



## UvA-DARE (Digital Academic Repository)

### What harms may come?

*Exploring the anticipatory dimensions of surveillance resistance in an age of datafication*

Kazansky, B.

### Publication date

2021

[Link to publication](#)

### Citation for published version (APA):

Kazansky, B. (2021). *What harms may come? Exploring the anticipatory dimensions of surveillance resistance in an age of datafication*.

### General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

### Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

# References

Abrahamsen R and Williams M (2011) Security Privatization and Global Security Assemblages. *The Brown Journal of World Affairs*, 18(1): 171-180.

Acquisti A (2010) From the Economics to the Behavioral Economics of Privacy: A Note. In: Kumar A., Zhang D (eds) Ethics and Policy of Biometrics. ICEB 2010. *Lecture Notes in Computer Science*. 6005. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-642-12595-9\\_4](https://doi.org/10.1007/978-3-642-12595-9_4)

Acquisti A and Grossklags J (2007) What can behavioral economics teach us about privacy. In: De Capitani di Vimercati S, Gritzalis S, Lambrinouidakis C, et al. (eds) *Digital Privacy: Theory, Technologies and Practices*. Auerbach Publications, pp. 363–377.

Adams A and Sasse MA (1999) Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12): 40–46, December 1999.

Adams V, Murphy M and Clarke AE (2009) Anticipation: Technoscience, life, affect, temporality. *Subjectivity* 28: 246–265.

Ahmed N and Aoun S (2018) Please Don't Include Us Thank You. In: *Theorizing the Web*, New York, 27 April 2018.

Alvial-Palavicino C (2015) The future as practice. A framework to understand anticipation in science and technology. *Tecnoscienza* 6(2): 135–172.

Amnesty International (2017) Human Rights Defenders Under Threat – a shrinking space for civil society. Report, Amnesty International Ltd London. Available at: <https://www.amnesty.nl/content/uploads/2017/05/HRD-briefing-26-April-2017-FINAL.pdf?x18276> (accessed March 5 2021).

Amoore L (2013) *The Politics of Possibility: Risk and Security beyond Probability*. Durham, NC: Duke University Press.

Amoore L (2020) *Cloud Ethics*. Durham, NC: Duke University Press.

Amoore L and de Goede M (2008) *Risk and the war on terror*. London: Routledge.

Amoore L and Langley P (2004) *Ambiguities of Global Civil Society*. *Review of International Studies*, 30(1): 89-110.

Amsler S and Facer K (2017) Contesting anticipatory regimes in education: Exploring alternative educational orientations to the future. *Futures*.  
<https://doi.org/10.1016/j.futures.2017.01.001>

Anderson B (2007) Hope for nanotechnology: Anticipatory knowledge and the governance of affect. *Area* 39(2): 156–165.

Anderson B (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34(6): 777–798.

Anderson B and Adey P (2011) Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue* 43(2): 99-117.

Andrejevic M (2005) The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society* 2(4): 479–97

Andrejevic M (2017) To pre-empt a thief. *International Journal of Communication* (11): 879–896.

Andrejevic M, Dencik L and Trere, E (2019) From preemption to slowness: assessing the contrasting temporalities of data-driven predictive policing. *New Media and Society* 22(9): 1528-1544.

Andrejevic M (2019). *Automated media*. London & New York: Routledge.

Annany M and Finn M (2020) Anticipatory news infrastructures: Seeing journalism's expectations of future publics in its sociotechnical systems. *New media & society* 22(9) 1600–1618

Aouragh M, Gürses S, Rocha J, et al. (2015) Let's first get things done! On division of labour and techno-political practices of delegation in times of crisis. *Fibreculture Journal* (26): 208–235. DOI: 10.15307/fcj.26.196.2015

Aradau C (2018) Governing others: Anomaly and the algorithmic subject of security. *European Journal of International Security* 3(1): 1-21. DOI:10.1017/eis.2017.14

Aradau C and Blanke T (2017) Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory* 20(3): 373–391.

Aradau C and van Munster R (2008) Taming the Future: The Dispositif of Risk in the War on Terror. In: Amoore L and de Goede M (eds). *Risk and the War on Terror*. London, UK: Routledge.

Aradau C and van Munster R (2012) The Time/Space of Preparedness: Anticipating the “Next Terrorist Attack”. *Space and Culture* 15(2): 98–109. DOI: 10.1177/1206331211430015.

APC Women's Rights Programme Feminist Tech eXchange (2019). Available at: <https://www.apc.org/en/project/feminist-tech-exchange> (accessed 5 August 2020).

Asgharpour F, Liu D and Camp LJ (2007) Mental models of computer security risks. In Proceedings of the 6th annual workshop on the economic of information security (WEIS 2007).

Baek G and Mooney T (2020) LAPD not giving up on data-driven policing, even after scrapping controversial program. *CBS news*, 23 February, 2020.

Ballesterio A (2015) The ethics of a formula: calculating a financial-humanitarian price for water American. *Ethnologist* 42 (2): 262-278

Ball K and Snider L (eds) (2013) *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. London: Routledge.

Baker K (2021) What is Cyber Threat intelligence? Available at: <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/> (accessed 1 August 2021).

Barnard-Wills D (2012) E-safety education: Young people, surveillance and responsibility. *Criminology & Criminal Justice* 12(3):239-255. DOI:10.1177/1748895811432957

Bauman Z, Bigo D, Esteves P, et al. (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121-144.

Baumer EPS, Ames, MG, Burrell J, et al. (2015) Why study technology non-use? *First Monday* 20 (11 – 2). <http://dx.doi.org/10.5210/fm.v20i11.6310>

Beck U (1992) *Risk Society: Toward a New Modernity*. New York: Sage.

Bellanova R and de Goede M (2020) The Algorithmic Regulation of Security: An Infrastructural Perspective. *Regulation & Governance*. <https://doi.org/10.1111/rego.12338>

Benjamin R (2016) Informed Refusal: Toward a Justice-Based Bioethics. *Science, Technology, & Human Values* 41(6): 967–90. <https://doi.org/10.1177/0162243916656059>

Benjamin R (2019) *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge, MA: Polity.

Beraldo D and Milan S (2019) From data politics to the contentious politics of data. *Big Data & Society*. <https://doi.org/10.1177/2053951719885967>

Bigo D (2006) Globalized in-security: The field of the professionals of unease management and the Ban- opticon. In: Solomon J and Sakai N (eds) *Traces: A Multilingual Series of Cultural Theory* 4 (Translation, Philosophy and Colonial Difference). Hong Kong: University of Hong Kong Press, pp. 109–157.

Boggs C (1977) Marxism, prefigurative communism and the problem of workers' control. *Radical America*, 6(Winter): 99– 122.

Blythe J and Camp LJ (2012) Implementing mental models. In: IEEE Symposium on Security and Privacy Workshops, pp. 86–90. IEEE Computer Society.

Body & Data (year unknown). Available at: <https://bodyanddata.org/> (accessed 18 January 2021).

boyd d (2008) *Taken out of context: American teen sociality in networked publics*. PhD Dissertation, University of California Berkeley.

Bouk D (2015) *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual*. Chicago: University of Chicago Press.

Bourbeau B (2018) A Genealogy of Resilience. *International Political Sociology*. 12(1): 19–35. <https://doi.org/10.1093/ips/olx026>

Bowker G and Star SL (1999) *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press.

Brand S and Sander I (2020) *Critical data literacy tools for advancing data justice: A guidebook*. Data Justice Lab, Cardiff, Wales, UK. Available at: <https://datajustice.files.wordpress.com/2020/06/djl-data-literacy-guidebook.pdf> (accessed 4 December 2020).

Braun V and Clarke V (2019) Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health* 11(4): 589-597. DOI:10.1080/2159676X.2019.1628806

Braun V and Clarke V (n.d.) Thematic analysis | a reflexive approach. Available at: <https://www.psych.auckland.ac.nz/en/about/thematic-analysis.html>

Brayne S (2017) Big data surveillance: the case of policing. *American Sociological Review* 82: 977–1008.

Brayne S (2020) *Predict and Surveil. Data, Discretion, and the Future of Policing*. Oxford University Press.

Brown D and Pytlak A (2020) Why Gender Matters in International Cyber Security. Report, Association for Progressive Communications, April. Available at: <https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security> (accessed 3 July 2020).

Browne S (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Brooks S (2019) Defending Politically Vulnerable Organizations Online. Report, Center for Long-term Cybersecurity. Available at: <https://cltc.berkeley.edu/2018/07/24/defending-politically-vulnerable-organizations-online/> (accessed 8 March 2019).

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.



Bucher T (2017) The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society* 20(1): 30–44.

Buolamwini J and Gebru T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness, accountability and transparency (2018), pp. 77-91 (January).

Burrell J (2009) The Field Site as a Network: A Strategy for Locating Ethnographic Research. *Field Methods* 21(2): 181–99.

Callon M and Law J (2005) On Qualculation, Agency, and Otherness. *Environment and Planning D: Society and Space* 23(5):717-733.  
DOI:10.1068/d343t

Carmi E, Yates S and Pawluczuk A et al. (2020) Data citizenship: rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review* [online] 9(2). Available at: <https://policyreview.info/articles/analysis/data-citizenship-rethinking-data-literacy-age-disinformation-misinformation-and>

Castoriadis C (2005) *The Imaginary Institution of Society*. Cambridge: Polity Press.

Chan SA (2013) *Networking Peripheries. Technological Futures and the Myth of Digital Universalism*. Cambridge: MIT Press.

Citizen Lab (2014) Extended analysis: Civil society perspectives and responses. *Communities @ Risk: Targeted Digital Threats Against Civil Society*. Report, Citizen Lab, University of Toronto. Available at: <https://targetedthreats.net/media/2.3%20Extended%20Analysis-CivilSociety.pdf> (accessed 23 December 2020).

Clarke AE (2015) Anticipation work: Abduction, simplification, hope. In: Bowker, GC, Timmermans, S, Clarke, AE, et al. (eds) *Boundary Objects*

*and Beyond: Working With Leigh Star* (pp. 85–120). Cambridge: MIT Press.

Clark-Ginsberg B and Slayton R (2017) A Innovation or Maintenance? The Creation and Evolution of Critical Infrastructure Cybersecurity Standards.

Coaffee J (2013) Rescaling and Responsibilising the Politics of Urban Resilience: From National Security to Local Place-Making. *Politics* 33(4): 240–252.

Cochoy F (2008) Calculation, qualculation, calculation: shopping cart arithmetic, equipped cognition and the clustered consumer. *Marketing Theory*. 8(1):15-44. DOI:10.1177/1470593107086483

Coding Rights (year unknown) Safer Nudes. Available at: <https://www.codingrights.org/safernudes/> (accessed June 20, 2019).

Coleman G (2013) *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.

Costanza-Chock, S, Wagoner, M, Taye, B, et al. (2018) #MoreThanCode: Practitioners Reimagine the Landscape of Technology for Justice and Equity. Report, Research Action Design & Open Technology Institute, Washington, DC, USA.

Cox J (2014) The rise of the anti-facial recognition movement. In: *The Kernel*. Available at: <https://kernelmag.dailydot.com/issue-sections/features-issue-sections/10247/anti-facial-recognition-movement>

Couldry N and Powell A (2014) Big data from the bottom up. *Big Data & Society* 1(2): 1–5. [https:// doi.org/10.1177/2053951714539277](https://doi.org/10.1177/2053951714539277).

Couture S and Toupin S (2019) What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*. 21(10): 2305-2322. DOI: 10.1177/1461444819865984

Crawford K (2019) Halt the use of facial-recognition technology until it is regulated. *Nature* 572(7771): 565. Available at: <https://www.nature.com/articles/d41586-019-02514-7> (accessed 21 January 2020).

Critical Arts Ensemble (2001) *Digital Resistance. Explorations in Tactical Media*. New York: Autonomedia.

Critical resistance (2021) History. Available at: <http://criticalresistance.org/about/history/> (accessed 3 May 2019).

Daskal E (2018) Let’s be careful out there...: how digital rights advocates educate citizens in the digital age. *Information, Communication & Society* 21(2): 241–256.

Datafication and Community Activism Workshop (2019) What we mean when we say #AbolishBigData2019. Medium. Mar. 22. Available at: <https://medium.com/@rncrooks/what-we-mean-when-we-say-abolishbigdata2019-d030799ab22e>

Davis A and Mendieta E (2005) *Abolition Democracy: Beyond Empire, Prisons, and Torture*. New York: Seven Stories.

de Goede M (2004) Repoliticising financial risk. *Economy and Society* 33(2): 197-217.

de Goede M (2008) The politics of preemption and the War on Terror in Europe. *European Journal of International Relations* 14(1): 161-185.

de Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.

- de Goede M (2014) Preemption Contested: Suspect Spaces and Preventability in the July 7 Inquest. *Political Geography* 39: 48-57.
- de Goede M (2014) The politics of privacy in the age of preemptive security. *International Political Sociology* 8(1): 100-104.
- de Goede M, Simon S and Hoijsink M (2014). Performing preemption. *Security Dialogue*, 45(5): 411-422.  
<https://doi.org/10.1177/0967010614543585>
- de Goede M and Randalls S (2009) Preemption, Precaution: Arts and Technologies of the Governable Future. *Environment and Planning D: Society and Space* 27(5): 859-878.
- De Filippi P and Treguer F (2014) Expanding the Internet commons: The subversive potential of wireless community networks. *Journal of Peer Production* 6. Available at:  
<http://peerproduction.net/wp-content/uploads/2015/01/De-Filippi-Tréguer-Expanding-the-Internet-Commons-with-Community-Networks.pdf>
- De Hert P and Vis T (2005) Intelligence led policing ontleed. *Tijdschrift voor Criminologie* 47(4): 365 – 376.
- Deleuze G (1992) Postscript on the societies of control. *October* 59(1): 3–7.
- Della Porta D, Peterson A and Reiter, H (2006) (eds) *The Policing of Transnational Protest*. Farnham: Ashgate.
- Della Porta D and Reiter H (1998) *Policing protest: The control of mass demonstrations in Western democracies*. Minneapolis: University of Minneapolis Press.
- Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society* 3(2): 1–12. DOI: 10.1177/2053951716679678.

Dencik L and Cable J (2017) The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication* 11: 763–781.

Dencik L, Hintz A, Carey Z et al. (2015) Managing 'threats': uses of social media for policing domestic extremism and disorder in the UK. Report, Cardiff University, Wales.

Dencik, L, Hintz, A, Carey, Z (2017) Prediction, preemption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. *New Media & Society* 20(4): 1433–1450.

Decnik L, Hintz A, Redden J et al. (2019). Data Scores as Governance: Investigating uses of citizen scoring in public services. Report, Data Justice Lab, Cardiff University, Wales, December.

De Vries P and Schinkel W (2019) Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms. *Big Data and Society*. <https://doi.org/10.1177/2053951719851532>.

Didier E (2018) Globalization of Quantitative Policing: Between Management and Statactivism. *Annual Review of Sociology* 44(1): 515-534.

D'Ignazio C (2017) Creative Data Literacy. *Information Design Journal* 23(1): 6-18.

D'Ignazio C and Klein L (2020) *Data Feminism*. Cambridge, MA: MIT Press.

Doringer B and Felderer B (eds) (2018) *Faceless. Re-Inventing Privacy Through Subversive Media Strategies*. Berlin: De Gruyter.

Douglas M (1992) *Risk and Blame: Essays in Cultural Theory*. London, UK: Routledge.

Dourish P, Grinter R, de la Flor D, et al. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8(6): 19-30.

Dowse (n.d.) What is Dowse? Available at: <http://www.dowse.eu/faq/>.

Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.

Dyne.org Foundation (2017) Dowse Whitepaper (v 1.2). Available at: [https://files.dyne.org/dowse/dowse\\_whitepaper.pdf](https://files.dyne.org/dowse/dowse_whitepaper.pdf) (accessed 3 March 2018).

Duffield M (2010) Risk-management and the fortified aid compound: Everyday life in post-interventionary society. *Journal of Intervention and Statebuilding* 4(4): 453–474.

Duffy BE and Chan, NK (2018) “You never really know who’s looking”: Imagined surveillance across social media platforms. *New Media & Society* 21(1): 119–138.

Dunbar-Hester C (2014) *Low Power to the People*. Cambridge, MA: MIT Press.

Dunbar-Hester C (2019) *Hacking Diversity: The Politics of Inclusion in Open Technology Cultures*. Princeton, NJ: Princeton University Press.

Dunn Caveltly 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. DOI:10.1111/misr.12023

Dwyer AC (2019) *Malware ecologies: a politics of cybersecurity* [PhD thesis]. Oxford, UK: University of Oxford.

Dyer-Witheyford N and Matviyenko S (2019) *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. Minneapolis, Minnesota: University of Minnesota Press.

Enslev L, Mirsal L and Winthereik BR (2018) Anticipatory infrastructural practices: The coming of electricity in rural Kenya. *Energy Research & Social Science*(44): 130-137.

Elder M (2013) Russia raids human rights groups in crackdown on ‘foreign agents.’ *The Guardian*. 27 March. Available at: <https://www.theguardian.com/world/2013/mar/27/russia-raids-human-rights-crackdown> (accessed 1 March 2021).

Emmer P, Rivas, C, Neves, BS; Schweidler, C (2020) Technologies for Liberation: Toward Abolitionist Futures. Report, Astraea Lesbian Foundation for Justice and Research Action Design, December. Available at: [astraeafoundation.org/FundAbolitionTech](http://astraeafoundation.org/FundAbolitionTech)

Epstein B (1991) *Political protest and cultural revolution*. Berkeley: University of California Press.

Enslev L, Mirsal L and Winthereik BR (2018) Anticipatory infrastructural practices: The coming of electricity in rural Kenya. *Energy Research & Social Science* (44): 130-137.

Enterprise Risk Management Initiative (2008) Eight Principles of Risk Convergence and Implications for GRC Technology Solutions. Available at: <https://erm.ncsu.edu/library/article/GRC-technology-solutions> (accessed 3 April 2021).

Earl S, Carden F, Smutylo T (2001) *Outcome Mapping*. Ottawa: International Development Research Centre.

Electronic Frontier Foundation (year unknown). Surveillance Self Defense. Available at: <https://ssd.eff.org> (accessed 29 June 2017).

Ermoshina K and Musiani F (2018) Hiding from whom? Threat models and in-the-Making encryption technologies. *Intermedialités*. DOI: 10.7202/1058473ar.

Ettlinger N (2018) Algorithmic affordances for productive resistance. *Big Data & Society*. <https://doi.org/10.1177/2053951718771399>

Eubanks V (2011) Popular Technology. In *Digital Dead End: Fighting for Social Justice in the Information Age* (pp. 99-128). Cambridge, Massachusetts; London, England: The MIT Press.

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.

Face Dazzler (n.d.) Counter Facial Recognition. Available at: <http://facedazzler.zweis-tein.cz> (accessed 5 March 2018).

Faulkner SL and Trotter SP (2017) Data Saturation. In *The International Encyclopedia of Communication Research Methods* (eds Matthes J, Davis CS and Potter, RF). <https://doi.org/10.1002/9781118901731.iecrm0060>

Fichtner L (2018) What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review* 7(2). <https://doi.org/10.14763/2018.2.788>

FIRST (2016) FIRST announces Traffic Light Protocol (TLP) version 1.0. Available at: <https://www.first.org/newsroom/releases/20160831> (accessed 23 September 2019).

Fernandez, E, Caraj, M (2009) *The New Protection Manual for Human Rights Defenders*. Report, Protection International, Brussels.

Fernandez LA and Huey L (2009) Is Resistance Futile? Some Thoughts on Resisting Surveillance. *Surveillance & Society* 6(3): 198-202.



Ferreira A, Huynen JL, Koenig V, et al. (2014) A conceptual framework to study socio-technical security. In: Human Aspects of information security, Privacy, and Trust. Los Angeles, HAS: International Conference on Human Aspects of Information Security, Privacy, and Trust, pp 318–329. doi:10.1007/978-3-319-07620-1\_28

Flichy P (2007) *The Internet Imaginaire*. Cambridge, MA: MIT Press.

Fotopoulou A (2014) Digital and networked by default? Women's organisations and the social imaginary of networked feminism. *New Media & Society* 18(6): 989–1005.

Front Line Defenders (2011) *Workbook on Security: Practical Steps for Human Rights Defenders at Risk*. Dublin Ireland: Front Line.

Funnell, A (2015) Predictive Policing: Putting Data on the Beat. Future Tense [Radio show]. Aired on August 23, 2015 on ABC Radio National, Australia. Available at: <http://www.abc.net.au/radionational/programs/futuretense/predictive-policing3a-putting-data-on-the-beat/6702640#transcript> (accessed 13 May, 2019).

Gabrys J (2017) Citizen sensing, air pollution and fracking: From 'caring about your air' to speculative practices of evidencing harm. *The Sociological Review Mono- graphs* 65(2):172–192.

Galvez R and Gürses S (2018) The Odyssey: Modelling privacy threats in a brave new world. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 87–94. DOI: 10.1109/EuroSPW.2018.00018.

Gandy OH (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colorado: Westview.

Gandy OH (2009) *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Routledge.

Gangadharan SP, Niklas J (2018) *Between Antidiscrimination and Data: Understanding Human Rights Discourse on Automated Discrimination in Europe*. Report, London School of Economics, London, UK, May.

Gangadharan SP (2020) Digital exclusion: a politics of refusal. In: Landemore H, Reich R, and Bernholz, L (eds.) *Digital Technology and Democratic Theory*. Chicago: University of Chicago Press, preprint.

Gaw S and Felten EW (2006) Password Management Strategies for Online Accounts. In: *Proceedings of the 2nd Symposium on Usable Privacy and Security*, ser. SOUPS '06, pp. 44–55.

Gillham PF (2011) Securitizing America: Strategic incapacitation and the policing of protest since the 11 September 2001 terrorist attacks. *Sociology Compass* 5(7): 636–652.

Gilmore RW (2007) *Golden Gulag: Surplus, Crisis, and Opposition in Globalizing*. Berkeley and Los Angeles, CA: University of California Press.

Gürses S (2014) Attitudes Towards “Spiny CACTOS. Available at: <http://vous-etes-ici.net/?p=80>. (Accessed: 9 March 2015).

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

Gürses S, Overdorf R and Balsa E (2018) POTs: The revolution will not be optimized? In: *Proceedings on Privacy Enhancing Technologies Symposium*, 2018. Available at: <https://www.petsymposium.org/2018/files/hotpets/3-gurses.pdf>.

- Gutiérrez M and Milan S (2019) Playing with data and its consequences. *First Monday* 24(1). <https://doi.org/10.5210/fm.v24i1.9554> [details]
- Haché A (2014) *La Souveraineté technologique* (Vol. 1). Dossier ritimo. Available at: .
- Haché A (2018) *La Souveraineté technologique—Volume 2. Dossier ritimo*. Available at: .
- Hackblossom.org (n.d.) A DIY Guide to Feminist Cybersecurity. Available at: <https://hackblossom.org/cybersecurity/>
- Hacking I (1975) *The Emergence of Probability*. Cambridge: Cambridge University Press.
- Hamid ST (2020) Community defense: Sarah T. Hamid on abolishing carceral technologies. *Logic Magazine*, 31 August. Available at: <https://logicmag.io/care/community-defense-sarah-t-hamid-on-abolishingcarceral-technologies/>
- Hankey S and Ó'Clunaigh D (2013) Rethinking risks and security of human rights defenders in the digital age. *Journal of Human Rights Practice* 5(3): 535–547.
- Hansen L and Nissenbaum H (2009) Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53(4): 1155–1175. DOI:10.1111/j.1468-2478.2009.00572.x
- Haraway D (1988) Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies* 14(3): 575-599.
- Haraway D (2016) Staying with the trouble. In: J.W. Moore, (ed) *Anthropocene or capitalocene?* Oakland: PM Press, pp. 34–76.

Hardt M and Negri M (2004) *Multitude: War and democracy in the age of empire*. New York, The Penguin Press. Koskela, Hille. 2004. Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism. *Surveillance & Society* 2(2/3): 199- 215.

Harvey P, Reeves M and Ruppert E (2012) Anticipating Failure: Transparency Devices and their Effects. *Journal of Cultural Economy* 6(4): 1–19.

Hellegren ZI (2017) A history of crypto-discourse: encryption as a site of struggles to de-fine internet Internet freedom. *Internet Histories* 1(4): 285–311. DOI: 10.1080/24701475.2017.1387466. c

Hintz A and Brown I (2017) Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden. *International Journal of Communication* 11: 782–801.

Hintz A and Milan S (2010) Social science is police science: researching grass-roots activism. *International Journal of Communication* 4: 837–844.

Hintz A and Milan S (2013) Networked collective action and the institutionalised policy debate: Bringing cyberactivism to the policy arena? *Policy & Internet* 5(1): 7–26.

Hintz A and Milan S (2018) Through a glass, darkly: Everyday acts of authoritarianism in the liberal West. *International Journal of Communication* 12: 3939–3959.

Hoffmann AL (2019) Where fairness fails: data, algorithms, and the limits of antidiscrim- ination discourse. *Information, Communication & Society* 22(7): 900–915.

Hoffman A (2020). Terms of Inclusion: Data, Discourse, Violence. *New Media & Society*. DOI: 10.1177/1461444820958725.

Hong S (2015) Subjunctive and interpassive knowing in the surveillance society. *Media and Communication* 3(2): 63–76.

Horgan, L and Dourish, P (2018). Ambiguity, Ambivalence, and Activism: Data Organizing Inside the Institution. *Krisis: Journal for Contemporary Philosophy*, Data Activism, no. 1.

Human Rights Watch (2020) India: Counterterrorism Raids Targeting Peaceful Critics, 30 October. Available at: <https://www.hrw.org/news/2020/10/30/india-counterterrorism-raids-targeting-peaceful-critics>,(accessed 2 March 2021).

Ioannis A, Nurse, JRC, Goldsmith M, Creese S, Upton, D (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). <https://doi.org/10.1093/cybsec/tyy006>

Jasanoff S (1998) The political science of risk perception. *Reliability Engineering & System Safety* 59(1): 91–99.

Jasanoff S (2004) (ed) *States of Knowledge: The Co-production of Science and the Social Order*. New York: Routledge.

Jasanoff S Kim S-H and Sperling S (2007) *Sociotechnical Imaginaries and Science and Technology Policy: A Cross-National Comparison*. NSF Research Project, Harvard University.

John G (2011) Freedom of information and transparency in Scotland: Disclosing persons as things and vice versa. *Anthropology Today* 27(3): 22–25.

Jolivet AJ (2015) *Research Justice: Methodologies for Social Change*, Bristol: Policy Press.

Jordan S, Mitterhofer H and Jørgensen L (2018) The interdiscursive appeal of risk matrices: collective symbols, flexibility normalism and the interplay of ‘risk’ and ‘uncertainty’. *Accounting, Organizations and Society* 67:4-55.

Kaun A and Treré E (2018) Repression, resistance and lifestyle: charting (dis)connection and activism in times of accelerated capitalism. *Social Movement Studies*. <https://doi.org/10.1080/14742837.2018.1555752>.

Kazansky B (2015) Privacy, responsibility, and human rights activism. *Fibreculture Journal* (26): 189–207. DOI: 10.15307/fcj.26.195.2015.

Kazansky B (2016) Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices. Report, Tactical Tech, Berlin, Germany. Available at: <https://cdn.ttc.io/s/secresearch.tacticaltech.org/pages/pdfs/original/DigitalSecurityInContext.pdf> (accessed 21 May 2016).

Kazansky B, Torres G, van der Velden L, Wissenbach KR and Milan S (2019) Data for the social good: Toward a data-activist research agenda. In: A. Daly & M. Mann (eds.) *Good Data*. Amsterdam: Institute of Network Cultures.

Kazansky B (2021) ‘It depends on your threat model’: Understanding the anticipatory dimensions of resistance to data harms. *Big Data and Society* 8(1). <https://doi.org/10.1177/2053951720985557>

Kazansky B and Milan S (2021) “Bodies not templates”: Contesting dominant algorithmic imaginaries. *New Media & Society* 23: 363-381.

Kennedy H (2016) *Post, Mine, Repeat: Social Media Data Mining Becomes Ordinary*. New York: Springer.

Kennedy H, Poell T and van Dijck J (2015) Data and agency. *Big Data & Society* 2(2). <https://doi.org/10.1177/2053951715621569>.

Kennedy H (2018) Living with Data: Aligning Data Studies and Data Activism Through a Focus on Everyday Experiences of Datafication. *Krisis: Journal for Contemporary Philosophy*, 2018 (1): 18-30. ISSN 0168-275X

Law J (2004) *After method: Mess in social science research*. Abingdon: Routledge.

Lea J and Stenson K (2007) Security, Sovereignty, and Non-State Governance "from Below". *Canadian Journal of Law and Society* 22(2): 9-27.

Lehtiniemi T and Ruckenstein M (2018) The social imaginaries of data activism. *Big Data & Society*. DOI: 2053951718821146.

Leistert, O (2012) Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance & Society* 9(4): 441–456.

Lewis B (2013) *Facial Recognition Defense Workshop: A Make-Up Tutorial*. Available at: <https://hankblog.wordpress.com/2013/04/09/facial-recognition-defense-work-shop-a-make-up-tutorial>

Lewis T, Gangadharan SP, Saba M, Petty T (2018) *Digital defense playbook: Community power tools for reclaiming data*. Detroit: Our Data Bodies.

Li S, Trendacosta, K (2019) Shoot the messenger: How can we share secure messaging advice without causing harm? Available at: <https://platform.internetfreedomfestival.org/en/IFF2019/public/schedule/custom/1342> (accessed 25 April 2019).

- L H (2020) A sociotechnical approach to cyber security. Report, National Cyber Security Centre, UK.
- Lopez-Neira I, Patel T, Parkin S, et al. (n.d.) ‘Internet of Things’: How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly* 63: 22–26.
- Lynn JW (2010) Defending a New Domain: The Pentagon’s Cyberstrategy *Foreign Affairs* 89(5):97–108;
- Lyon D (ed) (2002) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London and New York: Routledge
- Lyon D (2014) Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1(2).  
<https://doi.org/10.1177/2053951714541861>
- Lyon D (2015) *Surveillance After Snowden*. Cambridge and Malden, MA: Polity Press.
- Lyon D (2017) Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication* 11: 824–842.
- Mackenzie A (2013) Programming subjects in the regime of anticipation: Software studies and subjectivity. *Subjectivity* 6(4): 391–405.
- MacKenzie A (2017) *Machine Learners: Archeology of a Data Practice*. MIT Press, Cambridge, MA.
- Mann S (2002) ‘‘Reflectionism’’ and ‘‘diffusionism’’. In: Levin TY, Frohne U and Weibel P (eds) *CTRL [space]: Rhetorics of surveillance from Bentham to Big Brother*. Cambridge, Mass.: MIT Press



Mansell R (2012) *Imagining the Internet: Communication, Innovation, and Governance*. Oxford: Oxford University Press.

Marcus G (1998a) Ethnography in/of the world system: The emergence of multi-sited ethnography. In (ed. Marcus G) *Ethnography through thick and thin*. Princeton, NJ: Princeton University Press, pp.79-104.

Marcus G (1998b) Imagining the whole: Ethnography's contemporary efforts to situate itself. In (ed. Marcus G) *Ethnography through thick and thin*. Princeton, NJ: Princeton University Press, pp.33-56.

Marres N (2012) *Material Participation. Technology, the Environment and Everyday Publics*. Basingstoke, UK: Palgrave Macmillan.

Mayer J (2013) MakeUp Tutorial How to Hide from Cameras (n.d.) Available at: <https://www.youtube.com/watch?v=kGGnnp43uNM> (accessed 4 March 2018).

Martin A, Van Brakel R and Bernhard D (2009) Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6(3): 213-232.

Marwick, AE, boyd, d (2014) Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16(7): 1051–1067.

Marx GT (2009) A tack in the shoe and taking off the shoe: Neutralization and counter-neutralization dynamics. *Surveillance & Society* 6(3): 294–306.

Marx GT (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

Maschmeyer L, Diebert R and Lindsay J (2020) A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics* 18(1): 1-20. DOI:10.1080/19331681.2020.1776658.

Massumi B (2015) *Ontopower: War, Powers, and the State of Perception*. Durham, NC; London: Duke University Press.

McCue C (2015) *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. 2nd edition. Oxford: Butterworth-Heinemann.

McInerney PB (2009) Technology movements and the politics of free/open source software. *Science, Technology, & Human Values* 34(2): 206–233.

Meyerson DE and Scully M (1995) Tempered radicalism and the politics of ambivalence and change. *Organization Science* 6: 585–600.

Milan S (2013) *Social Movements and Their Technologies: Wiring Social Change*. Basingstoke, UK: Palgrave Macmillan.

Milan S (2017) Data activism as the new frontier of media activism. In P. Victor, & G. Yang (eds.) *Media Activism in the Digital Age* (pp. 151-163). (Shaping Inquiry in Culture, Communication and Media Studies). London: Routledge.

Milan S (2018) Political agency, digital traces and bottom-up data practices. *International Journal of Communication* 12: 507–527.

Milan S and ten Oever N (2017) Coding and encoding rights in internet infrastructure. *Internet Policy Review* 6(1). DOI: 10.14763/2017.1.442.

Milan S and Van der Velden L (2016) The alternative epistemologies of data activism. *Digital Culture & Society* 2(2): 57–74.

Millar K, Shires J and Tropina T (2021) Gender Approaches to Cybersecurity: Design, Defence and Response. Report, United Nations

Institute for Disarmament Research, Geneva, Switzerland. <https://doi.org/10.37559/GEN/21/01>

Miller A (2019) Shadows of war, traces of policing: The weaponization of space and the sensible in preemptionpreemption. In: Benjamin R (ed) *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham: Duke University Press, pp. 85–106.

Miller L (2020) LAPD will end controversial program that aimed to predict where crimes would occur *Los Angeles Times*, 21 April.

Milner Y (2019) December 31. Abolition means the creation of something new. Available at: <https://medium.com/@YESHICAN/abolition-means-the-creation-of-something-new-72fc67c8f493> (accessed 1 March 2021).

Minocher X and Randall C (2020) Predictable policing: New technology, old bias, and future resistance in big data surveillance. *Convergence: the international journal of research into new media technologies*. 26 (5-6): 1108-1124.

Mols AE and Pridmore JH (2019) When Citizens Are “Actually Doing Police Work”: The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands. *Surveillance & Society* 17 (3/4): 272-287. DOI: 10.24908/ss.v17i3/4.8664

Monahan T (2006) Counter-surveillance as political intervention? *Social Semiotics* 16(4): 515–534.

Monahan T (2010) *Surveillance in the Time of Insecurity*. Rutgers University Press.

Monahan T (2015) The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies* 12(2): 159– 178.

Monsees L (2020) Cryptoparties: empowerment in internetInternet security? *Internet Policy Review* 9(4). <https://doi.org/10.14763/2020.4.1508>

Morgus R, Skierka I and Hohmann M (2015) National CSIRTs and Their Role in Computer Security Incident Response. Report, GPPI, Berlin, Germany. Available at: <https://www.gppi.net/2015/11/19/national-csirt-and-their-role-in-computer-security-incident-response>

Mouffe C (2013) *Agonistics: Thinking the World Politically*. London: Verso

Mueller M, Schmidt A and Kuerbis B (2013) Internet Security and Networked Governance in International Relations. *International Studies Review*. 15(1):86-104.

Mujinga M, Eloff M and Kroeze J (2017) A socio-technical approach to information security. In: Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA, 10-12 August 2017 (pp. 1-10).

Murphy H and Bellamy M (2009) The Dazzling Zoologist: John Graham Kerr and the Early Development of Ship Camouflage. *The Northern Mariner/le marin du nord* XIX (2): 171–192.

Musiani F (2016) Alternative Technologies as Alternative Institutions: The Case of the Domain Name System. In: Musiani F, Cogburn DL, DeNardis L, et al. (eds) *The Turn to Infrastructure in Internet Governance*. Basingstoke, UK: Palgrave Macmillan, pp. 73–86.

Musiani F and Ermoshina K (2017) What is a good secure messaging tool? The EFF secure messaging scorecard and the shaping of digital (usable) security. *Westminster Papers in Communication and Culture* 12(3): 51–71.

Nissenbaum H (2005) Where computer security meets national security. *Ethics and Information Technology*, 7(2), 61–73. DOI: 10.1007/s10676-005-4582-3

- Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
- Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York, NY: NYU Press.
- Notley T and Hankey S (2013) Human Rights Defenders and the Right to Digital Privacy and Security in: *Human Rights and Information Communication Technologies: Trends and Consequences of use*. Hershey, PA: IGI Global.
- O’Grady N (2016) A politics of redeployment: Malleable technologies and the localisation of anticipatory calculation. In: Louise, A, Piotukh, V (eds) *Algorithmic Life: Calculative Devices in the Age of Big Data*. Abingdon: Routledge, pp. 72–86.
- O’Malley P (2010) Resilient subjects: uncertainty, warfare and liberalism. *Economy and Society* 39 (4): 488-509.
- Parks L (2015) ‘Stuff you can kick’: Toward a theory of media infrastructure. In: Svens- son P and Goldberg DT (eds) *Between Humanities and the Digital*. Cambridge, MA and London, England: MIT Press, pp. 355–373.
- Parrika, J (2007) *Digital Contagions – A Media Archaeology of Computer Viruses*. New York: Peter Lang.
- Petty T, Saba M, Lewis T, Gangadharan SP and Eubanks V (2018) *Our Data Bodies: Reclaiming Our Data*. Detroit, MI: Our Data Bodies Project.
- Pickett B (1996). *Foucault and the Politics of Resistance*. *Polity* 28(4), 445-466. DOI: 10.2307/3235341
- Pink S, Lanzeni D, Horst H (2018) Data anxieties: Finding trust in everyday digital mess. *Big Data & Society* 5(1). DOI: 2053951718756685.

Polletta F (1999) 'Free spaces' in collective action. *Theory and Society* 28:1–38.

Power M (2007) *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.

Power M (2009) The risk management of nothing. *Accounting, Organizations and Society*, 34(6/7): 849–855.  
DOI:10.1016/j.aos.2009.06.001.

Price R (2003) Transnational civil society and advocacy in world politics. *World Politics* 55(4): 579–606.

Puente M (2019) LAPD ends another data-driven crime program touted to target violent offenders. *Los Angeles Times* 12 April.

Purdon L (2017) Cybersecurity should protect us – not control us. *Open Democracy*, 13 March 13. Available at:  
<https://www.opendemocracy.net/en/digital liberties/cybersecurity-should-protect-us-not-control-us/>

Raghavan M, Barocas S, Kleinberg J (2020) Mitigating bias in algorithmic hiring: evaluating claims and practices. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. Pp. 469–481.

Radloff J (2013) Digital Security as Feminist Practice. *Feminist Africa*. 18: 145–55.

Radloff J (2018) Embedding digital security in feminist movement building. *Open Global Rights*. Available at:  
<https://www.openglobalrights.org/embedding-digital-security-in-feminist-movement-building/> (accessed 4 June 2020).

Reconfigure Network (2021) re: CONFIGURE. Feminist Action Research in Cybersecurity. Report, Oxford University, Oxford, UK. Available at:

<https://www.oii.ox.ac.uk/wp-content/uploads/2021/01/Reconfigure-Report.pdf>.

Reeves J (2012) If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility. *Surveillance & Society* 10(3/4): 235-248.

Rocha J (2021) A catalog of formats for digital discomfort... and other ways to resist totalitarian zoomification (eds) Gürses S and Rocha S (2021) available at:  
<http://titipi.org/projects/discomfort/CatalogOFFDigitalDiscomfort.pdf>

Rogers M and Eden G (2017) The Snowden disclosures, technical standards and the making of surveillance infrastructures. *International Journal of Communication* 11: 802–823.

Ruppert E (2018) Different Data Futures: An Experiment in Citizen Data. In: *DGINS* conference, Bucharest, 2018.

Ruppert E, Isin E and Bigo D (2017) Data Politics. *Big Data & Society* (July-December): 1–7. DOI: 10.1177/2053951717717749.

Rutkowska J (2011) The Invisible Things Lab’s blog: Partitioning my digital life into security domains. In: *The Invisible Things Lab’s blog*. Available at: <https://theinvisiblethings.blogspot.com/2011/03/partitioning-my-digital-life-into.html> (accessed 3 February 2018).

Rutkowska J and Wojtczuk R (2010) Qubes OS Architecture. Version 0.3. Invisible Things Lab.

Ryan-Mosley T and Strong J (2020) The activist dismantling racist police algorithms. MIT Technology Review.

Sassoon AS (2000) *Gramsci and Contemporary Politics: Beyond Pessimism of the Intellect*. London: Routledge.

Satchell C and Dourish P (2009) Beyond the user: use and non-use in HCI. *Human-Computer Interaction* 366: 9–16.

Schinkel W (2017) *Imagined Societies. A Critique of Immigrant Integration in Western Europe*. Cambridge: Cambridge University Press.

Schweitzer D (2003) How to toughen the weakest link in the security chain. *Computer world*, 8 January. Available at: <https://www.computerworld.com/article/2580125/how-to-toughen-the-weakest-link-in-the-security-chain.html> (accessed 21 May, 2021).

Scoones I and Stirling A (eds) (2020) *The politics of uncertainty: Challenges of transformation*. Routledge: Abingdon.

Shamas N (2017) Creating a pedagogy of empowerment. Available at: [https://internetinternetfreedomfestival.org/wiki/index.php/Creating\\_a\\_pedagogy\\_of\\_empowerment](https://internetinternetfreedomfestival.org/wiki/index.php/Creating_a_pedagogy_of_empowerment) (accessed 25 April 2019).

Shelton M (2018) Locking down signal: A guide for journalists. Available at: <https://medium.com/@mshelton/locking-down-signal-d71678f653d3> (accessed 23 December 2020).

Shostack A (2014) *Threat Modeling: Designing for Security*. Indianapolis: Wiley.

Slayton R (2015) Measuring risk: computer security metrics, automation, and learning. *IEEE Annals of the History of Computing* 37 (2): 32-45.

Slayton R and Clarke B (2020) Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005. *Technology and Culture* 61(1): 173-206.

Slupska, J (2019) Safe at Home: Towards a Feminist Critique of Cybersecurity. *St. Anthony's International Review* 15: 83-100. Whose



Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace.

Sheehy, B (2019) Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics and Information Technology* 21(1): 49–58.  
<https://doi.org/10.1007/s10676-018-9489-x>

Shove E, Pantzar M and Watson M (2012) *The Dynamics of Social Practice: Everyday Life and How It Changes*. London: Sage.

Smith AM (2012) *Laclau and Mouffe. The Radical Democratic Imaginary*. London: Routledge.

Smith GJD (2018) Data doxa: The affective consequences of data practices. *Big Data and Society* 5(1): 1–15.

Snow DA, Worden S and Benford R (1997) Frame Alignment Processes, Micromobilization, and Movement Participation. In: McAdam D and Snow DA (eds) *Social Movements. Readings on Their Emergence, Mobilization, and Dynamics*. Los Angeles: Roxbury, pp. 235–251.

Stachowitsch S and Sachseder J (2019) The gendered and racialized politics of risk analysis. The case of Frontex. *Critical Studies on Security* 7(20):107–123.

Star SL (1999) The Ethnography of Infrastructure. *American Behavioral Scientist* 43(3): 377–391.

Star SL and Bowker GC (2007) Enacting silence: Residual categories as a challenge for ethics, information systems, and communication. *Ethics and Information Technology* 9(4): 273–280.

Star SL and Griesemer, J (1989) Institutional ecology, ‘translations,’ and boundary objects: Amateurs and professionals in Berkeley’s museum of vertebrate zoology. *Social Studies of Science* 19: 387–420.

Star SL and Ruhleder K (1996) Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research*, 7(1): 111-134.

Stark L and Hoey J (2021) The ethics of emotion in AI systems. In FAccT'21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, March 2021 (pp. 782–793). New York (NY): Association for Computing Machinery (ACM).

Stop LAPD Spying Coalition (2015) Architecture of Surveillance – Explained. Available at: <https://stoplapdspying.org/policing-strategies-and-tactics/> (accessed 25 June 2020).

Stop LAPD Spying Coalition (2018) Before the Bullet Hits the Body — Dismantling Predictive Policing in Los Angeles. Report, Stop LAPD Spying Coalition, Los Angeles, CA. Available at: <https://stoplapdspying.org/before-the-bullet-hits-the-body-dismantling-predictive-policing-in-los-angeles/> (accessed: 4 October 2019).

Stop LAPD Spying Coalition (2019a) Stop LAPD Spying Coalition Wins Groundbreaking Public Records Lawsuit. Available at: <https://stoplapdspying.medium.com/stop-lapd-spying-coalition-wins-groundbreaking-public-records-lawsuit-32c3101d4575> (accessed: 6 April 2021).

Stop LAPD Spying Coalition (2019 b) The People’s Response to OIG Audit of Data-Driven Policing. Available at: <https://stoplapdspying.org/the-peoples-response-to-oig-audit-of-data-driven-policing> (accessed: 25 June 2020).

Stop LAPD Spying Coalition and Free Radicals (2020) The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms. Available at: <https://medium.com/@stoplapdspying/the-algorithmic->

[ecology-an-abolitionist-tool-for-organizing-against-algorithms-14fcbd0e64d0](#) (accessed 3 April 2021).

Strathern M (2000) The tyranny of transparency. *British Educational Research Journal* 26(3): 309–321.

Suchman L (2002) Located accountabilities in technology production. *Scandinavian Journal of Information Systems* (14)2: 91-105. Available at:

Suchman L (2015) Situational awareness: Deadly bioconvergence at the boundaries of bodies and machines. *MediaTropes* 5(1): 1–24

Suchman L (2020) Algorithmic Warfare and the Reinvention of Accuracy In: *Critical Studies on Security* 8(2): 175-187. DOI: 10.1080/21624887.2020.1760587

Suchman L, Follis K and Weber J (2017) Tracking and Targeting: Sociotechnologies of (In)security. *Science, Technology, and Human Values* 42(6): 983-1002.

Swain V (2013) Disruption Policing: Surveillance and the Right to Protest. *Open Democracy*, 8 August. Available at: <https://www.opendemocracy.net/en/opensecurity/disruption-policing-surveillance-and-right-to-protest> (accessed 15 October 2020).

Tactical Tech Collective (2015) *Zen and the Art of Making Technology Work for You*. Available at: [https://gendersec.tacticaltech.org/wiki/index.php/Complete\\_manual](https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual) (accessed 20 September 2018).

Tactical Technology Collective (2016) *Holistic Security Manual*. Available at: <https://holistic-security.tacticaltech.org/> (accessed 20 September 2018).

Tactical Technology Collective (n.d.) Gendersec training curricula. Available at: <https://xyz.informationactivism.org/en/> (accessed 20 September 2018).

Tactical Technology Collective (XYZ) (n.d.) Available at: <https://xyz.informationactivism.org/en/> (accessed 22 February 2021).

Tanczer L, Lopez-Neira I, Parkin S et al. (2018). Gender and IoT Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse. Report, STEaPP, PETRAS IoT Hub, London.

Tanczer L, Deibert RJ, Bigo D, Franklin MI, Melgaço L, Lyon D, Kazansky B and Milan S (2020) Online Surveillance, Censorship, and Encryption in Academia. *International Studies Perspectives* 21(1): 1-36.

Tarnoff B (2020) The Making of the Tech Worker Movement. *Logic Magazine*, 4 May. Available at: <https://logicmag.io/the-making-of-the-tech-worker-movement/full-text/>

Taylor L, Floridi L and van der Sloot B (eds) (2017) *Group Privacy: New Challenges of Data Technologies*, 1st ed. New York, NY: Springer.

The Citizen Lab (2014) Extended analysis: civil society perspectives and responses, from Communities @ Risk: Targeted Digital Threats Against Civil Society. Report, University of Toronto, Toronto. Available at: <https://targetedthreats.net/media/2.3%20Extended%20Analysis-CivilSociety.pdf>

The Engine Room (2013) Training digital security trainers: A preliminary review of methods, needs, and challenges. Report, The Engine Room for Internews, Washington DC, November.

The Engine Room (2018) *Ties That Bind: Organisational Security for Civil Society*. Report, The Engine Room for the Ford Foundation, New York, March.

Thomas DR (2003) A general inductive approach for qualitative data analysis. School of Population Health, University of Auckland, New Zealand.

Trottier D (2017) Digital Vigilantism as Weaponisation of Visibility. *Philosophy of Technology* 30: 55–72 <https://doi.org/10.1007/s13347-016-0216-4>

Tsing A (2015) *The Mushroom at the End of the World: on the Possibility of Life in Capitalist Ruins*. Princeton NJ: Princeton University Press.

Tufekci Z (2019) The Hong Kong Protesters Aren't Driven by Hope. *The Atlantic*, 12 November. Available at: <https://www.theatlantic.com/international/archive/2019/11/escalating-violence-hong-kong-protests/601804/>

Ullrich P and Knopp P (2018) Protesters' reactions to video surveillance of demonstrations: Counter-Moves, security cultures, and the spiral of surveillance and counter-surveillance. *Surveillance & Society* 16(2): 183–202.

Ulfstjerne MA (2020) BoB and the Blockchain: Anticipatory infrastructures of the cashless society. In *Who's cashing in? Contemporary perspectives on new monies and global cashlessness* (pp. 89-104). Berghahn Books.

Van Brakel R (2016) Preemptive big data surveillance and its (dis)empowering consequences: The case of predictive policing. In: van der Sloot B, Broeders D, Schrijvers E (eds) *Exploring the Boundaries of Big Data*. Amsterdam: Amsterdam University Press, pp. 117–141.

van der Velden L (2018) *Surveillance as public matter. Revisiting sousveillance through devices and leaks* (PhD dissertation). University of Amsterdam, The Netherlands.

van Dijck J (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208. <https://doi.org/10.24908/ss.v12i2.4776>

Van Dijck J, Poell T and De Waal M (2018) *The platform society. Public values in a connective world*. Oxford: Oxford University Press.

Veale M and Brown I (2020) Cybersecurity. *Internet Policy Review* 9(4) <https://doi.org/10.14763/2020.4.1533>

Verran H (1998) Re-imagining land ownership in Australia. *Postcolonial Studies* 1(2): 237–254.

Vertesi J (2014) Seamful Spaces Heterogeneous Infrastructures in Interaction. *Science, Technology, & Human Values* 39 (2): 264–84.

Wang, J (2018) *Carceral Capitalism*. Cambridge: The MIT Press.

Wash R and Rader E (2011) Influencing mental models of security: a research agenda. In Proceedings of the 2011 New Security Paradigms Workshop (NSPW '11). Association for Computing Machinery, New York, NY, USA, 57–66.

West SM (2017) Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk. In: *7th Workshop on Free and Open Communications on the Internet 17*, Vancouver, BC, 2017. USENIX Association.

Whitten A and Tygar JD (1999) Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium, pp. 169–183, Washington, DC, August 1999

Wood MA and Thompson C (2018) Crowdsourced Countersurveillance: A Countersurveillant Assemblage? *Surveillance & Society* 16(1): 20-38.

Woolgar S (1990) Configuring the user – The case of usability trials. In: Law, J (ed) *A Sociology of Monsters – Essays on Power, Technology and Domination*. London: Routledge, pp. 58–99.

Wyatt S (2003) Non-users also matter: The construction of users and non-users of the Internet In: Oudshoorn N and Pinch T (eds). *How users matter: The co-construction of users and technology*. Cambridge, Mass.: MIT Press, pp. 67–79.

Wyatt S (2004) Danger! Metaphors at work in economics, geophysiology, and the Internet. *Science, Technology & Human Values* 29(2): 242–261.

Zajko M (2018) Security against Surveillance: IT Security as Resistance to Pervasive Surveillance. *Surveillance&Society*16(1): 39-52.





