CANVAS BRIEFING PACKAGES

COMMENTED LITERATURE LIST

Compiled by

Eva Schlehahn

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) on the basis of input and support of the whole CANVAS project consortium

Co-funded by the Horizon 2020 programme of the European Union

The CANVAS project (Constructing an Alliance for Value-driven Cybersecurity) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540. This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

CONTENT

1 Brief introduction to the CANVAS literature lists

The commented literature lists provided by the CANVAS project is a cybersecurity-focused collection of resources e.g. from academia, EU-funded research, and policy/legislation.

First and foremost, this collection consists of the publications produced by the CANVAS project itself, namely its White Papers, plus the scientific publications of the consortium members brought forward as output of the project's research work.

Beyond this set of core resources, additional literature recommendations are provided in this document. While some of them were derived from the CANVAS White Paper's references sections, they have been enriched by additional, more recent publications which were made available after the submission of the White Papers.

2 CANVAS publications

This chapter lists all publications done of the CANVAS consortium members, either as official joint project results, or as individual research work done in the context of CANVAS.

2.1 CANVAS White Papers

CANVAS has produced four main deliverables, also called CANVAS White Papers, which are freely available via the project website (https://canvas-project.eu/results/whitepapers.html). They address the following cybersecurity-related research topics:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Options regarding cybersecurity
4. Technological challenges in cybersecurity

In the following, a brief overview over each of these four White Papers is given.

Cybersecurity and Ethics

Yaghmaei, Emad and van de Poel, Ibo and Christen, Markus and Gordijn, Bert and Kleine, Nadine and Loi, Michele and Morgan, Gwenyth and Weber, Karsten, Canvas White Paper 1 – Cybersecurity and Ethics (October 4, 2017). Available at SSRN: https://ssrn.com/abstract=3091909 or http://dx.doi.org/10.2139/ssrn.3091909

This White Paper outlines how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the “blind spots” in the current ethical discourse on cybersecurity are located. It has a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. For each domain, a systematic literature search has been performed and the identified papers have been analysed using qualitative and quantitative methods. An important observation is that the ethics of cybersecurity not an established subject. In all domains, cybersecurity is recognized as being an instrumental value, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres; for example between usability and security, accessibility and security, or privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data.

Cybersecurity and Law

Jasmontaite, Lina and González Fuster, Gloria and Gutwirth, Serge and Wenger, Florent and Jaquet-Chiffelle, David-Olivier and Schlehahn, Eva, Canvas White Paper 2 – Cybersecurity and Law (October 4, 2017). Available at SSRN: https://ssrn.com/abstract=3091939 or http://dx.doi.org/10.2139/ssrn.3091939

This White Paper explores the legal dimensions of the European Union (EU)’s value-driven cybersecurity. It identifies main critical challenges in this area and discusses specific controversies concerning cybersecurity regulation. The White Paper recognises that legislative and policy measures within the cybersecurity domain challenge EU fundamental rights and principles, stemming from EU values. Annexes provide a review on EU soft-law measures, EU legislative measures, cybersecurity and criminal justice affairs, the relation of cybersecurity to privacy and data protection, cybersecurity definitions in national cybersecurity strategies, and brief descriptions of EU values.

Attitudes and Opinions Regarding Cybersecurity

Wenger, Florent and Jaquet-Chiffelle, David-Olivier and Kleine, Nadine and Weber, Karsten and Morgan, Gwenyth and Gordijn, Bert and Inversini, Reto and Bangerter, Endre and Schlehahn, Eva, Canvas White Paper 3 – Attitudes and Opinions Regarding Cybersecurity (October 4, 2017). Available at SSRN: https://ssrn.com/abstract=3091920 or http://dx.doi.org/10.2139/ssrn.3091920

This White Paper summarises currently available empirical data about attitudes and opinions of citizens and state actors regarding cybersecurity. The data emerges from reports of EU projects, Eurobarometer surveys, policy documents of state actors and additional scientific papers. It describes what these stakeholders generally think, what they feel, and what they do about cyber threats and security (counter) measures. For citizens' perspectives, three social spheres of particular interest are examined: 1) health, 2) business, 3) police and national security.

Technological Challenges in Cybersecurity

Domingo-Ferrer, Josep and Blanco, Alberto and Parra Arnau, Javier and Herrmann, Dominik and Kirichenko, Alexey and Sullivan, Sean and Patel, Andrew and Bangerter, Endre and Inversini, Reto, Canvas White Paper 4 – Technological Challenges in Cybersecurity (December 21, 2017). Available at SSRN: https://ssrn.com/abstract=3091942 or http://dx.doi.org/10.2139/ssrn.3091942

This White Paper summarizes the current state of discussion regarding the main technological challenges in cybersecurity and impact of those, including ways and approaches to addressing them, on key fundamental values. It provides an overview on current cybersecurity threads and countermeasures and focuses on ethical dilemmas that emerge when counteracting those threads. It also points to the fact that the cybersecurity community relies much more on interpersonal relations when sharing intelligence and data than in explicit national or supranational regulations. Furthermore, the White Paper presents advanced cryptographic techniques and data anonymization techniques that may help to solve or minimize some of the ethical dilemmas.

2.2 CANVAS book 'The Ethics of Cybersecurity'

The consortium members of CANVAS produced a book to fully convey the outcomes of the project research and gained knowledge. The book will appear in November 2019; all book chapters will be available open access on the CANVAS website.

The Ethics of Cybersecurity

The International Library of Ethics, Law and Technology Vol. 21 Markus Christen, Bert Gordijn and Michele Loi (Eds.)
ISBN 978-3-030-29052-8; DOI: 10.1007/978-3-030-29053-5 https://www.springer.com/gp/book/9783030290528

About this book:

The increasing use of information and communication technology (ICT) in all spheres of modern life makes the world a richer, more efficient and interactive place. However, it also increases its fragility as it reinforces our dependence on ICT systems that can never be completely safe or secure. Therefore, cybersecurity has become a matter of global interest and importance. Accordingly, one can observe in today's cybersecurity discourse an almost constant emphasis on an ever-increasing and diverse set of threat forms, ranging from basic computer viruses to sophisticated kinds of cybercrime and cyberespionage activities, as well as cyber-terror and cyberwar. This growing complexity of the digital ecosystem in combination with increasing global risks has created the following dilemma. Overemphasizing cybersecurity may violate fundamental values like equality, fairness, freedom, or privacy. On the other hand, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure, policy makers and state authorities and thus supports the protection of those values. Cybersecurity thus imposes a complex relationship among values, some may be supportive, others conflicting, depending on context.

Understanding this dilemma has become imperative. Yet it is still an under-developed topic in technology ethics. Whilst there are lots of papers discussing issues such as "big data" and privacy, cybersecurity is – if at all – only instrumentally discussed as a tool to protect (or undermine) privacy. Nevertheless, cybersecurity raises a plethora of ethical issues such as "ethical hacking", dilemmas of holding back "zero day" exploits, weighting data access and data privacy in sensitive health data, or value conflicts in law enforcement raised by encryption algorithms. Those issues are usually discussed in an isolated manner, whereas a coherent and integrative view on the ethics of cybersecurity is missing. This book aims to extensively discuss the full plethora of ethical aspects of cybersecurity and it will thus complement two recently published monographs on the ethics of cybersecurity.

This book will not only be relevant for the philosophy and ethics of technology community. Many practitioners in cybersecurity – providers of security software, CERTs or Chief Security Officers in companies are increasingly aware of the ethical dimensions of their work. This book will therefore have a strong practical focus, including case studies that outline ethical dilemmas in cybersecurity and presenting guidelines and other measures to tackle those dilemmas.

Foreseeable content structure of the CANVAS book, with individual chapters:

Chapter 1: Introduction
Markus Christen, Bert Gordijn and Michele Loi

Part 1 - Foundations

Chapter 2: Basic Concepts and Models of Cybersecurity
Dominik Herrmann and Henning Pridöhl

Chapter 3: Core Values and Value Conflicts in Cybersecurity: beyond Privacy versus Security
Ibo van de Poel

Chapter 4 : Ethical Frameworks for Cybersecurity
Michele Loi and Markus Christen

Chapter 5: Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights
Gloria González Fuster and Lina Jasmontaite

Part 2 – Problems

Chapter 6: A Care-Based Stakeholder Approach to Ethics of Cybersecurity in Business
Gwenyth Morgan and Bert Gordijn

Chapter 7: Cybersecurity in Health Care
Karsten Weber and Nadine Kleine

Chapter 8: Cybersecurity of Critical Infrastructure
Eleonora Viganò, Michele Loi and Emad Yaghmaei

Chapter 9: Ethical and Unethical Hacking
David-Olivier Jaquet-Chiffelle and Michele Loi

Chapter 10: Cybersecurity and the State
Eva Schlehahn

Chapter 11: Freedom of Political Communication, Propaganda and the Role of Epistemic Institutions in Cyberspace
Seumas Miller

Chapter 12: Cybersecurity and Cyber Warfare: the Ethical Paradox of 'Universal Diffidence'
George Lucas

Chapter 13: Cyber Peace—and How it can be Achieved
Reto Inversini

Part 3 – Recommendations

Chapter 14: Privacy-preserving Technologies
Josep Domingo-Ferrer and Alberto Blanco-Justicia

Chapter 15: Best Practices and Recommendations for Cybersecurity Service Providers
Alexey Kirichenko, Markus Christen, Florian Grunow and Dominik Herrmann

Chapter 16: A Framework for Ethical Cyber-defence for Companies
Salome Stevens

Chapter 17: Towards Guidelines for Medical Professionals to ensure Cybersecurity in Digital Health Care'
David Koeppe

Chapter 18: Norms of Responsible State Behaviour in Cyberspace
Paul Meyer

2.3 Other CANVAS publications

In this section, a selection of other publications produced by CANVAS consortium members are provided, sorted by publication year and then with titles in alphabetical order. All papers listed here are available open access.

2019

Cybersecurity in Health – Disentangling Value Tensions

2019. Michele Loi, Markus Christen, Nadine Kleine, and Karsten Weber.
Journal of Information, Communication and Ethics in Society, May.
https://doi.org/10.1108/JICES-12-2018-0095 or https://doi.org/10.1108/JICES-12-2018-0095>.

This paper analyses the trade-offs facing the design of cybersecurity in healthcare, including medical devices and electronic health records and health-related administration systems. The trade-offs in the different design goals of cybersecurity (access and integrity, confidentiality, while preserving the usability of systems) are mapped into the four principles of biomedical ethics (beneficence, non-maleficence, autonomy and justice).

Digital cash and privacy: What are the alternatives to Libra?

2019. Christian Grothoff and Alex Pentland.
Article publication on Massachusetts Institute of Technology Media Lab Website, July 18, 2019.
https://www.media.mit.edu/posts/digital-cash-and-privacy-what-are-the-alternatives-to-libra/

Privacy-preserving Cloud Computing on Sensitive Data: a Survey of Methods, Products and Challenges

2019. Josep Domingo-Ferrer, Oriol Farràs, Jordi Ribes-González and David Sánchez,
Computer Communications, vol. 140-141, pp. 38-60, 2019
https://crises-deim.urv.cat/web/docs/publications/journals/1074.pdf

Steered microaggregation as a unified primitive to anonymize data sets and data streams

2019. Josep Domingo-Ferrer, Jordi Soria-Comas and Rafael Mulero-Vellido
IEEE Transactions on Information Forensics and Security vol. 14, no. 12, pp. 3298-3311, 2019
https://crises-deim.urv.cat/web/docs/publications/journals/1080.pdf

2018

AppPETs: A Framework for Privacy-Preserving Apps

2018. Erik Sy, Tobias Mueller, Matthias Marx, and Dominik Herrmann.
SAC 2018: Symposium on Applied Computing, Pau, France, April 9–13, 2018. DOI: 10.1145/3167132.3167415
https://svs.informatik.uni-hamburg.de/publications/2018/2018-04-09-Sy-ACM-SAC-AppPETs-AFramework-for-Privacy-Preserving-Apps.pdf

Book review Gry Hasselbalch and Pernille Tranberg, Data Ethics — The New Competitive Advantage

2018. Lina Jasmontaite.
The International Data Privacy Law Journal.
DOI: 10.1093/idpl/ipx025
https://doi.org/10.1093/idpl/ipx025

Dynamic group size accreditation and group discounts preserving anonymity

2018. Josep Domingo-Ferrer, Alberto Blanco-Justicia, and Carla Ràfols.
International Journal of Information Security. DOI: 10.1007/s10207-017-0368-y
https://crises-deim.urv.cat/web/docs/publications/journals/1013.pdf

Participatory Sensing und Wearable Technologies als partizipative Formen der Datengenerierung im Internet of Things: Potenziale, Herausforderungen und erste Lösungsansätze

2018. Nadine Kleine, Max-R. Ulbricht, Karsten Weber, and Frank Pallas.
In Grand Challenges‘ meistern – der Beitrag der Technikfolgenabschätzung, edited by M. Decker, R. Lindner, St. Lingner, C. Scherz, M. Sotoudeh. Baden-Baden: Nomos.
DOI: 10.5771/9783845283562-245
https://doi.org/10.5771/9783845283562-245

Privatsphäre als inhärente Eigenschaft eines Kommunikationsnetzes

2018. Matthias Marx, Maximilian Blochberger, Dominik Herrmann, and Hannes Federrath.
In Proceedings der Konferenz Forum Privatheit am 2. November 2017 in Berlin.
DOI: 10.1007/978-3-658-23727-1_12
https://doi.org/10.1007/978-3-658-23727-1_12

Sicherheit und Privatheit auf deutschen Hochschulwebseiten: Eine Analyse mit PrivacyScore

2018. Tobias Müller, Matthias Marx, Henning Pridöhl, Pascal Wichmann, and Dominik Herrmann.
25 DFN-Konferenz Sicherheit in vernetzten Systemen. Hamburg.
https://muelli.cryptobit.ch/paper/2018-02-DFN-PrivacyScore.pdf

2017

Adieu Einwilligung? Neue Herausforderungen für die informationelle Selbstbestimmung im Angesicht von Big Data-Technologien

2017. Max-R. Ulbricht, and Karsten Weber.
In Informationelle Selbstbestimmung im digitalen Wandel, edited by M. Friedewald, J. Lamla, A. Roßnagel. Wiesbaden: Springer. DOI: 10.1007/978-3-658-17662-4_16
https://doi.org/10.1007/978-3-658-17662-4_16

A methodology to compare anonymization methods regarding their risk-utility trade-off

2017. Josep Domingo-Ferrer, Sara Ricci, and Jordi Soria-Comas.
Lecture Notes in Computer Science, Vol. 10571: Modeling Decisions for Articial Intelligence-MDAI 2017, Oct 2017, pp. 132-143. ISSN: 0302-9743. DOI: 10.1007/978-3-319-67422-3_12
https://crises-deim.urv.cat/web/docs/publications/lncs/1017.pdf

A Review of Value-Conflicts in Cybersecurity

2017. Markus Christen, Bert Gordijn, Karsten Weber, Ibo van de Poel, and Emad Yaghmaei.
Orbit 1, no. 1.
DOI: 10.29297/orbit.v1i1.28
https://www.orbit-rri.org/ojs/index.php/orbit/article/download/28/31/

A Security Union In Full Respect Of Fundamental Rights: But How Effectively Respectful?

2017. Gloria González Fuster.
In Constitutionalising the Security Union: Effectiveness, Rule of Law and Rights on Countering Terrorism and Crime. Edited by Sergio Carrera, Valsamis Mitsilegas. Center for European Policy Studies (CEPS): 87-92.
https://www.ceps.eu/ceps-publications/constitutionalising-security-union-effectiveness-rulelaw-and-rights-countering

A semantic framework for noise addition with nominal data

2017. Mercedes Rodriguez-Garcia, Montserrat Batet, and David Sánchez. Knowledge-Based Systems 122 (April): 103-118. ISSN: 0950-7051. DOI: 10.1016/j.knosys.2017.01.032
https://crises-deim.urv.cat/web/docs/publications/journals/1009.pdf

Beyond Informed Consent – Investigating Ethical Justifications for Disclosing, Donating or Sharing Personal Data in Research

2017. Markus Christen, Josep Domingo-Ferrer, Dominik Herrmann, and Jeroen van den Hoven.
In Philosophy and Computing: Essays in epistemology, philosophy of mind, logic, and ethics:
CEPE-IACAP 2015, University of Delaware, June 22–25, 2015. PSSP 128, Springer.
DOI: 10.1007/978-3-319-61043-6_10
https://doi.org/10.1007/978-3-319-61043-6_10

Building a cybersecurity culture in the EU through mandatory notification of data breaches and incidents

2017. Lina Jasmontaite.
Proceedings of the Managing Risk in the Digital Society conference:
Internet, Law & Politics. Barcelona 2017.
https://symposium.uoc.edu/6747/section/5263/managing-risk-in-the-digital-society.-internetlaw-and-politics.-barcelona-2017.html

Co-utility: self-enforcing protocols for the mutual benefit of participants

2017. Josep Domingo-Ferrer, Sergio Martínez, David Sánchez, and Jordi Soria-Comas.
Engineering Applications of Artificial Intelligence 59 (March): 148-158. ISSN: 0952-1976.
DOI: 10.1016/j.engappai.2016.12.023
https://crises-deim.urv.cat/web/docs/publications/journals/990.pdf

Differentially private data sets based on microaggregation and record perturbation

2017. Jordi Soria-Comas, and Josep Domingo-Ferrer.
Lecture Notes in Computer Science, 10571 (October issue - Modeling Decisions for Artificial Intelligence-MDAI 2017): 119-131. ISSN: 0302-9743. DOI: 10.1007/978-3-319-67422-3_11
https://crises-deim.urv.cat/web/docs/publications/lncs/1018.pdf

Individual differential privacy: a utility-preserving formulation of differential privacy guarantees

2017. Jordi Soria-Comas, Josep Domingo-Ferrer, David Sánchez, and David Megías.
IEEE Transactions on Information Forensics and Security 12, no. 6 (June): 1418-1429. ISSN: 1556-6013. DOI: 10.1109/TIFS.2017.2663337
https://crises-deim.urv.cat/web/docs/publications/journals/995.pdf

Integrating Privacy-Enhancing Technologies into the Internet Infrastructure

2017. David Harborth, Dominik Herrmann, Stefan Köpsell, Sebastian Pape, Christian Roth, Hannes Federrath, Dogan Kesdogan, and Kai Rannenberg. arXiv:1711.07220 [cs.CR].
https://epub.uni-regensburg.de/36346/1/description_english.pdf

Klinische Register im 21. Jahrhundert

2017. C.-A. Behrendt, H. Pridöhl, K. Schaar, Hannes Federrath, and E. S. Debus.
Der Chirurg 88, no. 11: 944-949. DOI: 10.1007/s00104-017-0542-9
https://link.springer.com/content/pdf/10.1007%2Fs00104-017-0542-9.pdf

Methods for practising ethics in research & innovation: A literature review, critical analysis and recommendations

2017. Wessel Reijers, David Wright, Philipp Brey, Karsten Weber, Rowena Rodrigues, Declan O'Sullivan, and Bert Gordijn. In Science and Engineering Ethics.
DOI: 10.1007/s11948-017-9961-8
https://link.springer.com/content/pdf/10.1007%2Fs11948-017-9961-8.pdf

Privacy-preserving and co-utile distributed social credit

2017. Josep Domingo-Ferrer.
In Lecture Notes in Computer Science, Vol. 0: IWOCA 2017- 28th International Workshop on Combinatorial Algorithms, Jul 2017. ISSN: 0302-9743.
DOI: 10.1007/978-3-319-78825-8_30
https://crises-deim.urv.cat/web/docs/publications/lncs/1016.pdf

Privacy-preserving data outsourcing in the cloud via semantic data splitting

2017. David Sánchez, and Montserrat Batet. Computer Communications 110 (Sept): 187-201.
ISSN: 0140-3664. DOI: 10.1016/j.comcom.2017.06.012
https://crises-deim.urv.cat/web/docs/publications/journals/1023.pdf

PrivacyScore: Analyse von Webseiten auf Sicherheits- und Privatheitsprobleme – Konzept und rechtliche Zulässigkeit

2017. Max Maass, Anne Laubach, and Dominik Herrmann. Proceedings of INFORMATIK 2017,
Workshop "Recht und Technik". DOI: 10.18420/in2017_107
https://dl.gi.de/bitstream/handle/20.500.12116/3867/B13-3.pdf

PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites

2017. Maass, Max, Pascal Wichmann, Henning Pridöhl, and Dominik Herrmann.
Proceedings of ENISA Annual Privacy Forum, 7–8 June 2017, Vienna, LNCS 10518. Heidelberg:
Springer. DOI: 10.1007/978-3-319-67280-9_10
https://doi.org/10.1007/978-3-319-67280-9_10

Technik zur Unterstützung von Citizen Science und Open Science. Technische und organisatorische Herausforderungen und mögliche Lösungsansätze

2017. Karsten Weber, Nadine Kleine, Frank Pallas, and Max-R. Ulbricht.
TATuP 26 (1/2). DOI: 10.14512/tatup.26.1-2.25
http://tatup.de/index.php/tatup/article/download/22/61

Toward sensitive document release with privacy guarantees

2017. David Sánchez, and Montserrat Batet.
Engineering Applications of Artificial Intelligence 59 (March): 23-34. ISSN: 0952-1976.
https://crises-deim.urv.cat/web/docs/publications/journals/993.pdf

2016

Behavior-Based Tracking of Internet Users with Semi-Supervised Learning

2016. Dominik Herrmann, Matthias Kirchler, Jens Lindemann, and Marius Kloft.
Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST 2016), IEEE.
DOI: 10.1109/PST.2016.7906992
https://bits.informatik.hu-berlin.de/~kloftmar/publications/2016/pst.pdf

Darstellung der Möglichkeiten, mithilfe von – ggf. auch personenbezogenen – Daten eine Lokalisierung bzw. Ortung von Personen durchzuführen [Presentation of the possibilities to localize or locate persons with the help of - if necessary also personal data.]

2016. Hannes Federrath. Sachverständigengutachten für den 1. Untersuchungsausschuss ("NSAUntersuchungsausschuss") der 18. Wahlperiode des Deutschen Bundestages. [Expert opinions for the 1st Committee of Inquiry ("NSA Committee of Inquiry") of the 18th election period of the German Bundestag. 19 September 2016]
https://svs.informatik.uni-hamburg.de/publications/2016/2016-nsa-ua-gutachten-federrath.pdf

Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic

2016. Matthias Kirchler, Dominik Herrmann, Jens Lindemann, and Marius Kloft.
Proceedings of the 9th ACM Workshop on Artificial Intelligence and Security (AISec), co-located with the 23nd ACM Conference on Computer and Communications (CCS), 2016.
DOI: 10.1145/2996758.2996770
https://svs.informatik.uni-hamburg.de/publications/2016/2016-10-28-AISec2016-Trackedwithout-a-Trace.pdf

Unbemerktes Tracking im Internet: Unsere unerwünschte Identität

2016. Dominik Herrmann, and Hannes Federrath.
In Der digitale Bürger und seine Identität, edited by Gerrit Hornung und Christoph Engemann.
Der Elektronische Rechtsverkehr, Bd. 36. Baden-Baden: Nomos.
DOI: 10.5771/9783845276762-131
https://doi.org/10.5771/9783845276762-131

3 Selected reference sources (mainly) from the CANVAS White Papers

This chapter provides additional literature recommendations. In part, they were derived from the CANVAS White Paper's references sections, plus more recent publications (mainly those from 2019) which became available after the submission date of the project White Papers.

In general, the selection criteria for all literature recommendations are the open access availability and specifically dedicated pieces highlighted by the individual White Paper authors. For a few of the literature recommendations, the individual consortium members providing them for this list, a brief description has been delivered as well. These descriptions are highlighted in bold and blue font for easy recognition by any reader.

3.1 Academic sources

Alheit, K.
'The applicability of the EU Product Liability Directive to Software'
Comparative and International Law Journal of Southern Africa, Volume 34, Issue 2, Jul 2001.
Available at: https://www.jstor.org/stable/23251124

Árnason, Vilhálmur
'Coding and Consent: Moral Challenges of the Database Project in Iceland'
Bioethics 18, no. 1 (February 2004): 27–49. doi:10.1111/j.1467-8519.2004.00377.x.
Available at:
https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8519.2004.00377.x?sid=nlm%3Apubmed&

Austin, L. M.
'Surveillance and the Rule of Law'
Debate article published in the Surveillance & Society Journal Vol 13, No 2 (2015).
Available at:
http://ojs.library.queensu.ca/index.php/surveillance-andsociety/article/viewFile/law_rule/law_rul

Barrows, Randolph C., and Paul D. Clayton.
'Privacy, Confidentiality, and Electronic Medical Records.'
Journal of the American Medical Informatics Association 3, no. 2 (April 1996): 139–48.
Available at:
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC116296/

Bellovin, S. M.; Blaze, M.; Clark, S.; Landau, S.
'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet'
12 Nw. J. Tech. & Intell. Prop. 1 (2014).
Available at:
http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1

Black, J.
'The role of risk in regulatory processes'
Published in: R. Baldwin, M. Lodge and M. Cave, Oxford Handbook of Regulation, Oxford University Press, 2010.
Available at:
https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199560219.001.0001/oxfordhb-9780199560219-e-14

Cambon-Thomsen, Anne, Emmanuelle Rial-Sebbag, and Bartha M. Knoppers.
'Trends in Ethical and Legal Frameworks for the Use of Human Biobanks'
European Respiratory Journal 30, no. 2 (August 2007): 373–82.
doi:10.1183/09031936.00165006.

Carr, Madeline
'Public-Private Partnerships in National Cyber-Security Strategies'
International Affairs 92, no. 1 (January 2016): 43–62. doi:10.1111/1468-2346.12504.
Available at:
https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

Caulfield, Timothy, Amy L. McGuire, Mildred Cho, Janet A. Buchanan, Michael M. Burgess, et al.
'Research Ethics Recommendations for Whole-Genome Research: Consensus Statement'
PLoS Biology 6, no. 3 (March 2008): 430–35. doi:10.1371/journal.pbio.0060073.

Available at:
https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.0060073

Cavelty, Myriam Dunn
'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse'
International Studies Review 15, no. 1 (March 2013): 105–22. doi:10.1111/misr.12023.
Available at:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200862

Cavelty, Myriam Dunn
'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities'
Science and Engineering Ethics 20, no. 3 (September 2014): 701–15.
doi:10.1007/s11948-014-9551-y.
Available at:
https://link.springer.com/article/10.1007/s11948-014-9551-y

Chang, Betty L., Suzanne Bakken, S. Scott Brown, Thomas K. Houston, et al.
'Bridging the Digital Divide: Reaching Vulnerable Populations'
Journal of the American Medical Informatics Association 11, no. 6 (December 2004): 448–57.
doi:10.1197/jamia.M1535.
Available at:
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC524624/

Darmois, E. and Schméder, G.
'Cybersecurity: a case for a European approach'
Paper commissioned by the Human Security Study Group SiT/WP/11/16, 2016.
Available at:
http://www.securityintransition.org/wpcontent/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf

Delfs, H., Knebl, H.
'Introduction to cryptography (Vol. 2)'
Springer 2015 , ISBN: 978-3-662-47973-5 (Print) 978-3-662-47974-2 (Online).
This book covers key concepts in modern cryptography, from encryption and digital signatures to more advanced cryptographic protocols. Topics on algebra, number theory, probability theory and information theory are included, so no previous background is required.

Friedewald, Michael, J. Peter Burgess, Johann Čas, Walter Peissl and Rocco Bellanova (eds.)
'Surveillance, privacy and security: citizens' perspectives'
Oxon, Routledge, 2017
Available at:
http://www.tandfebooks.com/doi/book/10.4324/9781315619309

Gattiker, U. E., and H. Kelley
'Morality and Computers: Attitudes and Differences in Moral Judgments'
Information Systems Research 10, no. 3 (September 1999): 233–54. doi:10.1287/isre.10.3.233.
Available at:
https://pubsonline.informs.org/doi/10.1287/isre.10.3.233

Goldwasser, Shafi; Bellare, Mihir
Lecture notes on cryptography. Summer course 'Cryptography and computer security' at MIT.
Collection of 2008 lecture notes from the summer course on cryptography at MIT by Shafi Goldwasser and Mihir Bellare. The notes cover most of the basic topics in cryptography, including an introduction to information theory and number theory, which are the basis of modern cryptography.
Available at
https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

Hansen, Marit, Meiko Jensen and Martin Rost
'Protection goals for privacy engineering'
Security and Privacy Workshops (SPW), IEEE, 2015, p. 159-166
Available at:
https://doi.org/10.1109/SPW.2015.13

Harrington, S. J.
'The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions'
Mis Quarterly 20, no. 3 (September 1996): 257–78. doi:10.2307/249656.
Available at:
https://www.jstor.org/stable/249656

Hildebrandt, M., Tielemans, L.
'Data protection by design and technology neutral law'
Computer law & Security Review 29 (2013) 509-521.
Available at:
https://www.sciencedirect.com/science/article/pii/S0267364913001313

Hiller, Janine S., and Roberta S. Russell
'The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison'
Computer Law & Security Review 29, no. 3 (June 2013): 236–45. doi:10.1016/j.clsr.2013.03.003
Available at:
https://www.sciencedirect.com/science/article/pii/S0267364913000575

Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Nordholt, E.S., Spicer, K., de Wolf P.-P.
'Statistical disclosure control'
Wiley and Sons, ISBN: 978-1-119-97815-2
This book introduces the topic of statistical disclosure control and provides several strategies for protecting the privacy of respondents in microdata databases. The work most prominently contains the definition of k-anonymity and other privacy models, along with mechanisms to achieve k-anonymity.

Available at:
https://pdfs.semanticscholar.org/c686/2258a521e3902375b662a99fe897df7810f0.pdf

McGraw, Deven, James X. Dempsey, Leslie Harris, and Janlori Goldman
'Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange'
Health Affairs 28, no. 2 (April 2009): 416–27. doi:10.1377/hlthaff.28.2.416
Available at:
https://www.healthaffairs.org/doi/full/10.1377/hlthaff.28.2.416

Weber, Karsten, Michele Loi, Markus Christen, and Nadine Kleine
'Digital Medicine, Cybersecurity and Ethics: An Uneasy Relationship'
American Journal of Bioethics 18 (9): 52–53. September 2018.
Available at:
https://www.researchgate.net/publication/327551264_Digital_Medicine_Cybersecurity_and_Ethics_An_Uneasy_Relationship

Wiewiórowski Wojciech
'Privacy, security and technology: the Annual Privacy Forum 2017'
Available at:
https://edps.europa.eu/press-publications/press-news/blog/privacy-security-and-technologyannual-privacy-forum-2017_en.

Wright, Rob
'FBI: How we stopped the Mirai botnet attacks'
News article published 7 March 2019 on the SearchSecurity.techtarget.com website.
Available at:
https://searchsecurity.techtarget.com/news/252459016/FBI-How-we-stopped-the-Miraibotnet-attacks

3.2 Results of EU-funded projects

PRESCIENT - Privacy and emerging sciences and technologies

http://www.prescient-project.eu

'PRESCIENT D-3: Privacy, data protection and ethical issues in new and emerging technologies'
Public deliverable, 16 May 2012
Available at:
http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_Deliverable_3_Final.pdf

PRISE - Privacy enhancing shaping of security research and technology

http://www.prise.oeaw.ac.at

'PRISE D-5.8: Synthesis report – interview meetings on security technology and privacy'
Public deliverable, April 2008
Available at:
http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf

'PRISE D-6.2: Criteria for privacy enhancing security technologies'
Public deliverable, 2008
Available at:
http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf

'PRISE D-7.6: Concluding conference statement paper'
Public deliverable (no date)
Available at:
http://www.prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf

RESPECT - Rules, expectations and security through privacy enhanced convenient technologies

http://respectproject.eu

'RESPECT D-11.3: Synthesised all countries report (quantitative data)'
Public deliverable, 19 May 2015 (not available online)

'RESPECT: Periodic report summary 1'
Available at:
http://cordis.europa.eu/result/rcn/153820_en.html

SMART: scalable measures for automated recognition technologies

'SMART: Final Report Summary'
Available at:
http://cordis.europa.eu/result/rcn/178069_en.html

SurPRISE: surveillance, privacy and security

http://surprise-project.eu

'SurPRISE D-6.10: Synthesis report'
Public deliverable, February 2015
Available at:
http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesisreport.pdf

'SurPRISE D-6.12: Workshop report'
Public deliverable, December 2014
Available at:
http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.12-Workshopreport.pdf

'SurPRISE presentation: Aligning security and privacy. En route towards acceptable surveillance'
Sara Degli Esposti, Vincenzo Pavone and Elvira Santiago
Joint conference of SurPRISE, PRISMS and PACT, Vienna, 13-14 November 2014
Available at:
http://surprise-project.eu/wp-content/uploads/2014/11/Degli-Esposti_Aligning-securityand-privacy-en-route-to-ward-acceptable-surveillance.pdf

'SurPRISE, PRISMS and PACT: Abstract booklet'
Citizens' perspectives on surveillance, security and privacy: controversies, alternatives and solutions.
Joint final conference, Vienna, 13-14 November 2014
Available at:
http://surprise-project.eu/wp-content/uploads/2014/11/Booklet_Final.pdf

'SurPRISE: Report summary'
Available at:
http://cordis.europa.eu/result/rcn/171903_en.html

3.3 Policy Documents

Article 29 Working Party (now European Data Protection Board)

'Opinion 9/2001 on the Commission Communication on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"'
WP 51, 5 November 2001
Available at:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2001/wp51_en.pdf

European Commission

Communication from the commission to the European Parliament, the European Council and the Council - Sixteenth Progress Report towards an effective and genuine Security Union
COM (2018): Brussels, 10.10.2018. COM (2018) 690 final
Available at:
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/europeanagenda-security/20181010_com-2018-690-communication_en.pdf

'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'
Communication COM/2000/890 final, Brussels, 26 January 2001
Available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890

'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace'
Joint communication JOIN/2013/1 final, Brussels, 7 February 2013
Available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

'Scientific Advice Mechanism - Scoping Paper: Cybersecurity'
29 January 2016
This work provides an introduction on the cyber-security topic and the state of the policies of the EU.
Available at:
https://ec.europa.eu/research/sam/pdf/meetings/hlg_sam_012016_scoping_paper_cybersecurity.pdf

'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'
Communication COM/2016/410 final, Brussels, 5 July 2016
Available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410

European Union Agency for Network and Information Security (ENISA)

'Definition of Cybersecurity: Gaps and overlaps in standardization'
December 2015.
Available at:
https://www.enisa.europa.eu/publications/definition-of-cybersecurity

'Principles and opportunities for a renewed EU cyber security strategy'
ENISA contribution to the Strategy review, July 2017
Available at:
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-inputto-the-css-review-b

'Privacy and Data Protection by design - from policy to engineering'
This document collects previous works on Privacy-by-design and the strategies to develop software that preserves the privacy of their users. These strategies inspire part of the GDPR and should be followed by compliant software. Next, it describes specific tools and technologies to develop said strategies.
Available at:
https://www.enisa.europa.eu/publications/privacy-and-data-protection-bydesign/at_download/fullReport

'ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity'
Released December 2016
Available at:
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisasopinion-paper-on-encryption

'ENISA Threat Landscape Report 2017'
European Union Agency for Network and Information Security (ENISA), January 15, 2018
https://www.enisa.europa.eu/publications /enisa-threat-landscape-report-2017

ENISA Threat Taxonomy - A tool for structuring threat information.
This report by ENISA contains a taxonomy of threats to information and communication systems, both in the cyber- and physical space. The initial taxonomy was a compilation of works carried out from 2012 to 2015 and has been used internally by ENISA as a common reference in other cybersecurity related reports. In the following years, the ENISA has continually updated the first iteration of this report. At the time of compiling this literature list, the latest update originates from September 2016.
Current version available at:
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisathreat-landscape/threat-taxonomy/view

European Data Protection Supervisor

'Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)'
April 24th 2017
Available at:
https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

'Opinion 8/2015 Dissemination and use of intrusive surveillance technologies'
Brussels, 15 December 2015
Available at:
https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf

'Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a "Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace", and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union'
Brussels, 14 June 2013
Available at:
https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf

European Group on Ethics in Science and New Technologies

'Ethics of Security and Surveillance Technologies'
Opinion No. 28, Brussels, May 20th 2014
Available at:
https://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologiespbNJAJ14028/

Commission Nationale de l'Informatique et des Libertés (CNIL)

'Encryption: security element of information assets'
18 July 2017
Available at:
https://www.cnil.fr/en/what-cnils-position-terms-encryption

'Security of personal data'
4 April 2018.
Available at:
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf