).

Scholars have expressed a number of ethical and privacy concerns about preventive and anticipative surveillance. Data mining is based on the assumption that observation of past events can predict the future. The problem is that human behaviour is
not pre-determined and cannot be calculated because the human being as an active, creative being and not a computer. Its behaviour is unlike computers not deterministic. Another problem of data mining is that it provides assumptions for groups with a certain probability. But these assumptions cannot be applied to the individual because an individual may show different behaviour although s/he has been classified as being the member of a certain statistical group. “The actual assumption is based on the belief that patterns observed in the past provide useful information about activities and events that may take place in the future. [...] What is routinely ignored is the fact that predictions are made regarding averages for aggregates, rather than about any particular individual case” (Gandy 2009, 9). Resulting problems can be:

- **Rational discrimination of certain social groups (especially racial discrimination):**
  “The actual assumption is based on the belief that patterns observed in the past provide useful information about activities and events that may take place in the future. [...] What is routinely ignored is the fact that predictions are made regarding averages for aggregates, rather than about any particular individual case” (Gandy 2009, 9). As a result, social discrimination of certain groups can be the result of the application of predictive algorithms in marketing, policing, insurances, finance, the housing market, public policy, education, health care, etc (Gandy 2009). This concerns especially black and poor people. The “use of discriminatory technologies contributes to the social, economic and political disparities that continue to assign African Americans and other poor people of color to the fringes of society, and condemns many of them to a life of extreme relative deprivation” (Gandy 2009, 12). Especially after 9/11, there have been “increased possibilities for ‘racial profiling’ along ‘Arab’ lines in particular” (Lyon 2003b, 20). The danger is that Arabs and Muslims in general are considered to be terrorists until they prove not to be.

- **Categoric suspicion:** There is a danger that the presumption of innocence is removed because of algorithmic calculations (Nabeth 2010, 32).

- **Control and power inequality:** Profiling can enforce “social control” and is “used to maintain people in their initial condition” (Nabeth 2010, 33). Gutwirth and De Hert (2010, 286) speak of the emergence of “correlatable humans” and “traceable or detectable human” beings: “Profiling practices lead to an accumulation of power in the hands of those that command them and to a loss of control of the concerned individuals” (Gutwirth and De Hert 2010, 289).

- **Data abuse:** There is a threat of the abuse of the information about individuals and groups by companies and organizations (van der Hof and Prins 2010).

- **Intransparency:** “The problem is that we have very little access to which data are processed by which organisation, which knowledge is constructed with my data and how this may impact me” (Hildebrandt 2010b, 308).

- **Criminalization:** There is the danger of the attribution of certain risks (criminality, terrorism, etc) to certain groups (van der Hof and Prins 2010), especially (e.g. ethnic and religious) minorities.
• *Cumulative disadvantage*: “Cumulative disadvantage refers to the ways in which historical disadvantages cumulate over time, and across categories of experience” (Gandy 2009, 12). “People who have bad luck in one area, are likely to suffer from bad luck in other areas as well” (Gandy 2009, 116). This means that if by accident you have dark skin, are poor, live in a deprived, neighbourhood, have become unemployed or ill, etc, you are more likely to be discriminated and flagged as a risk group by data mining technologies. The arbitrary disadvantages an individual has suffered cumulate and result in further disadvantages that are enforced by predictive algorithms that calculate that based on certain previous behaviour an individual is part of a risk group and should therefore be discriminated (by not being offered a service, being offered a lower quality service at a higher price (e.g. in the case of a loan or mortgage), by being considered as a criminal or terrorist, etc). “Once they have been identified as criminals, or even as potential criminals, poor people, and black people in particular, are systematically barred from the opportunities they might otherwise use to improve their status in life” (Gandy 2009, 141). Data mining can easily intensify disadvantages and inequalities that structurally disadvantaged or racialized groups are facing. Being identified as belonging to a risk group and being therefore discriminated can also result in self-fulfilling prophecy and result in the very behaviour that was predicted (crime, terrorism, etc) although it was not present in the first instance (Gandy 2009, 187).

• *Inaccuracy*: Algorithms are not perfect and are error-prone. Therefore humans can be treated unfairly as result and there can be “far reaching consequences for basic notions such as identity, agency, liability, fair treatment and due process” (Hildebrandt and Gutwirth 2010, 367).

• *Amplification of crime and terror*: If groups or individuals feel unfairly discriminated (e.g. by racism, classism, sexism, etc), they may react to this circumstance with an intensification of hatred against those whom they perceive hates and discriminates them. If certain groups or individuals (such as Arabs) are labelled as terrorists or criminals or denied certain possibilities (such as entering a certain country, area or building) because data mining algorithms have calculated that they may be part of a risk group, there is the risk that an intensification or creation of hate can set in, which can result in the creation or intensification of the very phenomenon (crime, terror, etc) that the algorithm wanted to prevent in the first instance. Wilkins (1964/2001), Cohen (1972/2002, 226), Hall et al. (1978) and Jewkes (2011) describe this process with the concept of the deviancy amplification spiral.

4. Conclusion

EUobserver ([http://euobserver.com/](http://euobserver.com/)) is an online news service that focuses on discussions on European affairs. It is a medium well suited for gaining an overview which topics that relate to privacy and security were of major importance in the EU in
2012. A search with the keywords “privacy” and “security” resulted in a number of results that help identifying some important privacy and security issues that were relevant in the EU in 2012.

In January 2012, the EU introduced a new draft for a Data Protection Regulation that defines a right to be forgotten, the right of citizens not to be profiled, a right to personal data portability, and relatively high fines for non-compliance (up to 1 000 000 Euros and 2% of the annual worldwide turnover of a company)\(^8\). The Article 29 Data Protection Working Party criticised that the legislation de facto excludes data protection by law enforcement agencies\(^9\). No privacy protection and accountability procedures by the police and legal institutions that conduct investigations on criminal matters would be included. The EU introduced a European Cybercrime Centre. Its chief Troels Oerting says that cybercrime has become a major problem, whereas Hiekle from the European Data Protection Supervisor (EDPS) notes that the fight against cyber crime often takes place in a pro-active preventive manner by trying to link individuals who are not yet suspected of crime\(^10\). In April 2012, the EU Parliament voted for a new air data agreement that transfers data such as names, addresses, credit card data, flight details etc of all passengers who travel from the EU to the USA. The Dutch MEP Dutch Liberal MEP Sophie In’t Veld criticised: "Ask yourselves, if other countries knock on our doors, and we know that they will, [...] Cuba, China, Russia - are we willing to give them our data and (see it used) for profiling on the same terms as we are doing with the United States?"\(^11\). There are long retention periods, the data (also sensitive one) can be used for profiling. The EU has in 2012 discussed implementing a similar EU Passenger Name Record System for profiling and filtering out potential terrorists\(^12\). The German MEP Jan Philipp Albrecht argued: “There is evidence to suggest that passengers with unusual names or noteworthy dietary requests may already be regarded as suspicious, with those affected having no influence on potentially erroneous evaluations, as they have no right to access the data collected, let alone to correct or delete it”\(^13\). In July 2012, the European Parliament voted with a large majority against the Anti-Counterfeiting Trade Agreement (ACTA) that planned to implement monitoring procedures of file sharing users who infringe intellectual copyrights. The vote was preceded by large protests in several European countries and three European-wide protest days. MEP David Martin commented that the “intended benefits of this international agreement are far outweighed by the potential threats to civil liberties”\(^14\). In 2008 and 2009, Google cars that took pictures of

\(^8\) Euobserver, EU bill gives web users 'right to be forgotten'. January 25\(^{th}\), 2012.
\(^9\) Euobserver, Police largely exempt from data protection directive. April 23\(^{rd}\), 2012.
\(^10\) Euobserver, EU cyber-crime chief fears massive proliferation. September 18, 2012
\(^11\) EUobserver, Parliament gives “half-hearted” support for US data deal. April 19\(^{th}\), 2012.
\(^12\) EUobserver, EU plans for big brother data analysis must be nipped in the bud. April 24\(^{th}\), 2012.
\(^13\) Ibid.
\(^14\) EUobserver, Politicians divided on “Big Brother” Internet laws. April 25\(^{th}\), 2012.
streets in Europe for Google Street View also collected data from open Wi-Fis, which sparked a big debate in Europe. Google promised to destroy all collected data. In July 2012, Google’s privacy advisor Peter Fleischer wrote in a letter to the UK Information Commissioner that not all of these data were destroyed\textsuperscript{15}. The French data protection authority CNIL fined Google with Euro 100 000 because it retained personal data without consent. Nick Pickles, director of the UK-based Big Brother Watch, argued that the Google Street View case shows that powerful regulation of data protection, as planned by the Data Protection Regulation would be needed that has the “the powers and punishments to fully protect […] privacy”\textsuperscript{16}. The draft of the Data Protection Regulation defines fines of up to 2\% of a company’s turnover if it breaches data protection legislation.

All of these examples show that many discussions about data processing in the EU revolve around the relations between privacy/ethics and security/surveillance: The Data Protection Regulation wants to strengthen citizens’, consumers’ and users’ privacy, but at the same time wants to take concerns about the efficiency of law enforcement into account, which raises new privacy concerns. The founding of the European Cybercrime Centre has resulted in discussions about the increase of online crime on the one hand and privacy violations by preventive policing on the other hand. Also the discussions on the EU’s passenger flight data agreement with the USA and the planning of a similar European system for the purpose of trying to prevent terrorism and catching terrorists before they strike have focused on the potential negative ethical impacts of profiling and data that we previously outlined. The defeat of ACTA in the European Parliament with a majority of 438 votes against the proposal over 38 votes in favour of it that was accompanied by European-wide protests shows that there are data processing issues (such as intellectual property rights, where there is a strong concern in Europe that surveillance limits privacy and civil rights. ACTA as well as the Google Street View controversy show that debates on and controversies over the relationship of privacy and security/surveillance are not limited to the realm of the state, but also deeply penetrate the economic realm, where the basic question is to which extent companies should be allowed to commodify personal data or use such data for marketing and company purposes and if such practices violate users’ and consumers’ privacy rights.

This discussion shows that the relationship of privacy and security/surveillance is in Europe first and foremost a strongly contested issue. Policy documents such as the Stockholm Programme and the EU’s Internal Security Strategy de facto define a trade-off model that advances the development and use of surveillance technologies at the expense of privacy rights. At the same time, the EU Parliament’s vote against ACTA and to a certain degree the draft of the Data Protection Regulation are strong expression of taking measures for privacy protection, whereas other examples, such as the EU’s passenger flight data agreement with the USA advance a security agenda. Politics

\textsuperscript{15} EUobserver, Google in EU privacy row over Street view data. August 3\textsuperscript{rd}, 2012.

\textsuperscript{16} Ibid.
and policies that concern the relationship between privacy and security/surveillance are contested and controversial. Whereas there is a strong agenda in Europe that wants to put security interests over privacy rights, there are at the same time representatives of civil society, consumer protection organisation, privacy and data protection advocacy organisations, members of political parties and the European Parliaments, unions etc that remind us of the political threats connected to security politics that have a narrow understanding of security and security measures and believe in the power of surveillance technology to solve problems that have societal causes. The debate on privacy and security puts the European public sphere to a test and poses the question if the outcome of the ongoing controversies will be a Europe that protects human privacy by protecting human security (security understood in a broad way) or if Europe will increasingly trade-off privacy and civil rights against security interests so that negative features are enhanced and the European information society turns into a European surveillance society.

References


