Inclusive Security: Digital Security Meets Web Science

Other titles in Foundations and Trends® in Web Science

An Introduction to Hybrid Human-Machine Information Systems
Gianluca Demartini, Djellel Eddine Difallah, Ujwal Gadiraju and Michele Catasta
ISBN: 978-1-68083-374-4

Minds Online: The Interface between Web Science, Cognitive Science and the Philosophy of Mind
Paul Smart, Robert Clowes and Richard Heersmink
ISBN: 978-1-68083-322-5

Collective Attention on the Web
Christian Bauckhage and Kristian Kersting
ISBN: 978-1-68083-204-4

Inclusive Security: Digital Security Meets Web Science

Lizzie Coles-Kemp
Information Security Group, Royal Holloway University of London
lizzie.coles-kemp@rhul.ac.uk

Artwork used by kind permission of Alice Angus.
Artwork is copyright Alice Angus 2020.

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Web Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

L. Coles-Kemp. *Inclusive Security: Digital Security Meets Web Science*. Foundations and Trends® in Web Science, vol. 7, no. 2, pp. 88–241, 2020.

ISBN: 978-1-68083-783-4

Foundations and Trends® in Web Science

Volume 7, Issue 2, 2020

Editorial Scope

Topics

Foundations and Trends® in Web Science publishes survey and tutorial articles in the following topics:

- Agents and the Semantic Web
- Collective Intelligence
- Content Management
- Databases on the Web
- Data Mining
- Democracy and the Web
- Dependability
- Economics of information and the Web
- E-Crime
- E-Government
- Emergent behaviour
- Ethics
- Hypertext/Hypermedia
- Identity
- Languages on the Web
- Memories for Life
- Mobile/Pervasive
- Network Infrastructures
- Performance
- Privacy
- Scalability
- Security
- Semantic Web
- Social Networking
- Standards
- The Law and the Web
- The Web as an Educational Tool
- The Web in the Developing World
- Trust and Provenance
- Universal Usability
- User Interfaces
- Virtual Reality
- Web Art
- Web Governance
- Search
- Web Services

Information for Librarians

Foundations and Trends® in Web Science, 2020, Volume 7, 4 issues. ISSN paper version 1551-3939. ISSN online version 1551-3947. Also available as a combined paper and online subscription.

Contents

Inclusive Security: Digital Security Meets Web Science

Lizzie Coles-Kemp[1]

[1] *Information Security Group, Royal Holloway University of London*

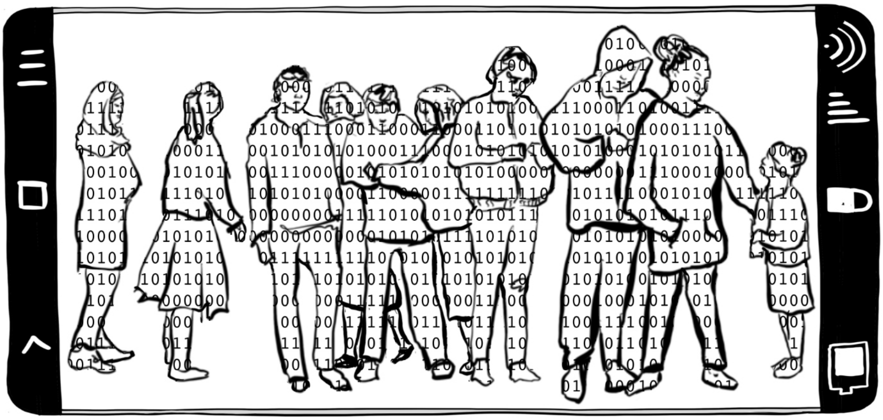
ABSTRACT

The rationale for designing, implementing and managing security technologies has a notion of "risk" at its core; the risk of compromise to technology or information weighed up against the cost of protecting against such an incursion. However, such approaches have been focused on the protection of technology and information, with the assumption that if this is protected then people are also protected; an assumption that is much harder to maintain in a more open, networked context such as the one that has been enabled by growth of the World Wide Web. Grounded in the interdisciplinary endeavours that characterise Web Science, this monograph presents the case for a more inclusive form of technological security. Such a security places the security of technology in the context of the security of people operating in a web-enabled and digitally-connected society and results in a digital security that responds to the enmeshed nature of technology and society. This monograph uses a wide analytical lens that encompasses the sociotechnical infrastructures, networks of power and the practices that shape our interactions with and through digital technologies to explore this more expansive form of security.

Lizzie Coles-Kemp (2020), "Inclusive Security: Digital Security Meets Web Science", Foundations and Trends® in Web Science: Vol. 7, No. 2, pp 88–241. DOI: 10.1561/1800000030.

1

Introduction



Digital technologies are woven across our everyday lives

As we become increasingly dependent on digital products in all aspects of our lives, the reliability of that technology increases in importance. Technological security mechanisms, such as passwords and data encryption, are a key way to ensure reliability in the technological delivery by ensuring that the technology performs as expected. Technological security can be thought of as the control of access to technical systems and the control of the use of those systems.

However, the way that digital technologies are woven across the fabric of our everyday lives, and are embedded in all our institutions, means that we need a paradigm for understanding technological security as being part of other forms of security. This monograph introduces the paradigm of digital security that not only encompasses the protection of digital technologies and the data it produces, but also the practices and processes that link those technologies. It also encompasses the political and social processes and practices that shape the meanings, and experiences of the digital protection mechanisms. In a digitally mediated society, security of the state, of society, of individuals and of technologies are bound together through these processes and practices, giving new security meanings to security technologies and policies.

The political dimensions of security technologies are addressed in cybersecurity scholarship. The study of cybersecurity examines technological security as it intersects with national or global interests (Carr and Lesniewska, 2020). Cybersecurity is primarily understood from the perspective of the state (Carr, 2016; Stevens, 2013), global human rights (Carr, 2013; Deibert, 2018) and global governance (Carr, 2015). There is also an acknowledgement that security has a moral force (Nissenbaum, 2005) and that security technology is political, but there have been few studies that examine how people respond to cybersecurity programmes and to the use of security technologies to regulate everyday transactions and practices. Therefore, the term *"digital security"* is introduced in this monograph to reference the security issues and responses that emerge at the intersections between technological security and other forms of security, from the perspective of a person's everyday lived experience. Digital security connects technological security with social and political issues that shape a person's everyday security and examines technological security in terms of the social impacts that it has. Digital security is an inherently interdisciplinary study and practice that focuses on technologies that predominantly rely on access to the World Wide Web. This makes it a type of interdisciplinary study that falls under the remit of Web Science.

Whilst the connection between technological security and social and political forms of security in people's everyday lives has been made in reference to particular groups of technology users (Parkin *et al.*, 2019; Strohmayer *et al.*, 2017; Matthews *et al.*, 2017) or in reference to surveillance technologies (Gürses *et al.*, 2016; Huysmans, 2011), the connection is not made in the more mainstream security technology studies or practices. This monograph seeks to address this gap and the work presented shows why this perspective should be routinely included in technological security analysis and design.

1.1 Background Research

This monograph distils a body of research and study that began with the VOME project – Visualisation and Other Methods of Expression (VOME, 2010). This 3-year project started in 2007 and re-examined how people use digital services and why they share what they share on-line. In line with a Web Science research approach (Berners-Lee *et al.*, 2006, p.71), VOME acknowledged from the outset that the securing of digital services and technology is embedded in a social setting. The VOME project took an embodied position: wanting to understand how people felt and experienced security when using digital technologies. VOME's core research question was: *"What does privacy sound, feel and look like?"*. The project examined people's attitudes towards informational privacy in on-line settings, and we discovered that when examined from an embodied perspective, the sharing and protection of personal security on-line is experienced as a means of protecting the individual, and their kin and friendship network. The VOME project therefore strayed from traditional privacy studies, and instead focused on the intersections between different types of security, and the security feelings and responses that emerge at those intersections. From this start point, subsequent projects examined how information sharing and protection practices evoke feelings of security and how these feelings, in turn, shape those practices.

The project committed to working with the creative arts in a humanities tradition, as well as drawing on the more traditional digital privacy and usable security research to explore these embodied dimensions and pursue this line of enquiry. In following an embodied line of enquiry, the research revealed that how security technology was *intended* to feel, look and work like was not the actual experience of many of the groups that the project worked with. This was because technological security intersects with other forms of security, and these intersections can engender an embodied sense of insecurity as well as security. For example, if someone is financially insecure, then a complex process of accessing financial services can exacerbate that feeling of insecurity, making the access control processes seem hostile.

Technological security sits at the intersection with other forms of security

People are called upon to prove or verify who they are when setting up a financial service account. This is often a process that requires multiple sources of documentation, not always readily available to the individual or that are costly for the individual to provide. This evidence might be requested using language that can be difficult for the individual to follow and the process might result in a negative outcome if not followed precisely as set-out. For those already feeling insecure or lacking in confidence, the identity verification process can be anxiety-inducing, and result in that individual asking for informal help from their kin and friendship network. This help might be constructive but also might increase the vulnerability of the individual.

Similarly, if someone is feeling anxious and uncertain about their health, remote access to a health system that is complex and impersonal can amplify those feelings of health insecurity. This can lead to either avoidance of the health service or the altering of data submitted to the health system. Both of these information sharing practices can result in increasing the vulnerability of the individual. The anxiety a person experiences with digital health services can be amplified by limited access to digital connectivity and to data. This can result in an individual having to borrow a device from a family member or friend, or can result in an individual having to rely on someone else to upload their records. Both courses of action can increase an individual's anxiety and extend their vulnerabilities to information misuse or denial of access. If healthcare is not free at the point of access, financial worries can also increase the stress of this situation. The research concluded that security technology often felt alienating, confusing and either threatening or useless to many people. Those negative feelings thus shaped how people used such technology and, in particular, the ways in which they shared and protected information.

Taking an embodied position to examine security aspects of human computer interaction was an unusual starting point for research in this area. The more typical position was to examine the topic from an objective, external perspective, using a positivist research paradigm to focus on the security functionality of the digital technology, and the security of the digital interaction.

An embodied position also revealed a wider view of security in digital settings; it revealed that the security practices people undertake in a digital setting are not limited to the interaction with the technology, but are set in the context of wider interactions with people within their kin and friendship networks. For example, Light and Coles-Kemp (2013) showed that in family settings grandmothers with little or no digital expertise can play a significant role in the information sharing and protection practices of their digitally-confident granddaughters. The study with grandmothers and granddaughters challenged the notion that information sharing and protection practices relevant to digital interaction only take place within the interaction itself. The study showed that the information sharing and protection that takes place *around* the digital interaction can have a significant effect on the information sharing and protection that takes place within the interaction. The study also showed that working through a social proxy (somebody who carries out information sharing and protection actions on behalf of another person) can engender feelings of confidence in information sharing and protection practices, as well as encourage critical reflection on those practices within the digital interaction itself.

In the finance, health and family examples above, the traditional focus on the security design of the technology, and the focus on the information sharing and protection within the digital interaction, have meant that exploring the significance of what happens in the space around the digital interaction has been ignored. At the same time, the traditional approach has also not taken into account the ways in which technological security intersects with other forms of security, and how an individual responds to those intersections. Finally, the traditional approach has not examined how the political, social and economic context in which people use technologies shapes the meanings of technological controls. As a result, opportunities for security interventions in those wider spaces have been lost, and the conditions for effective use of technological security have not been created. Based on our research, we argue that studying the information sharing and protection practices in the space around the digital interaction, brings to the fore the political, social and economic meanings of technological controls. We also argue that the embodied position from which these practices emerge must also be understood if technological security controls are to be effective and the value of the expertise in creating such technologies is to be realised.

The VOME research therefore identified a number of blind spots within the traditional ways that we understand technological security:

- Security issues in digitally-mediated interactions are not considered from the perspective of those using the technologies. Instead they are typically considered from the perspective of the experts designing and implementing the relevant technologies and consequently often address issues that are only partially relevant to the users of those technologies.

- Security practices are not understood in the wider context of the social, political and economic complexities within which the interactions take place. Consequently, practices are dismissed as non-compliant when they are, in fact, responding to a different security imperative.

- The potential for technologies and services to harm their users, both intentionally and unintentionally, is not considered as part of the security analysis of a digital product, and yet the potential for harm shapes people's digital practices and experiences.

The research further shone a light on the importance of understanding how technological security intersects with other forms of security, and the responses that emerge at those intersections. VOME research yielded three core insights that illuminate these intersections:

- Assessing risk to digitally-mediated networked interactions requires both the assessment of risks to technology, and of the risks networked technology use pose to the users of that technology;

- The understanding of technological risk needs to be set in the context of the wider concerns that networked technology users are experiencing;

- People often focus on the benefits that they gain from using a technology or service, and consider the technological security risks in relation to that benefit.

The VOME research showed that it is important to understand technological security both in relation to the protection of technology and of people so that we can better understand where:

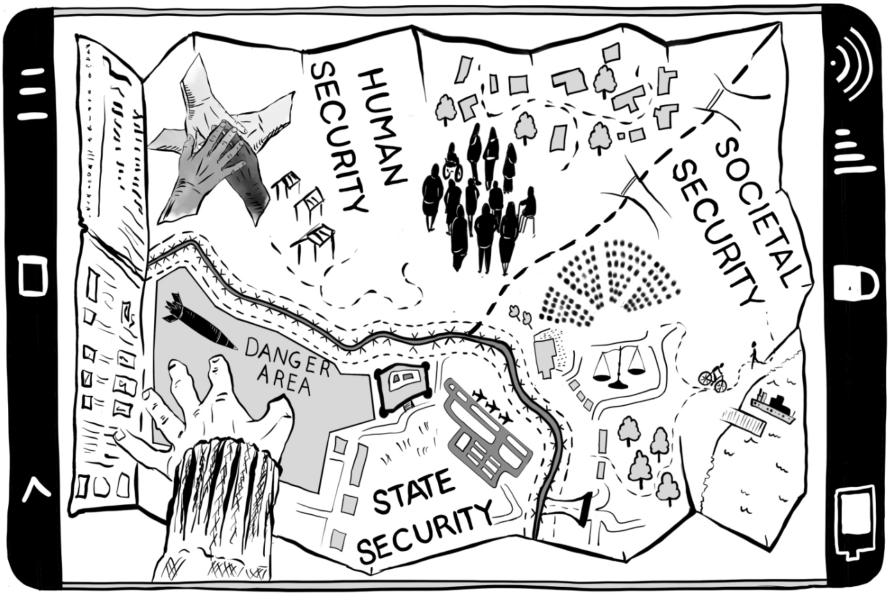
- Security technologies create threats to human computer interaction; and

- Interventions and responses might be made in the spaces around the human computer interaction.

The research has been recognised by the UK's Cyber Security Body of Knowledge (CyBOK, 2019a) as a new area in Cybersecurity Human Factors (CyBOK, 2019b). The practice has also been recognised as part of the UK's National Cyber Security Centre guidance on people-centred security (NCSC, 2019). The guidance titled *You Shape Security* is primarily written for security practitioners: from those who design approaches to technological security within organisations, to those who deploy and manage those approaches.

1.2 Adoption and Development

Following on from VOME, five further projects formed a programme of work grounded on the following position: *for technological security to be effective, a broader digital security must be designed that supports people to both realise the benefits of a digital service and to realise those benefits safely.*



Mapping out a broader digital security

The programme of work has focused on the following research aspirations:

- *Alternative paradigms of technological security*: using the social and political theories of security for inspiration, alternative paradigms for technological security have been investigated and developed.
- *Participatory design and practice for technological security*: using the principles of participatory design and arts-based research practice, methods that generate a wider lens for understanding people-centrred security have been developed and practiced.
- *Inclusion as a form of security*: drawing on thinking and practices related to a conceptualisation of security as a form of empowerment and enablement (and as a collective rather than individualistic issue), digital security structures and practices have been developed using ideas that focus on trust, resilience and collaboration.

The programme of research has developed an inclusive position on digital security that foregrounds benefits for people, and places technological risk in relation to those benefits. The programme of research was further developed through the a UK Research Council funded fellowship, Everyday Safety-Security for Essential Services (ESSfES), and a UK Research Council funded research network that co-ordinates research in social justice in the digital economy (Not-Equal). This network includes a focus on inclusive digital security research under the theme of "Digital Security For All".

1.3 Structure of this Monograph

The monograph starts with a sketch of the main schools of security theory that set out the broader social and political conceptualisations of security into which technological security is deployed. The monograph then briefly sketches technological security and its position on the protection of people, before placing technological security in the wider security theory landscape.

These first three chapters reveal the limitations of traditional security thinking when examining technology use in a digitally-mediated society. In particular, the three chapters show how on the one hand digital technology creates spaces in which people can be empowered to create and shape opportunities, but on the other hand does not provide a means with which to respond to many of the security issues that emerge as a result of that creativity. The next three chapters present a possible way forward in the form of a digital security paradigm that draws on the trust-led, relational, issues-focused work of digital civics, and the broad range of ontological positions from security theory, in order to respond to these limitations.

As a reference, this monograph has the remaining chapters:

- *Security Theory Building Blocks*
  chapter 2: maps out the main schools of thought in political and social theories of security, and reflects on their relevance to technological security.

- *Technological Security and Its Users*
  chapter 3: maps the history of technological security with respect to understanding its intersections with other forms of security.

- *Connecting Technological Security and Security* Theory
  chapter 4: examines how security theory and technological security can be brought further into conversation.

- *Digital Civics, A Practice-Lens and Digital Security*
  chapter 5: introduces a wider lens on human-computer interaction and introduces the notion of practice.

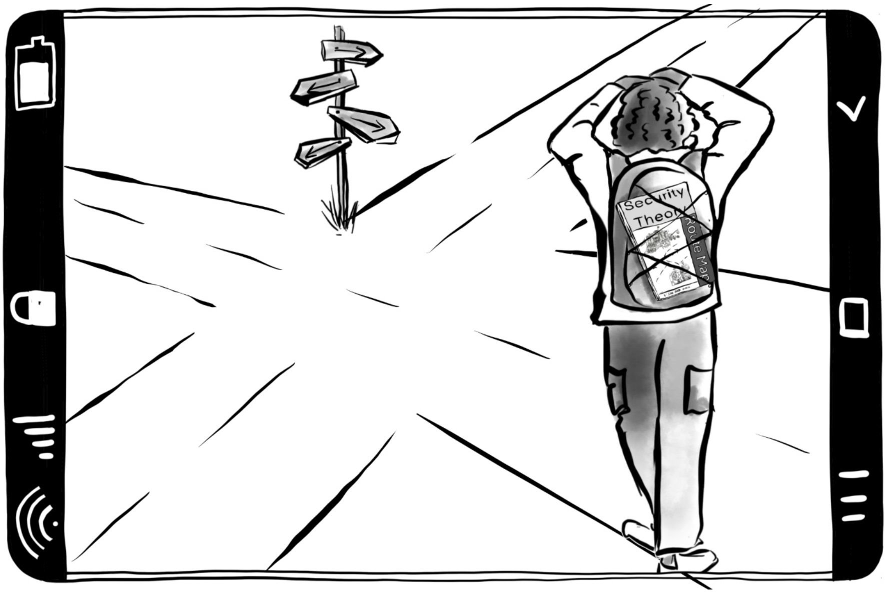
- *Digital Security: Practice and Methods*
  chapter 6: sets out possible approaches to practising and researching digital security.

- *Digital Security From Research to Application*
  chapter 7: sets out three worked examples of digital security and presents key digital security principles.

- *Conclusions and Call to Action*
  chapter 8: summarises the arguments set out in the monograph and issues a call to action.

The intended audience for this monograph is those studying and researching digital design and interaction. The monograph introduces the reader to alternative ways of conceptualising digital technology security. The call to action is to bring together diverse communities of scholarship to develop ideas of inclusive digital security as part of a wider move to build a society that is secure for all.

1.4 Concluding Comments



Setting out on a journey into the security theory landscape

This introduction has set out the case for considering technological security from two positions: from the position of protecting data and technology, and from the position of protecting people in a digitally-mediated society. When considering the latter, we are not solely considering technological security, but where technological security intersects with both other securities and with an individual's embodied sense of security and insecurity. To denote this wider position, the term “digital security” is being applied to this intersectional form of technological security.

In the next chapter we explore political and social theories of security to set the scene for a wider conversation about digital security, and to provide conceptualisations that might help us to better understand some of these intersections outlined in this introductory chapter.

References

Acquisti, A. (2013). “Complementary perspectives on privacy and security: Economics”. *IEEE Security & Privacy*. 11(2): 93–95.

Adams, A. and M. A. Sasse. (1999). “Users are not the enemy”. *Communications of the ACM*. 42(12): 41–46.

Albert, M. and B. Buzan. (2011). “Securitization, sectors and functional differentiation”. *Security dialogue*. 42(4-5): 413–425.

Albrechtsen, E. and J. Hovden. (2009). “The information security digital divide between information security managers and users”. *Computers & Security*. 28(6): 476–490.

Albrechtsen, E. and J. Hovden. (2010). “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study”. *Computers & Security*. 29(4): 432–445.

Anderson, R. (2001). “Why information security is hard-an economic perspective”. In: IEEE. Seventeenth Annual Computer Security Applications Conference. 358–365.

Arcury, T. A. and S. A. Quandt. (1999). “Participant recruitment for qualitative research: A site-based approach to community research in complex societies”. *Human Organization*. 58(2): 128.

Asad, M., C. A. Le Dantec, B. Nielsen, and K. Diedrick. (2017). "Creating a Sociotechnical API: Designing City-Scale Community Engagement". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM. 2295–2306.

Ashenden, D. (2016). "Your employees: the front line in cyber security".

Ashenden, D. and D. Lawrence. (2013). "Can we sell security like soap?: a new approach to behaviour change". In: *Proceedings of the 2013 New Security Paradigms Workshop*. ACM. 87–94.

Ashenden, D. and D. Lawrence. (2016). "Security dialogues: Building better relationships between security and business". *IEEE Security & Privacy*. 14(3): 82–87.

Ashenden, D. and A. Sasse. (2013). "CISOs and organisational culture: Their own worst enemy?" *Computers & Security*. 39: 396–405.

Baldwin, D. A. (1997). "The concept of security". *Review of international studies*. 23(1): 5–26.

Balzacq, T. (2010). "Constructivism and securitization studies". In: *The Routledge handbook of security studies*. Routledge. 56–72.

Balzacq, T. and M. D. Cavelty. (2016). "A theory of actor-network for cyber-security". *European Journal of International Security*. 1(2): 176–198.

Bardzell, J. and S. Bardzell. (2013). "What is critical about critical design?" In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM. 3297–3306.

Baskerville, R. (1991). "Risk analysis: an interpretive feasibility tool in justifying information systems security". *European Journal of Information Systems*. 1(2): 121–130.

Beautement, A., M. A. Sasse, and M. Wonham. (2009). "The compliance budget: managing security behaviour in organisations". In: *Proceedings of the 2008 New Security Paradigms Workshop*. ACM. 47–58.

Becker, I., S. Parkin, and M. A. Sasse. (2017). "Finding security champions in blends of organisational culture". *Proc. USEC*. 11.

Beecham, S., N. Baddoo, T. Hall, H. Robinson, and H. Sharp. (2008). "Motivation in Software Engineering: A systematic literature review". *Information and software technology*. 50(9-10): 860–878.

Bella, G. and L. Coles-Kemp. (2012). “Layered analysis of security ceremonies”. In: *IFIP International Information Security Conference*. Springer. 273–286.

Berners-Lee, T., W. Hall, and J. A. Hendler. (2006). *A framework for web science*. Now Publishers Inc.

Bishop, M. (2005a). “Position: " insider" is relative”. In: *Proceedings of the 2005 workshop on New security paradigms*. 77–78.

Bishop, M. (2005b). “The insider problem revisited”. In: *Proceedings of the 2005 workshop on New security paradigms*. 75–76.

Bissell, D. (2013). “Pointless mobilities: rethinking proximity through the loops of neighbourhood”. *Mobilities*. 8(3): 349–367.

Bjarnason, E. and H. Sharp. (2017). “The role of distances in requirements communication: a case study”. *Requirements Engineering*. 22(1): 1–26.

Blythe, J. M., L. Coventry, and L. Little. (2015). “Unpacking security policy compliance: The motivators and barriers of employees’ security behaviors”. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 103–122.

Box, G. E., N. R. Draper, *et al.* (1987). *Empirical model-building and response surfaces*. Vol. 424. Wiley New York.

Brandt, E. (2006). “Designing exploratory design games: a framework for participation in Participatory Design?” In: *Proceedings of the ninth conference on Participatory design: Expanding boundaries in design-Volume 1*. 57–66.

Burdon, M. and L. Coles-Kemp. (2019). “The significance of securing as a critical component of information security: An Australian narrative”. *Computers & Security*. 87: 101601.

Burdon, M., J. Siganto, and L. Coles-Kemp. (2016). “The regulatory challenges of Australian information security practice”. *Computer Law & Security Review*. 32(4): 623–633.

Buzan, B., O. Wæver, O. Wæver, and J. De Wilde. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Caine, B. (1977). “Computers and the Right to Be Let Alone-A Civil Libertarian View”. *Vill. L. Rev.* 22: 1181.

Caputo, D. D., S. L. Pfleeger, M. A. Sasse, P. Ammann, J. Offutt, and L. Deng. (2016). "Barriers to usable security? Three organizational case studies". *IEEE Security & Privacy*. 14(5): 22–32.

Carlos, M. C., J. E. Martina, G. Price, and R. F. Custódio. (2013). "An updated threat model for security ceremonies". In: *Proceedings of the 28th annual ACM symposium on applied computing*. 1836–1843.

Carr, M. (2013). "Internet freedom, human rights and power". *Australian Journal of International Affairs*. 67(5): 621–637.

Carr, M. (2015). "Power plays in global internet governance". *Millennium*. 43(2): 640–659.

Carr, M. (2016). "Public–private partnerships in national cyber-security strategies". *International Affairs*. 92(1): 43–62.

Carr, M. and F. Lesniewska. (2020). "Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance". *International Relations*. 34(3): 391–412.

Castro Leal, D. de, M. Krüger, K. Misaki, D. Randall, and V. Wulf. (2019). "Guerilla Warfare and the Use of New (and some old) Technology: Lessons from FARC's Armed Struggle in Colombia". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

Chavez, M., B. A. Cotner, and W. Hathaway. (2017). "Building Rapport during Applied Research Recruitment". *Anthropology News*. 58(3): e271–e275.

Chipperfield, C. and S. Furnell. (2010). "From security policy to practice: Sending the right messages". *Computer Fraud & Security*. 2010(3): 13–19.

Cipolla, C. (2009). "Relational services and conviviality". *Designing Services with Innovative Methods. Helsinki, University of Art and Design and Kuopio Academy of Design*: 232–245.

Coles-Kemp, L. (2018). "Practising Creative Securities". https://bookleteer.com/collection.html?id=28.

Coles-Kemp, L. and A. Ashenden. (2012). "Community-centric engagement: lessons learned from privacy awareness intervention design". In: *The 26th BCS Conference on Human Computer Interaction 26*. 1–4.

Coles-Kemp, L., D. Ashenden, A. Morris, and J. Yuille. (2020a). "Digital welfare: designing for more nuanced forms of access". *Policy Design and Practice*: 1–12.

Coles-Kemp, L., D. Ashenden, and K. O'Hara. (2018). "Why should I?: Cybersecurity, the security of the state and the insecurity of the citizen". *Politics and Governance*.

Coles-Kemp, L. and R. B. Jensen. (2019). "Accessing a New Land: Designing for a Social Conceptualisation of Access". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

Coles-Kemp, L., R. B. Jensen, and C. P. Heath. (2020b). "Too Much Information: Questioning Security in a Post-Digital Society". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

Coles-Kemp, L. and F. Stang. (2019). "Making Digital Technology Research Human: Learning from Clowning as a Social Research Intervention". English. *Rivista Italiana di Studi sull'Umorismo (RISU)*. 2(1): 35–45. ISSN: 2611-0970.

Coles-Kemp, L., A. Zugenmaier, and M. Lewis. (2014). "Watching You Watching Me: The Art of Playing the Panopticon". *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*: 147.

Connell, R. W. (2005). *Masculinities*. Polity.

Corbett, E. and C. A. Le Dantec. (2018a). "Exploring trust in digital civics". In: *Proceedings of the 2018 Designing Interactive Systems Conference*. 9–20.

Corbett, E. and C. A. Le Dantec. (2018b). "Going the Distance: Trust Work for Citizen Participation". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM. 312.

Coventry, L., P. Briggs, D. Jeske, and A. van Moorsel. (2014). "Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment". In: *International conference of design, user experience, and usability*. Springer. 229–239.

Crinson, I. (2008). “Assessing the ‘insider–outsider threat’duality in the context of the development of public–private partnerships delivering ‘choice’in healthcare services: A sociomaterial critique”. *Information Security Technical Report*. 13(4): 202–206.

Crivellaro, C., R. Comber, J. Bowers, P. C. Wright, and P. Olivier. (2014). “A pool of dreams: facebook, politics and the emergence of a social movement”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3573–3582.

Crivellaro, C., R. Comber, M. Dade-Robertson, S. J. Bowen, P. C. Wright, and P. Olivier. (2015). “Contesting the city: Enacting the political through digitally supported urban walks”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2853–2862.

Croft, S. (2012). “Constructing ontological insecurity: the insecuritization of Britain’s Muslims”. *Contemporary security policy*. 33(2): 219–235.

Croft, S. and N. Vaughan-Williams. (2017). “Fit for purpose? Fitting ontological security studies ’into’ the discipline of International Relations: Towards a vernacular turn”. *Cooperation and conflict*. 52(1): 12–30.

CyBOK. (2019a). “Cyber Security Body of Knowledge”. https://www.cybok.org/.

CyBOK. (2019b). “Human Factors KA”. https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf.

Deibert, R. J. (2018). “Toward a human-centric approach to cybersecurity”. *Ethics & International Affairs*. 32(4): 411–424.

Deibert, R. J. and R. Rohozinski. (2010). “Risking security: Policies and paradoxes of cyberspace security”. *International Political Sociology*. 4(1): 15–32.

Dewey, J. and M. L. Rogers. (2012). *The public and its problems: An essay in political inquiry*. Penn State Press.

DiSalvo, C., M. Gregg, and T. Lodato. (2014). “Building belonging”. *interactions*. 21(4): 58–61.

DiSalvo, C., T. Jenkins, and T. Lodato. (2016). “Designing speculative civics”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 4979–4990.

Doty, R. L. (1998). “Immigration and the Politics of Security”. *Security Studies*. 8(2-3): 71–93.

Dunn Cavelty, M. (2013). “From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse”. *International Studies Review*. 15(1): 105–122.

Dunphy, P., J. Vines, L. Coles-Kemp, R. Clarke, V. Vlachokyriakos, P. Wright, J. McCarthy, and P. Olivier. (2014). “Understanding the experience-centeredness of privacy and security technologies”. In: *Proceedings of the 2014 New Security Paradigms Workshop*. ACM. 83–94.

Ehn, P. (2008). “Participation in design things”. In: *Proceedings Participatory Design Conference 2008*. ACM.

Flechais, I., J. Riegelsberger, and M. A. Sasse. (2005). “Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems”. In: *Proceedings of the 2005 workshop on New security paradigms*. ACM. 33–41.

Foster, V. (2015). *Collaborative arts-based research for social justice*. Routledge.

Frey, S., A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi. (2017). “The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game”. *IEEE Transactions on Software Engineering*. 45(5): 521–536.

Friedman, B., D. C. Howe, and E. Felten. (2002). “Informed consent in the Mozilla browser: Implementing value-sensitive design”. In: *Proceedings of the 35th annual hawaii international conference on system sciences*. IEEE. 10–pp.

Fukuda-Parr, S. and C. Messineo. (2012). “Human Security: A critical review of the literature”. *Centre for Research on Peace and Development (CRPD) Working Paper*. 11.

Furnell, S. and K.-L. Thomson. (2009). “Recognising and addressing ‘security fatigue’”. *Computer Fraud & Security*. 2009(11): 7–11.

Gabriel, T. and S. Furnell. (2011). “Selecting security champions”. *Computer Fraud & Security*. 2011(8): 8–12.

Geer, D. (2010). “Are companies actually using secure development life cycles?” *Computer*. 43(6): 12–16.

Gjørv, G. H. (2012). “Security by Any Other Name: Negative Security, Positive Security, and a Multi-Actor Security Approach”. *Review of International Studies*. 38(4): 835–859.

Gollmann, D. (1999). *Computer Security*. Wiley.

Guillaume, X. and J. Huysmans. (2019). “The concept of ‘the everyday’: Ephemeral politics and the abundance of life”. *Cooperation and Conflict*. 54(2): 278–296.

Gürses, S., A. Kundnani, and J. Van Hoboken. (2016). “Crypto and empire: the contradictions of counter-surveillance advocacy”. *Media, Culture & Society*. 38(4): 576–590.

Hall, P., C. Heath, L. Coles-Kemp, and A. Tanner. (2015). “Examining the contribution of critical visualisation to information security”. In: *Proceedings of the 2015 New Security Paradigms Workshop*. 59–72.

Haney, J. M. and W. G. Lutters. (2017). “Skills and Characteristics of Successful Cybersecurity Advocates.” In: *SOUPS*.

Hansen, L. (2000). “The Little Mermaid’s silent security dilemma and the absence of gender in the Copenhagen School”. *Millennium*. 29(2): 285–306.

Hansen, L. and H. Nissenbaum. (2009). “Digital disaster, cyber security, and the Copenhagen School”. *International studies quarterly*. 53(4): 1155–1175.

Harbach, M., M. Hettig, S. Weber, and M. Smith. (2014). “Using personal examples to improve risk communication for security & privacy decisions”. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM. 2647–2656.

Harding, M., B. Knowles, N. Davies, and M. Rouncefield. (2015). “HCI, civic engagement & trust”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2833–2842.

Herley, C., P. C. Van Oorschot, and A. S. Patrick. (2009). “Passwords: If we’re so smart, why are we still using them?” In: *International Conference on Financial Cryptography and Data Security*. Springer. 230–237.

HMG. (2012). “Government Digital Strategy”. https://www.gov.uk/government/publications/government-digital-strategy.

HMG. (2019). "The Cross Government Transformation". https://www.gov.uk/government/collections/the-cross-government-transformation-programme.

Hoogensen, G. and S. V. Rottem. (2004). "Gender Identity and the Subject of Security". *Security Dialogue*. 35(2): 155–171.

Hooper, C. (2001). *Manly states: Masculinities, international relations, and gender politics*. Columbia University Press.

Howard, M. and S. Lipner. (2006). *The security development lifecycle*. Vol. 8. Microsoft Press Redmond.

Hudson, H. (2005). "'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security". *Security Dialogue*. 36(2): 155–174.

Hudson, N. F., A. Kreidenweis, and C. Carpenter. (2013). "Human security". In: *Critical approaches to security*. Routledge. 24–36.

Huysman, M., V. Wulf, *et al.* (2004). *Social capital and information technology*. Mit Press.

Huysmans, J. (2011). "What's in an act? On security speech acts and little security nothings". *Security dialogue*. 42(4-5): 371–383.

Inglesant, P. G. and M. A. Sasse. (2010). "The true cost of unusable password policies: password use in the wild". In: ACM.

Kaldor, M. (2007). *Human security*. Polity.

Kiran, A. H. and P.-P. Verbeek. (2010). "Trusting our selves to technology". *Knowledge, Technology & Policy*. 23(3-4): 409–427.

Kirlappos, I., S. Parkin, and M. A. Sasse. (2014). "Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security". In:

Kitchin, R. and M. Dodge. (2011). *Code/space: Software and everyday life*. Mit Press.

Knowles, B. and V. L. Hanson. (2018). "Older adults' deployment of 'distrust'". *ACM Transactions on Computer-Human Interaction (TOCHI)*. 25(4): 1–25.

Kocksch, L., M. Korn, A. Poller, and S. Wagenknecht. (2018). "Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices". *Proceedings of the ACM on Human-Computer Interaction*. 2(CSCW): 1–20.

Kuutti, K. (2013). "'Practice turn'and CSCW identity". *ECSCW 2013 Adjunct Proceedings*: 39–44.

Kuutti, K. and L. J. Bannon. (2014). "The turn to practice in HCI: towards a research agenda". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3543–3552.

Le Dantec, C. (2012). "Participation and publics: supporting community engagement". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1351–1360.

Le Dantec, C. A. (2016). *Designing publics*. MIT Press.

Le Dantec, C. A., J. E. Christensen, M. Bailey, R. G. Farrell, J. B. Ellis, C. M. Danis, W. A. Kellogg, and W. K. Edwards. (2010). "A tale of two publics: Democratizing design at the margins". In: *Proceedings of the 8th acm conference on designing interactive systems*. 11–20.

Lefebvre, H. and C. Levich. (1987). "The everyday and everydayness". *Yale French Studies*. (73): 7–11.

Lester, H. D., G. B. McKay, and E. A. Lester. (2019). "Sociotechnical systems for high rise detention". In: *Transdisciplinary Engineering for Complex Socio-technical Systems: Proceedings of the 26th ISTE International Conference on Transdisciplinary Engineering, July 30–August 1, 2019*. Vol. 10. IOS Press. 319.

Lewis, J. D. and A. Weigert. (1985). "Trust as a social reality". *Social forces*. 63(4): 967–985.

Lewis, M., L. Coles-Kemp, *et al.* (2014). "A tactile visual library to support user experience storytelling". *DS 81: Proceedings of NordDesign 2014, Espoo, Finland 27-29th August 2014*: 386–395.

Light, A. and L. Coles-Kemp. (2013). "Granddaughter beware! an intergenerational case study of managing trust issues in the use of Facebook". In: *International Conference on Trust and Trustworthy Computing*. Springer. 196–204.

Lippmann, W. *et al.* (1943). "US foreign policy: Shield of the republic".

Lipschutz, R. D. (1995). *On security*. Columbia University Press.

Lopez, T., M. Petre, and B. Nuseibeh. (2012). "Getting at ephemeral flaws". In: *Proceedings of the 5th International Workshop on Co-operative and Human Aspects of Software Engineering*. IEEE Press. 90–92.

Lovejoy, K. and G. D. Saxton. (2012). “Information, community, and action: How nonprofit organizations use social media”. *Journal of computer-mediated communication*. 17(3): 337–353.

Luhmann, N. (2000). “Familiarity, confidence, trust: Problems and alternatives”. *Trust: Making and breaking cooperative relations*. 6: 94–107.

MacEwan, N. F. (2017). “Responsibilisation, rules and rule-following concerning cyber security: findings from small business case studies in the UK”. *PhD thesis*. University of Southampton.

Martina, J. E., E. Dos Santos, M. C. Carlos, G. Price, and R. F. Custódio. (2015). “An adaptive threat model for security ceremonies”. *International Journal of Information Security*. 14(2): 103–121.

Mattelmäki, T. *et al.* (2006). *Design probes*. Aalto University.

Matthews, T., K. O’Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo. (2017). “Stories from survivors: Privacy & security practices when coping with intimate partner abuse”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2189–2201.

McCarthy, J. and P. Wright. (2004). “Technology as experience”. *interactions*. 11(5): 42–43.

McLoughlin, I. and R. Wilson. (2013). *Digital government at work: a social informatics perspective*. OUP Oxford.

Miettinen, R., D. Samra-Fredericks, and D. Yanow. (2009). “Re-turn to practice: An introductory essay”. *Organization studies*. 30(12): 1309–1327.

Mollering, G. (2006). *Trust: Reason, routine, reflexivity*. Emerald Group Publishing.

Molotch, H. (2013). “Everyday security: Default to decency”. *IEEE Security & Privacy*. 11(6): 84–87.

Mols, F., S. A. Haslam, J. Jetten, and N. K. Steffens. (2015). “Why a nudge is not enough: A social identity critique of governance by stealth”. *European Journal of Political Research*. 54(1): 81–98.

Muir, R. and I. Parker. (2014). *Many to many: How the relational state will transform public services*. IPPR.

Müller, C., C. Neufeldt, D. Randall, and V. Wulf. (2012). “ICT-development in residential care settings: sensitizing design to the life circumstances of the residents of a care home”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2639–2648.

Nadi, S., S. Krüger, M. Mezini, and E. Bodden. (2016). “Jumping through hoops: Why do Java developers struggle with cryptography APIs?” In: *Proceedings of the 38th International Conference on Software Engineering*. ACM. 935–946.

NCSC. (2019). “You Shape Security”. https://www.ncsc.gov.uk/collection/you-shape-security.

Nicholson, J., L. Coventry, and P. Briggs. (2017). “Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection”. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 285–298.

Nicholson, J., L. Coventry, and P. Briggs. (2019). “If It’s Important It Will Be A Headline: Cybersecurity Information Seeking in Older Adults”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. 349.

Nicolini, D. (2012). *Practice theory, work, and organization: An introduction*. OUP Oxford.

Nissenbaum, H. (2005). “Where computer security meets national security”. *Ethics and Information Technology*. 7(2): 61–73.

Nyman, J. (2013). “Securitization theory”. In: *Critical approaches to security*. Routledge. 51–62.

Olivier, P. and P. Wright. (2015). “Digital civics: Taking a local turn”. *interactions*. 22(4): 61–63.

OpenUniversity. (2020). “Motivating Jenny”. https://www.motivatingjenny.org.

Parkin, S., T. Patel, I. Lopez-Neira, and L. Tanczer. (2019). “Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse”. In: *Proceedings of the New Security Paradigms Workshop*. 1–15.

Peacock, S. and D. Al-Shahrabi. “HCI, Digital Civics and the Refugee Crisis: Challenges at the Intersection of the Field”.

Pham, H. C., L. Brennan, and S. Furnell. (2019). "Information security burnout: Identification of sources and mitigating factors from security demands and resources". *Journal of Information Security and Applications*. 46: 96–107.

Pierce, J. (2019). "Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. 45.

Pieters, W. (2011). "Representing humans in system security models: An actor-network approach." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 2(1): 75–92.

Potter, B. (2009). "Microsoft SDL threat modelling tool". *Network Security*. 2009(1): 15–18.

Power, M. (1994). *The audit explosion*. No. 7. Demos.

Probst, C. W. and R. R. Hansen. (2008). "An extensible analysable system model". *Information security technical report*. 13(4): 235–246.

Probst, C. W., R. R. Hansen, and F. Nielson. (2006). "Where can an insider attack?" In: *International Workshop on Formal Aspects in Security and Trust*. Springer. 127–142.

Puussaar, A., I. G. Johnson, K. Montague, P. James, and P. Wright. (2019). "Making Open Data Work for Civic Advocacy". *CSCW Paper, In Press.*

Reinfelder, L., R. Landwirth, and Z. Benenson. (2019). "Security Managers Are Not The Enemy Either". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. 433.

Renaud, K. (2011). "Blaming noncompliance is too convenient: What really causes information breaches?" *IEEE Security & Privacy*. 10(3): 57–63.

Renaud, K., S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron. (2018). "Is the responsibilization of the cyber security risk reasonable and judicious?" *computers & security*. 78: 198–211.

Riegelsberger, J., M. A. Sasse, and J. D. McCarthy. (2005). "The mechanics of trust: A framework for research and design". *International Journal of Human-Computer Studies*. 62(3): 381–422.

RISCS. (2018). "Annual Report 2018". https://www.riscs.org.uk/wp-content/uploads/2019/03/2018-RISCS-Annual-Report.pdf.

Roe, P. (2008). “The ’value’ of positive security”. *Review of international studies*. 34(4): 777–794.

Rogaway, P. (2009). “Practice-oriented provable security and the social construction of cryptography”. *Unpublished essay.*

Rosenberg, S. (2008). *Dreaming in Code: Two Dozen Programmers, Three Years, 4,732 Bugs, and One Quest for Transcendent Software.* Three Rivers Press. ISBN: 9781400082476.

Rossitto, C., M. Normark, and L. Barkhuus. (2017). “Interactive Performance as a Means of Civic Dialogue”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM. 4850–4862.

Saltzer, J. H. and M. D. Schroeder. (1975). “The protection of information in computer systems”. *Proceedings of the IEEE*. 63(9): 1278–1308.

Schmidt, K. (2014). “The concept of ‘practice’: What’s the point?” In: *COOP 2014-Proceedings of the 11th International Conference on the Design of Cooperative Systems, 27-30 May 2014, Nice (France)*. Springer. 427–444.

Schofield, T., J. Vines, T. Higham, E. Carter, M. Atken, and A. Golding. (2013). “Trigger shift: participatory design of an augmented theatrical performance with young people”. In: *Proceedings of the 9th ACM Conference on Creativity & Cognition*. ACM. 203–212.

Schorch, M., L. Wan, D. W. Randall, and V. Wulf. (2016). “Designing for those who are overlooked: Insider perspectives on care practices and cooperative work of elderly informal caregivers”. In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. 787–799.

Shea, P. (2016). “Civic practices, design, and makerspaces”. *Negotiating digital citizenship: Control, contest and culture*: 231–246.

Shires, J. (2019). “Family Resemblance or Family Argument? Three Perspectives on Cybersecurity and their Interactions”. *St Antony’s International Review*. 15(1): 18–36.

Shires, J. (2020). “Cyber-noir: Cybersecurity and popular culture”. *Contemporary Security Policy*. 41(1): 82–107.

Shostack, A. (2008). “Experiences Threat Modeling at Microsoft.” In: *MODSEC@ MoDELS*.

Singh, S., A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. (2007). “Password sharing: implications for security design based on social practice”. In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM. 895–904.

Sismondo, S. (2010). *An introduction to science and technology studies*. Vol. 1. Wiley-Blackwell Chichester.

Smith, G. M. (2005). “Into Cerberus’ Lair: Bringing the Idea of Security to Light”. *The British Journal of Politics & International Relations*. 7(4): 485–507.

Stanton, B., M. F. Theofanos, S. S. Prettyman, and S. Furman. (2016). “Security fatigue”. *IT Professional*. 18(5): 26–32.

Stevens, G. and V. Wulf. (2002). “A new dimension in access control: Studying maintenance engineering across organizational boundaries”. In: *Proceedings of the 2002 ACM conference on Computer supported cooperative work*. 196–205.

Stevens, T. (2013). *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Taylor & Francis.

Stewart, G. and D. Lacey. (2012). “Death by a thousand facts: Criticising the technocratic approach to information security awareness”. *Information Management & Computer Security*. 20(1): 29–38.

Strohmayer, A., M. Laing, and R. Comber. (2017). “Technologies and social justice outcomes in sex work charities: fighting stigma, saving lives”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3352–3364.

Taylor, A. S., S. Lindley, T. Regan, D. Sweeney, V. Vlachokyriakos, L. Grainger, and J. Lingel. (2015). “Data-in-place: Thinking through the relations between data and community”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM. 2863–2872.

Tronto, J. C. (1993). *Moral boundaries: A political argument for an ethic of care*. Psychology Press.

UKRI. (2020). “UKRI Grants”. https://gtr.ukri.org/person/7CBB849B-4C10-46F9-9B14-F00670C59A10.

Vaughan-Williams, N. and D. Stevens. (2016). “Vernacular theories of everyday (in) security: The disruptive potential of non-elite knowledge”. *Security Dialogue*. 47(1): 40–58.

Vines, J., M. Blythe, P. Dunphy, V. Vlachokyriakos, I. Teece, A. Monk, and P. Olivier. (2012). “Cheque mates: participatory design of digital payments with eighty somethings”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1189–1198.

Vines, J., R. Clarke, P. Wright, J. McCarthy, and P. Olivier. (2013). “Configuring participation: on how we involve people in design”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 429–438.

Vlachokyriakos, V., C. Crivellaro, C. A. Le Dantec, E. Gordon, P. Wright, and P. Olivier. (2016). “Digital civics: Citizen empowerment with and through technology”. In: *Proceedings of the 2016 CHI conference extended abstracts on human factors in computing systems*. ACM. 1096–1099.

VOME. (2010). “VOME Website”. http://vome.uk/.

Weir, C., A. Rashid, and J. Noble. (2016). “Reaching the masses: A new subdiscipline of app programmer education”. In: *Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering*. ACM. 936–939.

Wensveen, S., K. Overbeeke, and T. Djajadiningrat. (2000). “Touch me, hit me and I know how you feel: a design approach to emotionally rich interaction”. In: *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques*. ACM. 48–52.

Whitworth, S. (1994). *Feminism and international relations: towards a political economy of gender in interstate and non-governmental institutions*. Springer.

Whyte, C. (2018). “Crossing the digital divide: Monism, dualism and the reason collective action is critical for cyber theory production”. *Politics and Governance*. 6(2): 73.

Wibben, A. T. (2010). “Feminist security studies”. In: *The Routledge Handbook of Security Studies*. Routledge. 84–94.

Wixon, D., K. Holtzblatt, and S. Knox. (1990). “Contextual design: an emergent view of system design”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Citeseer. 329–336.

Wolfers, A. (1952). “" National security" as an ambiguous symbol”. *Political science quarterly*. 67(4): 481–502.

Woltjer, R. (2017). “Workarounds and trade-offs in information security–an exploratory study”. *Information & Computer Security*. 25(4): 402–420.

Zurko, M. E. and R. T. Simon. (1996). “User-centered security”. In: *NSPW*. Vol. 96. Citeseer. 27–33.