Chapter 11
Privacy and Security – On the Evolution of a European Conflict

Matthias Leese

Abstract Privacy and security have long been framed as incommensurable concepts that had to be traded off against each other. While such a notion is rather under-complex, it has been quite persistent. In recent years, however, the relation has undergone a transformation and is now apparently conceived of as a technological issue that is set to be resolved through privacy by design. This paper retraces, through an analysis of EU security research funding, how this shift has come about, and critically assesses its potential to eventually resolve the conflict between privacy and security in a world of data-driven security measures.

Keywords Security • Privacy • Research • Horizon 2020 • European Union

Privacy and security have often been framed as conflicting concepts that must be conceived of as incommensurable and thus constitute a trade-off.[1] And although such a notion has been largely criticized for using under-complex definitions of both privacy and security, as well as for neglecting empirical examples of positive sum games and questions of whose privacy and whose security are affected,[2] the trade-off model appears quite persistent. Considering the contemporary nature of data-driven security measures, much digital ink has been spilled about the presumably weak standing of privacy in the face of a more or less overwhelming context of (inter-)national security.[3] This paper analyzes how the relation between privacy and

[1] Marc van Lieshout et al., "Reconciling Privacy and Security," *Innovation: The European Journal of Social Science Research* 26 (2013).

[2] Govert Valkenburg. "The Trade-Off Model Between Privacy and Security From a Sociotechnical Perspective. Paper presented at Computers, Privacy and Data Protection Conference, Brussels, 22–24 January." 2014.

[3] see for instance Colin J. Bennett, "What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11," in *Global Surveillance and Policing. Borders, Security, Identity*, ed. Elia Zureik and Mark B. Salter (Cullompton/Portland: Willan,

M. Leese (✉)
University of Tuebingen, Tübingen, Germany
e-mail: matthias.leese@izew.uni-tuebingen.de

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_11

security has been framed and re-framed in the field of European security research, eventually ending up as a question of privacy by design. Privacy by design, so the argument goes, enables new security technologies to be both privacy-preserving as well as effective and efficient, and thus would ultimately serve as the silver bullet that resolves the conflict/trade-off. However, this paper puts forward the claim that the notion of privacy by design rather puts old wine into new bottles, as a closer look reveals that the core problem is not tackled, but only re-framed according to the general technical scope of security research. Thus, it appears that the new emphasis on privacy and the ensuing argumentative mitigation of the conflict merely intends to comply with the EU's increased focus on normative security and at the same time renders research governance as a technological fix for the technological fix that security is conceptualized as in the first place.

The paper proceeds by providing a brief overview of the emergence of security research at the EU level over the last decade and sheds light on its underlying rationalities, *en passant* retracing how the presumed trade-off between privacy and security was framed and eventually evolved into a privacy by design approach alongside the emergence of a more normatively coined EU 'security project'. The paper concludes with a critical assessment that questions the suitability of privacy by design as the panacea that it comes advertised as.

11.1 EU Security Research – On the Emergence of a Field and a Conflict

"Security research is the new guy in town."[4] As opposed to 'traditional' fields of research funded by the European Union, research that is explicitly dedicated to the security of the EU and its citizens has only been around for the relatively short term of about a decade,[5] and has at times struggled to find its niche among related fields with a strong 'security touch', such as for instance Information and Communication Technologies (ICTs). However, fostered by 'new' and global threat scenarios,

2005); Matthias Leese, "Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs," *Computer Law & Security Review* 29 (2013); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford Law Books, 2010); Anastassia Tsoukala, "Risk-focused Security Policies and Human Rights. The Impossible Symbiosis," in *Mapping Transatlantic Security Relations. The EU, Canada, and the War on Terror*, ed. Mark B. Salter (London/New York: Routledge, 2010).

[4] J. Peter Burgess. "Ethical Review and the Value(s) of Security Research." Paper presented at the Workshop Ethical Issues in Security Research – a Practical Approach, Brussels, 29 September, 2011.

[5] Ibid.; ECORYS. "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report." 2009; Didier Bigo and Julien Jeandesboz. "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5." 2010.

the quest for appropriate remedies has become an integral part of the realm of fundamental and applied research that is set to produce new tools and technologies, and thus to contribute to effectively establishing security in the European Union – or so the argument goes. Arguably, the need for reinforced security solutions has been catalyzed by the debate that was kindled by the events of 9/11 and their massive aftermath in terms of security policy adjustments.[6] In the EU, security is now conceived of as a cross-cutting concept that has to tackle widespread areas such as terrorism, serious and organised crime, cybercrime, cross-border crime, violence itself, and natural and man-made disasters.[7] Thus, security research has eventually been established as a key area within the European funding framework.

This very framework, however, is currently undergoing structural change. In 2014, EU research funding has hit an institutional threshold as the established Framework Programmes (FP) come to an end with FP7 and will be replaced by an overhauled, streamlined, and arguably simplified and more efficient program entitled Horizon 2020.[8] Official documents promise that this new framework will, amongst other, set clearer scopes on societal issues, most notably privacy and data protection.[9] Thus, this structural change appears an appropriate break to analyze how the still emerging field of security research is being (re-)shaped alongside economic rationalities and the emergence of a European 'security project' itself, and how the relationship between privacy and security keeps evolving. In order to set out an analytical framework, this paper argues that EU security research funding follows two general trajectories: it is mainly conceived of as (1) a means to foster the European economy, and (2) as a primarily technical framework that aims to produce specific solutions to clearly defined security problems. In recent years, however, a third notion has been added to this dichotomy, as 'security' itself is now increasingly presented as a normatively embedded concept that needs to comply with human rights and civil liberties. This appears to be a major reason for abandoning the trade-off model and the search for new and integrative approaches, eventually ending up with privacy by design.

'Historically' speaking, EU security research can be framed as a field that has been shaped through an inextricable entanglement with the industrial sector, as

[6] It should be noted, however, that the notion of a post-9/11 'break' in terms of security policy has been contested such that recent developments should rather be seen as part of a larger historical trajectory. See David Lyon, "Airports as Data Filters: Converging Surveillance Systems after September 11th," *Journal of Information, Communication and Ethics in Society* 1 (2003).

[7] European Union. "Internal Security Strategy for the European Union: Towards a European Security Model." 2010, 14–16.

[8] For an overview of Horizon 2020, see http://ec.europa.eu/programmes/horizon2020/ (last accessed 26 February 2014).

[9] European Commission. "Commission Staff Working Paper. Impact Assessment. Accompanying the Communication from the Commission 'Horizon 2020 – The Framework Programme for Research and Innovation'." SEC(2011) 1427 final, 30 November, 2011.

has been compellingly shown by Bigo, Jeandesboz, Hayes, and others.[10] Multiple companies and personalities from the branch have been involved in setting up of the field and the intensified cooperation between the Commission and the industry, taking off in 2003 with the establishment of the *Group of Personalities in the Field of Security Research* (GoP)[11] and the initiation of the *Preparatory Action on Security Research* (PASR) in 2004. The GoP was eventually followed up by the *European Security: High Level Study on Threats, Responses and Relevant Technologies* (ESSTRT) in 2006[12] and the setting up of the *European Security Research Advisory Board* (ESRAB)[13] in 2005 and the *European Security Research Innovation Forum* (ESRIF)[14] in 2008, both of which further envisioned the future of security research at the EU level.

Throughout the published reports of the aforementioned fora, particularly privacy and data protection have been framed as disruptive elements for security technologies and thus for the overall goal of a secure European Union. For instance, as Bigo and Jeandesboz have pointed out, the ESSTRT final report frames the conflict such that "the underlying assumption is that intrusiveness is a requirement for efficiency, and that privacy undermines efficiency",[15] and the ESRAB report states that "research into ethics and privacy, and the trade-off between improved security and loss of privacy, will influence technology development and in parallel address aspects of how citizens perceptive security and insecurity."[16] Thus, privacy and security were generally conceived of as incommensurable concepts, and it was very clear where the preferences for effective security research had to be placed – the need for security apparently trumped the need for privacy. Either security measures would work, and this would be because they would be based on a sufficiently large database that allowed for glimpses of the future and the next event that needs to be

[10] Bigo and Jeandesboz, "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5."; Ben Hayes, *NeoConOpticon. The EU Security-Industrial Complex* (Amsterdam: Transnational Institute/Statewatch, 2009); Ben Hayes, *Arming Big Brother: The EU's Security Research Programme* (Amsterdam: Transnational Institute/Statewatch, 2006).

[11] Group of Personalities in the Field of Security Research. "Research for a Secure Europe. Report of the Group of Personalities in the Field of Security Research." 2004.

[12] European Security: High Level Study on Threats Responses and Relevant Technologies. "Deliverable D6-1 (Final Report): New European Approaches to Counter Terrorism, 21 March." 2006.

[13] European Security Research Advisory Board. "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board." 2006.

[14] European Security Research & Innovation Forum. "ESRIF Final Report, available at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (last accessed 26 February 2014)." 2009.

[15] Bigo and Jeandesboz, "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5," 6.

[16] European Security Research Advisory Board, "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board," 8.

canceled out – or they wouldn't work because privacy claims and the restrictions of the data protection framework would thwart their effectiveness. More or less independent of any actual conceptualizations of privacy, be it as the classical "right to be left alone"[17] that entails a "boundary control process",[18] as the "claim of an individual to determine what information about himself of herself should be known to others"[19] which in terms involves "a constraint on the use of power",[20] or politically as the foundation of the democratic constitutional state[21] – any position that values the (digital) personal sphere would be considered disruptive from an industry point of view. Especially when taking into consideration Helen Nissenbaum's concept of privacy in context,[22] one might indeed be inclined to say that threat scenarios were used to create a contextual override for privacy arguments.

As mentioned earlier, such a trade-off model is certainly oversimplified, and arguably only represents a part of the full story. How come we find such a striking neglect of privacy arguments in official documents, then? The next section aims at unpacking the underlying notions of security and security research in the European Union. It will become clear that EU security research unfolds along a clear-cut economic agenda, and thus introduces a very specific and market-driven approach to the relationship between privacy and security.

11.2 Economics and Technologies

First trajectory. Both FP7 and Horizon 2020 documents acknowledge the economic goals identified by the Europe 2020 strategy,[23] framing "research and innovation as central to achieving the objectives of smart, sustainable and inclusive growth."[24] The underlying rationale, as stated by the Staff Working Paper on Horizon 2020, is

[17] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890).

[18] Irwin Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?," *Journal of Social Issues* 33 (1977): 67.

[19] Alan F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59 (2003): 431.

[20] Priscilla M. Regan, "Response to Bennett: Also in Defence of Privacy," *Surveillance & Society* 8 (2011): 498.

[21] Michael Friedewald et al., "Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework," *Innovation: The European Journal of Social Science Research* 23 (2010): 62.

[22] Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*.

[23] European Commission. "Communication from the Commission. Europe 2020: A strategy for Smart, Sustainable and Inclusive Growth." COM(2010) 2020 final, 3 March, 2010.

[24] European Commission. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules for the Participation and Dissemination in 'Horizon 2020 – the Framework Programme for Research and Innovation (2014–2020)'." COM(2011) 810 final, 30 November, 2011, 2.

that “modern economic theory unanimously recognises that research and innovation are prerequisites for the creation of more and better jobs, for productivity growth and competitiveness, and for structural economic growth.”[25] For that purpose, a study on behalf of DG Industry & Enterprise has analyzed the global security market and the position of the European security industry, coming to the conclusion that “it appears vital to stimulate and create a proper innovation framework in the security domain and establish fast track development procedures for new market technology requirements.”[26] As a consequence from those findings, the European Commission in 2012 adopted an “Action Plan for an innovative and competitive Security Industry”[27] in order to secure and extend market shares in a rapidly growing global security economy.

In the same year, the Commission published a document on EU security research entitled “Safeguarding Society, Boosting Growth.”[28] Overlooking its content, it quickly becomes clear that the emphasis lies on the latter part, as the document states that

> our objective, notably through our Security Industrial Policy initiative, is to improve the global competitiveness of the EU security industry by stimulating its growth, invest in the research and development of future, world-leading security technologies and processes, and launch any effort necessary to overcome the current market fragmentation for security products in the EU and thus establish a true Internal Market.[29]

In fact, the conceptualization of EU research funding as a policy tool for economic growth has always been out in the open. Particularly, the purpose of security research can be identified by its institutional location. The housing within DG Enterprise and Industry instead of the maybe more natural fit DG Research & Innovation indeed provides a clear statement and has been criticized for its “significant consequences for the way we understand and do research on security as an ethically charged field of research.”[30] This general economic scope will likely be reinforced with the start of Horizon 2020. As the joint communication on the new framework states, “since the launch of the Seventh Framework Programme (FP7), the economic context has changed dramatically”,[31] and now urges the EU to

[25] European Commission, “Commission Staff Working Paper. Impact Assessment. Accompanying the Communication from the Commission ‘Horizon 2020 – The Framework Programme for Research and Innovation’,” 7.

[26] ECORYS, “Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report,” xvii.

[27] European Commission. “Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry.” COM(2012) 417 final, 26 July, 2012.

[28] European Commission. “EU Security Research: Safeguarding Society, Boosting Growth.” 2012.

[29] Ibid., 1.

[30] Burgess, “Ethical Review and the Value(s) of Security Research,” 1.

[31] European Commission. “Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions.

provide even stronger incentives, since “research and innovation help deliver jobs, prosperity, quality of life and global public goods.”[32]

The ECORYS report on the competitiveness of the European security industry bolsters those general assumptions with factual numbers. The global security market is estimated to be worth €100 billion, with the size of the European market in the range of €26 to €36.5 billion.[33] This translates into roughly 180,000 employees in the European security sector. Accordingly, security research receives a considerable amount of funding, with the security theme under the FP7 being worth an overall amount of €1.4 billion[34] and the financial terms for the “Secure Societies” action under Horizon 2020 alone determined at €1.7 billion. However, despite those efforts, the ECORYS report points out a “low aggregate level of EU funding for security-related research, technology development and innovation.”[35] In a comparative perspective, EU security research funding still remains “considerably below the efforts made in the USA”, leading to “potential weaknesses in the underlying competitiveness of the EU security sector.”[36] This could in terms lead to a predicted loss of market shares to a low of 20 % in 2020,[37] particularly with the Asian security industry massively catching up in the high-tech area, but also with considerable competition from Russia and Israel.[38] The remedy for such a threatening scenario appears quite simple: reinforcement of market stimulation through enhanced security research funding and faster product cycles.[39] Thus, one might indeed be inclined to agree with Bill Clinton’s famous statement that “it’s the economy, stupid”. Economic prosperity has been the driving force behind European integration from the beginning, and why should it change within security research, of all things?

The Action Plan for the security industry subsequently provides concrete steps of action in order to reinforce the competitiveness of the European security industry, suggesting the creation of a true Internal Market through favorable conditions, the enhancement of competition and lower production costs, as well as strengthened

Horizon 2020 – The Framework Programme for Research and Innovation.” COM(2011) 808 final, 30 November, 2011, 2.

[32] Ibid.

[33] ECORYS, “Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report,” v.

[34] European Commission, “EU Security Research: Safeguarding Society, Boosting Growth,” 2.

[35] ECORYS, “Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report,” x.

[36] Ibid., 38.

[37] European Commission, “Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry,” 2.

[38] ECORYS, “Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report,” 51–60.

[39] Ibid., xvii.

support for SMEs.[40] Apart from those issues, however, one of the most pressing concerns still appears to be the potential of privacy and data protection to thwart the effectiveness of security technologies and thus their successful market impact in the first place. Subsequently, the Action Plan takes up on that conflict and states that a major problem arising from the societal dimension of security research is the social acceptance of security technologies – or rather the lack thereof, which could result in a number of negative consequences for the security industry, i.e. wasted investments.[41] Most strikingly, privacy requirements are regarded to hurt the security market on both supply and demand side. For the supply side (i.e. the European security industry), this would mean that its products might not reach their maximum 'security potential' due to constraints in data collection and analysis, and "for the demand side it means being forced to purchase a less controversial product which however does not entirely fulfill the security requirements."[42] Thus, from an industry angle, the situation appears quite clear: privacy hampers security. Or rather, it hampers security technologies, as EU security research is indeed primarily locked in on the emergence of new technologies.

Second trajectory. The rationale behind this scope becomes clearer when looking at how current security efforts within the EU are conceptualized as data-driven and risk-mitigating measures. As security policies increasingly emphasize the potential of databases, data-sharing and interoperability for the purpose of gathering knowledge and thus being able to prevent future risks,[43] Information and Communication Technologies (ICTs) have spilled over into security contexts – and with them issues of privacy (and data protection). Security technologies heavily focus on communication, social networks, and other forms of individual interaction with a digitized everyday environment, such as sensors or biometrics. The massive amount of personal and behavioral data constantly produced then serves as the basis for fighting crime and terrorism through various forms of data exploitation such as algorithmic profiling and probabilistic risk calculations.[44] Or, put more simply:

[40] European Commission, "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry," 3.

[41] Ibid., 5.

[42] Ibid.

[43] see for instance Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41 (2009); Florian Geyer, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice," *Challenge Research Paper No. 9* (2008); Leese, "Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs."; Gary T. Marx and Glenn W. Muschert, "Personal Information, Borders, and the New Surveillance Studies," *Annual Review of Law and Social Science* 3 (2007); Paul de Hert and Rocco Bellanova, *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals* (Washington, DC: Migration Policy Institute, 2011).

[44] see for instance Martijn van Otterlo, "A Machine Learning View on Profiling," in *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology*, ed. Mireille Hildebrandt and Katja de Vries (Milton Park/New York: Routledge,

security itself has indeed become dominated by the desire to accumulate data in order to predict the future and counter-act criminal and terrorist incidents. But when security is supposed to be enacted through mitigation of future risks, those risks first have to be identified.

ICTs have emerged as the very tools to do so, and such a notion has obviously evoked critical reactions. Thus, ICT research ethics have specifically been concerned with the implications of the use of personal information in distinct contexts.[45] Arguably, the increasing spill-over of ICTs into the realm of security is also the reason why privacy and data protection are framed as predominant ethical concerns of current security research within official EU documents. Whether or not this limitation of ethical concerns to one clear-cut area is by any means adequate remains questionable. It should clearly be noted that multiple other pending ethical issues such as autonomy, social inclusion, human dignity, or dual use and function creep/mission creep between the civil and the military realm of security also do require attention.

However, when looking at the political and financial efforts put into security research over the last decade, one might indeed be under the impression that "our political masters, aided and abetted by the security industry, often appear willing to sacrifice some of the citizenry's privacy in order to better secure society",[46] as van Lieshout et al. have provocatively formulated it. Thus, how come the stark contrast of a presumed trade-off was eventually transformed and is now conceived of as a resolvable privacy by design issue instead of the irreconcilable conflict that it was before?

11.3 A Normative Turn?

The answer arguably lies in the re-framing of the overall European 'security project'. With the Treaty of Lisbon in 2009 and the ensuing legally binding status of the European Charter of Fundamental Rights,[47] the EU has – at least on paper – made a clear commitment to human rights and civil liberties. For the (broader) field of security, this commitment is reflected in the European Internal Security Strategy[48]

2013); Colleen McCue, *Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis* (Burlington/Oxford: Elsevier, 2007); Evelien de Pauw et al., eds., *Technology-led Policing* (Antwerpen/Apeldoorn/Portland: Maklu, 2011).

[45] David Wright, "A Framework for the Ethical Impact Assessment of Information Technology," *Ethics and Information Technology* 13 (2011).

[46] van Lieshout et al., "Reconciling Privacy and Security," 120.

[47] European Union. "Charter of Fundamental Rights of the European Union." 2000/C 364/01, 18 December, 2000.

[48] European Union, "Internal Security Strategy for the European Union: Towards a European Security Model."

of 2010 and the Stockholm program that provides the current concrete policy framework (2010–14).[49] The Internal Security Strategy, for instance, explicitly states that "Europe must consolidate a security model, based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity."[50] And the Stockholm Programme puts forward a Europe built on human rights, and goes as far as to claim that when it comes to security measures,

> basic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured and a comprehensive protection scheme must be established.[51]

This strengthened emphasis on normative aspects of security can also be found in the FP7 security scheme, claiming that "the potential impact of the resulting technologies and activities on Fundamental Rights, ethical principles and societal values should be addressed as part of the proposed research."[52] Again, especially privacy and data protection have thus been officially tagged as norms that potentially become infringed by security technologies.[53] Apart from such official statements, the predominantly technological security tools that have emerged from the FP frameworks in recent years have become the target of normative interventions due to their potential negative impact on society.[54]

Third trajectory. Alongside this new scope on the normative dimension of security, research funding, or rather the governance thereof, is also undergoing change. Security research now has to be 'ethically compliant' in order to take into account possible negative impacts on the societal level. Security research projects are thus to be accompanied by the explicit coverage of ethics boards in order to ensure that research is in line with normative principles. Subsequently, research ethics have come to enact a key role in the governance of security research, and are set to establish safeguards against detrimental societal impacts of security technologies at an early stage during research and development. In EU research

[49] European Council. "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens." Official Journal of the European Union, 2010/C 115/01, 4 May, 2010.

[50] European Union, "Internal Security Strategy for the European Union: Towards a European Security Model," 8.

[51] European Council, "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens," 10.

[52] European Commission. "FP7-SEC-2013-1 Call Fiche, 10 July." 2012, 10.

[53] European Commission. "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level." 2012.

[54] Geyer, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice."; Elspeth Guild and Sergio Carrera, "The European Union's Area of Freedom, Security and Justice Ten Years On," in *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme*, ed. Elspeth Guild, Sergio Carrera, and Alejandro Eggenschwiler (Brussels: Centre for European Policy Studies, 2010).

funding, a dedicated ethical coverage of the research process has been introduced as "fundamental ethical principles"[55] since FP5 (1998–2002). Particularly, fields such as medical and biological research have a long history of a need for ethical coverage, as has become apparent by the emerging possibilities of 'engineering' human life at the genetic or molecular level. Security research is joining those fields as one of the areas that has be monitored and advised closely. As Burgess notes, "security comes with its own special ethical baggage",[56] since it carries the potential to inflict curtailments on fundamental societal and individual values. In fact, numerous scholars have in recent years engaged with the threatening and negative consequences of new and emerging security technologies.[57]

However, on the other hand, security itself represents an important value as it "embodies the social and cultural needs of a society, its hopes and fears, its past and its ambitions for the future."[58] Read through that lens, security represents its own ethics as an overarching prerequisite for any society. Much has been written on the problems that can arise from over-emphasized security and ensuing detrimental impacts on human rights and civil liberties.[59] Adding to that list of potential negative consequences, security research

> can include particular measures that have as a secondary effect an increase in insecurity – such as the development of scanning devices that cause unease, weapons systems that provoke fear or insecurity among innocent bystanders, or surveillance systems that are experienced as too invasive.[60]

Thus, security research appears a Janus-faced phenomenon that possesses the potential of both detrimental and beneficial outcomes that indeed come as "inseparably intertwined."[61] The delicate balance of the 'goods' and 'bads' of security for society subsequently underlies constant challenges through security research and the technological tools that emerge from it. A close look reveals, as mentioned earlier, that nearly all security-related research projects within FP7 do feature a technological scope, as "the Security theme supports R&D actions oriented towards

[55] Lisa Stengel and Michael Nagenborg. "Reconstructing European Ethics. How does a Technology Become an Ethical Issue at the Level of the EU? ETICA Deliverable 3.2.2 Annex I." undated, 2.

[56] Burgess, "Ethical Review and the Value(s) of Security Research," 2.

[57] see for instance Mark B. Salter, ed. *Politics at the Airport* (Minneapolis/London: University of Minnesota Press, 2008); Didier Bigo and Anastassia Tsoukala, eds., *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes After 9/11* (London/New York: Routledge, 2008); Torin Monahan, ed. *Surveillance and Society. Technological Politics and Power in Everyday Life* (New York/London: Routledge, 2006); David Lyon, ed. *Theorizing Surveillance. The Panopticon and Beyond* (Cullompton/Portland: Willan, 2006); Louise Amoore and Marieke de Goede, eds., *Risk and the War on Terror* (London/New York: Routledge, 2008).

[58] Burgess, "Ethical Review and the Value(s) of Security Research," 2.

[59] for a comprehensive account, see Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal of Political Philosophy* 11 (2003).

[60] J. Peter Burgess. "The Societal Impact of Security Research, PRIO Policy Brief 09/2012." 2012.

[61] Ibid.

new methodologies and technologies."[62] Due to the sketched potential detrimental impact of security technologies on societies, coupled with the financial volume of security research funding, the stakes for particular security research ethics appear exceptionally high.[63] This constellation is indeed reflected in official documents – and once again it is predominantly framed in terms of privacy. The last call fiche for the security theme of FP7, for instance, states that "if ethical issues, including privacy are raised, they should be addressed in the core of the proposed activity",[64] and the EC document on ethical and regulatory issues in research policy dedicates a whole chapter to "New Security Technologies and Privacy."[65]

This emphasis on privacy arguably comes from the aforementioned data-driven nature of contemporary security technologies that build on the collection and analysis of large amounts of data, as well as from the well-defined legal applicability of the data protection framework that gives privacy concerns a 'procedural advantage' over other normative concerns when it comes to security technologies. The interesting fact is now, that with this 'new' scope on morally right security, the original conflict between security and privacy becomes rather reinforced than mitigated. In other words: with the increased emphasis on the importance of privacy, the privacy side of the original equation has been upgraded and is now not so likely to be overridden by security anymore. And since there no longer seems to be an *a priori* choice which part of the equation should be more cherished, the decisive question then becomes: how to possibly resolve this dilemma and reconcile privacy and security such that their relationship complies with the upgraded normative take on security within the EU? The answer appears indeed an intriguing one: if it is not possible to overcome the conflicting positions of the trade-off (however oversimplified they appear), why not abandon the model, after all? The ensuing move beyond, as enthusiastically announced, has eventually resulted in privacy by design.

11.4 Privacy by Design: A Technological Fix for a Technological Fix?

In the effort to effectively govern emerging technologies from security research, the Commission has identified three main dimensions of regulatory privacy protection: (1) technical, (2) legal, and (3) self-regulatory.[66] Characteristically for the legal dimension is its rather spatial scope, as it is based on the European Convention

[62] http://cordis.europa.eu/fp7/security/about-security_en.html (last accessed 9 January 2014).

[63] Burgess, "Ethical Review and the Value(s) of Security Research."

[64] European Commission, "FP7-SEC-2013-1 Call Fiche, 10 July."

[65] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," ch. 2.

[66] Ibid., 20.

on Human Rights[67] and the European Charter of Fundamental Rights,[68] rendering its power strongly connected to the jurisdiction of the EU. Within this jurisdiction, legal privacy and data protection provisions possess an enforceable status and thus provides strong incentives for any supplier of security technologies to stay within the explicitly formulated boundaries of data collection and processing. However, in times of global data flows, such a (supra-)national regulation appears hardly up to the task of effective privacy protection.

The self-regulatory dimension of security research governance, on the contrary, is based on voluntary commitments from the private sector. Self-regulation towards technology development that fulfills ethical requirements then is set to be achieved through the involvement of stakeholders and the establishment of 'soft' regulations.[69] The scope within self-regulatory governance lies on non-enforceable concepts such as "market self-regulation, corporate social responsibility (CSR), and governmental incentives for research that can drive technology towards more ethical development."[70] Albeit admitting the potential of voluntary forms of research governance, Székely et al. have pointed out that monitoring and supervision of self-regulation within the area of emerging technologies appears a highly difficult task.[71]

Thus, the official position of the European Commission with regard to security research governance can be summarized such that "weaknesses in self-regulation and legal governance suggest technological governance as a good site for concrete, operationalized engagement with tensions between the protection of privacy and the pursuit of security."[72] One might be inclined to say that this preference in fact appears a technological fix to right the technological fix that is security research in the first place. Now how to achieve such technological reconciliation? From the official documents, it becomes quite clear that Ann Cavoukian's concept of privacy by design[73] is now considered to be the silver bullet for the old clash between

[67] European Court of Human Rights/Council of Europe. "European Convention on Human Rights." 2010.

[68] European Union, "Charter of Fundamental Rights of the European Union."

[69] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," 20.

[70] Ibid.

[71] Iván Székely, Máté Dániel Szabó, and Beatrix Vissy, "Regulating the Future? Law, Ethics, and Emerging Technologies," *Journal of Information, Communication and Ethics in Society* 9 (2011): 183.

[72] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," 24.

[73] see for instance Ann Cavoukian. "Privacy by Design. Available at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (last accessed 26 February 2014)." 2009; Ann Cavoukian, Scott Taylor, and Martin E. Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," *Identity in the Information Society* 3 (2010).

security and privacy. Thus, researchers and developers are encouraged to tackle possible privacy and data protection issues pro-actively from the very beginning in order to avoid costly adjustments later on.

In fact, the ESRIF final report in 2009 made an early effort to bridge the gap between privacy and security and stated that "ESRIF advocates implementation of a 'privacy by design' data protection approach that should be part of an information system's architecture from the start."[74] How does this work? Privacy by design starts with the assumption that "privacy is good for business",[75] and develops the idea that privacy can be conceived of as a positive sum game. This is a crucial notion, as it stands opposed to the postulated zero sum game that is central to the hitherto dominant trade-off model. Furthermore, privacy safeguards then should be implemented proactively and early within the development and design of information processing technologies, and be built in a way that they last throughout the entire product life cycle.

Central in such a conceptualization of the relationship between technology and privacy/data protection is the assumption that privacy principles should be incorporated early in research and development in order to avoid costly retrofits at later stages.[76] It is exactly this presupposition that is now mirrored in EU security research. As stated by the Commission, privacy by design "should be recognized as a guiding and technologically neutral principle, suitable for flexible applications, in a general provision mandating that existing privacy and data protection principles be integrated into ICTs."[77] Just as well, the Action Plan for the security industry suggests to make use of a privacy by design approach.[78] This falls also well in line with recent discussions about privacy-preserving data mining and privacy-enhancing technologies.[79]

But does it really resolve the original conflict, namely the presumable choice between improved security or the protection of privacy? There are a number of issues to be found in the relationship of 'security and/vs privacy' that might not

[74] European Security Research & Innovation Forum, "ESRIF Final Report, available at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (last accessed 26 February 2014)," 31.

[75] Cavoukian, Taylor, and Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," 405.

[76] Cavoukian, "Privacy by Design. Available at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (last accessed 26 February 2014)."

[77] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," 26.

[78] European Commission, "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry," 11.

[79] Bart Custer et al., eds., *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Heidelberg/New York/Dordrecht/London: Springer, 2013); Charu C. Aggarwal and Philip S. Yu, eds., *Privacy-Preserving Data Mining: Models and Algorithms* (New York: Springer Science + Business Media, 2008).

be elegantly resolved through privacy by design. A key element in privacy by design are the Fair Information Principles (FIPs), that are set "to limit collection, use and disclosure of personal data, to involve individuals in the data lifecycle, and to apply appropriate safeguards in a continuous manner."[80] Thus, as Schaar argues, this means "the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible."[81] Such practices are undeniably suitable for organizational and economic contexts. However, as has been argued throughout this paper, data-driven security technologies derive their added value exactly from the information surplus that is accumulated through collection and processing of data that could eventually be connected to possible criminals or terrorists in order to cancel out future risks. And we should remember that by the logic of security experts and policy makers, the more information one can get, the better the prediction of the future and thus the better our overall security will be. In other words: security cannot thrive on informational parsimony. FIPs on the contrary radically take away the possibilities that come with advanced analytics in security contexts. This stark contrast stunningly reminds of the early days of security research, when the "trade-off between improved security and loss of privacy"[82] was openly framed as a major obstacle for the field. But how to achieve both effective security and non-intrusive privacy, then?

Certainly, there has been considerable progress in the techniques for data analytics. For instance, algorithms that allow for privacy-preserving ways of data mining[83] have been on the rise in recent years. But even with such privacy-friendly methods of data collection/analytics, the tension between privacy and security cannot be fully resolved. The "dimensionality curse"[84] states that in order to fully preserve privacy, the amount of personal attributes would need to be reduced to such an extent that the utility of processing the data is lost. Hence, the contradicting interests between privacy on the one hand and the benefit of being able to process data on the other hand cannot simply be resolved using technical means. Thus, a certain conflict remains between efficiency in terms of the generation of security knowledge and the preservation of privacy. In simple terms, the more (individual) attributes are reduced from the dataset, the less utility will emerge from analytics. Is

[80] Cavoukian, Taylor, and Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," 406.

[81] Peter Schaar, "Privacy by Design," *Identity in the Information Society* 3 (2010): 267–8.

[82] European Security Research Advisory Board, "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board," 8.

[83] Aggarwal and Yu, *Privacy-Preserving Data Mining: Models and Algorithms*.

[84] Charu C. Aggarwal. "On Randomization, Public Information and the Curse of Dimensionality." Paper presented at IEEE 23rd International Conference on Data Engineering, Istanbul, 11–15 April, http://charuaggarwal.net/curse.pdf, 2007; Charu C. Aggarwal and Philip S. Yu. "On Variable Constraints in Privacy Preserving Data Mining." Paper presented at SIAM International Conference on Data Mining, Newport Beach, 21–23 April, http://charuaggarwal.net/aggar140.pdf, 2005.

the turn to privacy by design merely old wine in new bottles, then? Even if it does not convincingly resolve the tension between privacy and security, the transformative framing of the old ‘conflict’ tells us a lot about the current state of affairs with regard to privacy and security.

11.5 Conclusions

This paper has shown that the relationship between the concepts of privacy and security has come a long way from an early conceptualization as a sharp trade-off towards a contemporary framing as a technological issue that appears resolvable through privacy by design. However, this paper has put forward the claim that the current re-framing is not particularly well suited to actually mitigate or resolve the tension between privacy and security, but rather pays tribute to the technological scope on security, while at the same time acknowledging the increasingly normative take on security with the EU.

The trade-off model has always been troubled by the oversimplified claim that it was possible to put forward two unspecified concepts and outweigh them against each other. And while privacy has long been conceived of as “a moving target”,[85] the conceptualization of security is shifting as well. To stay within the metaphor, the second target is also starting to move quite rapidly, as the notion of security is undergoing deep-seated normative transformations. When thinking about the current relationship of privacy and security, it appears only appropriate to take into consideration the changing state of security between abstract concepts, concrete technological applications, economic desires and normative prerequisites and implications.

Is security merely a driver for economic growth and prosperity, or does it indeed come as an intrinsic value that has to be handled with care in order to avoid detrimental effects on societal values? Is privacy a value that is still trumped by the seemingly overarching desire for security, or does it have the capacity to challenge the paradigm of security through the EU’s confession to more human rights and civil liberties based security measures and the further incorporation of ethics into EU funded research? The ensuing constellation appears a puzzling one: depending on the perspective, security (technology) is regarded as either a serious threat for privacy or an opportunity for massive economic revenue – but should security by default not be a value itself? A basic need for any society to ensure its present and future prosperity and a safeguard for its individuals to flourish and realize their potential? It remains up for discussion whether privacy by design can provide a true reconciliation of privacy and security, or whether it solely serves as a veil that is set to obscure major concerns with regard to data-driven security technologies. It appears that such a technological approach to the governance of

[85] Friedewald et al., “Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework,” 61.

security research (and subsequently to 'security' itself) falls well in line with the general technological scope of EU security research. However, it remains open whether this 'technological fix for a technological fix' will strengthen the position of privacy and data protection, or whether security will further trump normative considerations and civil liberties/rights. To end on a critical note: privacy-by-design might not be the silver bullet that it is regarded to be right now, but might rather be a concept that at first sight appears to be easily applicable within the general technological paradigm of security, but only seemingly soothes the conflict between privacy and security.

References

Aggarwal, Charu C. "On Randomization, Public Information and the Curse of Dimensionality." Paper presented at IEEE 23rd International Conference on Data Engineering, Istanbul, 11–15 April, http://charuaggarwal.net/curse.pdf, 2007.

Aggarwal, Charu C., and Philip S. Yu. "On Variable Constraints in Privacy Preserving Data Mining." Paper presented at SIAM International Conference on Data Mining, Newport Beach, 21–23 April, http://charuaggarwal.net/aggar140.pdf, 2005.

Aggarwal, Charu C., and Philip S. Yu, eds. *Privacy-Preserving Data Mining: Models and Algorithms*. New York: Springer Science + Business Media, 2008.

Altman, Irwin. "Privacy Regulation: Culturally Universal or Culturally Specific?". *Journal of Social Issues* 33 (1977): 66–84.

Amoore, Louise. "Algorithmic War: Everyday Geographies of the War on Terror." *Antipode* 41 (2009): 49–69.

Amoore, Louise, and Marieke de Goede, eds. *Risk and the War on Terror*. London/New York: Routledge, 2008.

Bennett, Colin J. "What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11." In *Global Surveillance and Policing. Borders, Security, Identity*, edited by Elia Zureik and Mark B. Salter, 113–38. Cullompton/Portland: Willan, 2005.

Bigo, Didier, and Julien Jeandesboz. "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5." 2010.

Bigo, Didier, and Anastassia Tsoukala, eds. *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes After 9/11*. London/New York: Routledge, 2008.

Burgess, J. Peter. "Ethical Review and the Value(s) of Security Research." Paper presented at the Workshop Ethical Issues in Security Research – a Practical Approach, Brussels, 29 September, 2011.

Burgess, J. Peter. "The Societal Impact of Security Research, PRIO Policy Brief 09/2012." 2012.

Cavoukian, Ann. "Privacy by Design. Available at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (last accessed 26 February 2014)." 2009.

Cavoukian, Ann, Scott Taylor, and Martin E. Abrams. "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices." *Identity in the Information Society* 3 (2010): 405–13.

Custer, Bart, Toon Calders, Bart Schermer, and Tal Zarsky, eds. *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*. Heidelberg/New York/Dordrecht/London: Springer, 2013.

de Hert, Paul, and Rocco Bellanova. *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals*. Washington, DC: Migration Policy Institute, 2011.

de Pauw, Evelien, Paul Ponsaers, Kees van der Vijver, Willy Bruggeman, and Piet Deelman, eds. *Technology-led Policing*. Antwerpen/Apeldoorn/Portland: Maklu, 2011.

ECORYS. "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report." 2009.

European Commission. "Commission Staff Working Paper. Impact Assessment. Accompanying the Communication from the Commission 'Horizon 2020 – The Framework Programme for Research and Innovation'." SEC(2011) 1427 final, 30 November, 2011.

European Commission. "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions. Horizon 2020 – The Framework Programme for Research and Innovation." COM(2011) 808 final, 30 November, 2011.

European Commission. "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry." COM(2012) 417 final, 26 July, 2012.

European Commission. "Communication from the Commission. Europe 2020: A strategy for Smart, Sustainable and Inclusive Growth." COM(2010) 2020 final, 3 March, 2010.

European Commission. "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level." 2012.

European Commission. "EU Security Research: Safeguarding Society, Boosting Growth." 2012.

European Commission. "FP7-SEC-2013-1 Call Fiche, 10 July." 2012.

European Commission. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules for the Participation and Dissemination in 'Horizon 2020 – the Framework Programme for Research and Innovation (2014–2020)'." COM(2011) 810 final, 30 November, 2011.

European Council. "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens." Official Journal of the European Union, 2010/C 115/01, 4 May, 2010.

European Court of Human Rights/Council of Europe. "European Convention on Human Rights." 2010.

European Security Research & Innovation Forum. "ESRIF Final Report, available at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (last accessed 26 February 2014)." 2009.

European Security Research Advisory Board. "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board." 2006.

European Security: High Level Study on Threats Responses and Relevant Technologies. "Deliverable D6-1 (Final Report): New European Approaches to Counter Terrorism, 21 March." 2006.

European Union. "Charter of Fundamental Rights of the European Union." 2000/C 364/01, 18 December, 2000.

European Union. "Internal Security Strategy for the European Union: Towards a European Security Model." 2010.

Friedewald, Michael, David Wright, Serge Gutwirth, and Emilio Mordini. "Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework." *Innovation: The European Journal of Social Science Research* 23 (2010): 61–67.

Geyer, Florian. "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice." *Challenge Research Paper No. 9* (2008).

Group of Personalities in the Field of Security Research. "Research for a Secure Europe. Report of the Group of Personalities in the Field of Security Research." 2004.

Guild, Elspeth, and Sergio Carrera. "The European Union's Area of Freedom, Security and Justice Ten Years On." In *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme*, edited by Elspeth Guild, Sergio Carrera and Alejandro Eggenschwiler, 1–12. Brussels: Centre for European Policy Studies, 2010.

Hayes, Ben. *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: Transnational Institute/Statewatch, 2006.

Hayes, Ben. *NeoConOpticon. The EU Security-Industrial Complex*. Amsterdam: Transnational Institute/Statewatch, 2009.

Leese, Matthias. “Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs.” *Computer Law & Security Review* 29 (2013): 480–90.

Lyon, David. “Airports as Data Filters: Converging Surveillance Systems after September 11th.” *Journal of Information, Communication and Ethics in Society* 1 (2003): 13–20.

Lyon, David, ed. *Theorizing Surveillance. The Panopticon and Beyond*. Cullompton/Portland: Willan, 2006.

Marx, Gary T., and Glenn W. Muschert. “Personal Information, Borders, and the New Surveillance Studies.” *Annual Review of Law and Social Science* 3 (2007): 375–95.

McCue, Colleen. *Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis*. Burlington/Oxford: Elsevier, 2007.

Monahan, Torin, ed. *Surveillance and Society. Technological Politics and Power in Everyday Life*. New York/London: Routledge, 2006.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books, 2010.

Regan, Priscilla M. “Response to Bennett: Also in Defence of Privacy.” *Surveillance & Society* 8 (2011): 497–99.

Salter, Mark B., ed. *Politics at the Airport*. Minneapolis/London: University of Minnesota Press, 2008.

Schaar, Peter. “Privacy by Design.” [In English]. *Identity in the Information Society* 3 (2010): 267–74.

Stengel, Lisa, and Michael Nagenborg. “Reconstructing European Ethics. How does a Technology Become an Ethical Issue at the Level of the EU? ETICA Deliverable 3.2.2 Annex I.” undated.

Székely, Iván, Máté Dániel Szabó, and Beatrix Vissy. “Regulating the Future? Law, Ethics, and Emerging Technologies.” *Journal of Information, Communication and Ethics in Society* 9 (2011): 180–94.

Tsoukala, Anastassia. “Risk-focused Security Policies and Human Rights. The Impossible Symbiosis.” In *Mapping Transatlantic Security Relations. The EU, Canada, and the War on Terror*, edited by Mark B. Salter, 41–59. London/New York: Routledge, 2010.

Valkenburg, Govert. “The Trade-Off Model Between Privacy and Security From a Sociotechnical Perspective. Paper presented at Computers, Privacy and Data Protection Conference, Brussels, 22–24 January.” 2014.

van Lieshout, Marc, Michael Friedewald, David Wright, and Serge Gutwirth. “Reconciling Privacy and Security.” *Innovation: The European Journal of Social Science Research* 26 (2013): 119–32.

van Otterlo, Martijn. “A Machine Learning View on Profiling.” In *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology*, edited by Mireille Hildebrandt and Katja de Vries, 41–64. Milton Park/New York: Routledge, 2013.

Waldron, Jeremy. “Security and Liberty: The Image of Balance.” *Journal of Political Philosophy* 11 (2003): 191–210.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 4 (1890): 193–220.

Westin, Alan F. “Social and Political Dimensions of Privacy.” *Journal of Social Issues* 59 (2003): 431–53.

Wright, David. ”A Framework for the Ethical Impact Assessment of Information Technology.” *Ethics and Information Technology* 13 (2011): 199–226.