Breaking Barriers, Talking Trust

Juliet Grotrian

Humans have always broken barriers. Barriers to progress, to education; breaking records, the glass ceiling; surpassing the sound barrier, the Kármán line, technological boundaries. In doing so, we have broken barriers we did not wish to break, including the barrier between our information and the vast surveillance networks of the modern age; and, in our disregard for the consequences of progress, our control-based privacy definitions have not caught up with the omniscient power of surveillance technologies. It is imperative that we formulate a new framework of privacy that can continue to evolve along with surveillance, to better balance our individual rights with public safety; one based on a very human concept: trust.

There are many individual rights implicated in surveillance; however, the right to privacy, enshrined in the Universal Declaration of Human Rights, is often the most discussed in this context (Richards; Wheatley; United Nations).

Traditional notions of privacy prize our ability to control the dissemination and access of our personal information (Richards and Hartzog 'Trust Gap'; Bennett 486; Lazaro and Le Métayer; Bazarova and Massur; Waldman 15). However, we simply do not have this control anymore. Our personal information has been 'greased' by computerisation; already in 2014, 91% of adults in a Pew Research survey felt they had 'lost control over how personal information is collected and used by companies' (Moor 27; Madden). Surveillance technologies only exacerbate this lack of control due to their ubiquitous nature; and, as they seem destined to only increase in pervasiveness and usage, we will never regain this control (Walker).

Similar notions focusing subtly on control, such as 'the right to be left alone'– freedom from intrusion into the private life – have also passed their use-by date; the home, 'traditionally seen as the bastion of privacy…a barrier between surveillance and the details of private life', has been evaporated due to the cloud storage and transmission of personal information where it is vulnerable to digital surveillance (Newell et al. 13; Brandeis and Warren).

This power imbalance between surveilled and surveillant is ingrained, to some extent, into modern surveillance.[1] It has been lamented worldwide as the 'death of privacy'; however, this does not have to be the case (Froomkin 1461; Wacks; Solove 9; Richards and Hartzog 'Trust Gap').

If *we* do not have control over our personal information, and our privacy concerns as they relate to surveillance are primarily based on our lack of control, the next-best option to redefine privacy would emphasise trust, or 'control by proxy' (Nissenbaum; Liu et al. 552, 554; Thompson 7-8; Waldman 67; Richards and Hartzog 'Trust Gap'). Trust is a central component of all social relationships and facilitates the sharing of information; therefore, if we have reason to trust those who *do* have control over our personal information to act in our best interests as a proxy, we would be more accepting of their control over our information and thus feel our privacy is breached to a lesser degree (Waldman 62, 67; Richards and Hartzog 'Trust Gap', Cayford 15, Thompson 10, 18; Liu et al. 551-556).[2] But, at present, we do not trust the surveillants; our information continues to flow, unbidden, into surveillance systems that conjure up Orwellian dystopias or Cold War spies in the minds of many. To ensure minimum infringement on individual rights, the surveillants must *gain* our trust. This ensures the onus is not on powerless individuals to battle against surveillance; the responsibility to build trust must be held by those with the most control over our information (Richards and Hartzog 'Trust Gap').

---

[1] A 'surveillant', in this essay, is a person, institution, or machine who collects, stores, accesses, and/or utilises surveillance-collected data.

[2] We could also consider, here, the concept of intellectual privacy, which, elsewhere, might be referred to as 'civil liberties' (Richards). A concern about surveillance is its 'chilling effect' on intellectual privacy; it can cause self-censorship and modification of behaviour, discouraging activities important to democracy out of fear of repression (Murray et al. 402-403, 405; Penney 1455). Fortunately, a trust-based approach to privacy can also lessen this chilling effect, as uncertainty around surveillance purposes and usage, causing mistrust of others and of institutions, is a key contributor to the chilling effect's prevalence; if we trust the surveillants not to repress essential democratic activity, and to be honest about data practices and consequences for those posing public safety threats, we would be less inclined to self-censor (Perlin; Murray et al. 406; Penney 1488, 1513). Further, the Hawthorne effect – elsewhere called the 'deterrent effect' - happens where surveillance or observation promotes positive behaviour, such as productivity, rather than chilling the exercise of civil liberties; the Hawthorne effect is one of the main reasons why surveillance is used, in that it promotes socially positive behaviour and so deters crime and public safety-threatening behaviours (Spencer & Mahtani; Yang et al..; Priks 289; McCullen; Gómez et al. 569). In some ways, the chilling effect could be thought of as the Hawthorne effect gone too far (Ucchwas). If we consider that fact, and that researchers often use rapport with participants to diminish the Hawthorne effect where it is unhelpful for a study, it follows that trust can diminish the chilling effect to some extent, ensuring the deterrent nature of surveillance goes only so far as to promote safe behaviour rather than chill dissent (Oswald et al. 59-63).

The question now is: how should this trust be gained? Fortunately, there are methods through which tech developers, lawmakers, and other surveillants can begin to implement a trustbased privacy framework. For instance, continuous honesty and involvement of the public in surveillance implementation can garner public trust (Simply Privacy, Richards & Hartzog 'Seriously' 462-463). An example of this can be seen in Kakogawa, Japan, 'one of the most surveilled cities in the nation', where there is 'exceptionally high' acceptance of CCTV cameras due to 'collective trust' between citizens and city (Yang et al.). Public meetings and discussions were held to involve citizens in surveillance implementation, consulting them about privacy and camera locations (Yang et al.). The city 'reassures residents about the transparency process of decision-making and the responsible utilisation of data' (Yang et al.). This successful trust-based implementation of surveillance, with some 95% of Kakogawa residents trusting their privacy will be protected, demonstrates that a similar trust-based approach – with lawmakers and tech developers collaborating to work with the public and develop mandatory trust-based, transparency-promoting implementation procedures such as those in Kakogawa – could balance public safety and individual rights (Yang et al.; Wheatley).

Public trust could be further built by increasing surveillance utility and equity – Liu et al.'s 'perceived benefit[s] of disclosure' – and ensuring technologies 'limit…the uses of our shared information in accordance with our social expectations' by only capturing and accessing data to the extent necessary (Liu et al. 553; Waldman 67; Moor). Currently, surveillance technologies are not easy to trust, due to their narrow utility, biased algorithms, inaccuracies, and ineffective and/or targeted placement meaning they are both inequitable and impractical, considering that they also create privacy concerns (Liu et al. 553; Waldman 67; Leslie 5; Slobogin and Brayne; Walker; Hill; Lang et al 266.; Alexandrie 213-214; Cayford and Pieters 90; Priks 289; Welsh and Farrington 8-9; Leslie 17; Slobogin and Brayne; Walker; Hill; Löfstrand 1).[3] Tech developers could remedy these issues by increasing technology accuracy and removing biases to gain public trust, while simultaneously improving public safety. Additionally, by working with lawmakers to mandate restrictions on surveillance technology use only where it captures useful data, creating access restrictions for that data, and encrypting personal information, they could prove a commitment to a secure, trusting relationship where no more data is collected than needed (Wheatley).

Of course, the trust-based model relies on the assumption that the surveillants *are* trustworthy; to mitigate this limitation, laws should be created to hold surveillants accountable for data breaches and other untrustworthy behaviour to incentivise the adoption of the trust framework (Richards and Hartzog 'Trust Gap').

We have lost control over our personal information. Under current law, our privacy is threatened by surveillance. However, by redefining privacy in terms of trust, and creating a trust-based privacy framework, in which lawmakers and tech developers are engaged to develop public trust in surveillance through honesty, public involvement, and technological and implementational improvements, we can protect our privacy and move towards a balance between individual rights and public safety in the age of surveillance.

[3] Technologies such as aerial surveillance and automatic licence plate readers are compromised by a lack of evidence for effectiveness or accuracy; AI-powered facial recognition technologies such as Microsoft's FaceDetect have been shown to have racially biased algorithms (Leslie 17; Slobogin and Brayne; Walker; Hill). Even the ubiquitous CCTV has issues; despite some studies showing an up to 30% crime reduction rate, others have found it may only be significantly effective in particular environments and for specific types of crime, and may displace crime to non-surveilled areas (Lang et al. 266; Alexandrie 213-214; Priks 289; Cayford and Pieters 90; Welsh and Farrington 8-9). Social equity is also a concern; in Sweden, for instance, 'CCTV surveillance disproportionately targets disadvantaged areas' (Löfstrand 1).

Works Cited

Alexandrie, Gustav. "Surveillance cameras and crime: a review of randomized and natural experiments." *Journal of Scandinavian Studies in Criminology and Crime Prevention*, vol. 18, no. 2, 3 Jul. 2017: 210-222. *Scandinavian University Press*, https://doi.org/10.1080/14043858.2017.1387410.

Bazarova, Natalya N., and Philipp K. Massur. "Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology." *Current Opinion in Psychology*, vol. 36, December 2020: 118- 123. *ScienceDirect*, https://doi.org/10.1016/j.copsyc.2020.05.004 .

Bennett, Colin J. "In Defence of Privacy: The concept and the regime." *Surveillance & Society*, vol. 8, no. 4, 24 Mar. 2011: 485-496. *Surveillance & Society*, https://doi.org/10.24908/ss.v8i4.4184. PDF download.

Cayford, Michelle, and Wolter Pieters. "The effectiveness of surveillance technology: What intelligence officials are saying." *The Information Society*, vol. 35, no. 2, 08 Mar. 2018: 88- 103. *Taylor & Francis Online*, https://doi.org/10.1080/01972243.2017.1414721.

Cayford, Michelle, Wolter Pieters, and P.H.A.J.M van Gelder. "Wanting it all – public perceptions of the effectiveness, cost, and privacy of surveillance technology." *Journal of Information, Communication and Ethics in Society*, vol. 18, no. 1, 2020: 10-27. *ResearchGate*, www.researchgate.net/profile/MichelleCayford/publication/335488130_Wanting_it_all_-_public_perceptions_of_the_effectiveness_cost_and_privacy_of_surveillance_technology/lin ks/5d7f8c54458515fca16cc299/Wanting-it-all-public-perceptions-of-the-effectiveness-costand- privacy-of-surveillance-technology.pdf .

Froomkin, A. M. "The Death of Privacy?" *Stanford Law Review*, vol. 52, no. 5, May 2000: 1461-1543. *JSTOR*, https://doi.org/10.2307/1229519.

Gómez, Santiago, Daniel Mejía, and Santiago Tobón. "The deterrent effect of surveillance cameras on crime". *Journal of Policy Analysis and Management*, vol. 40, no. 2, 05 Jan. 2021:553-571. *Wiley Online Library*, https://doi.org/10.1002/pam.22280.

Hill, Rebecca. "London cops urged to scrap use of 'biased' facial recognition at Notting Hill Carnival". *The Register*. 17 Aug. 2017, www.theregister.com/2017/08/17/concerns_over_facial_recognition_at_notting_hill_carnival/.

Lang, Kay, Justin Sanford, and Christopher Murtagh. "Assessing CCTV in Preventing and Reducing Property Crime." *Justice Evaluation Journal*, vol. 8, no.2, 08 Mar. 2025: 263-283. *Taylor & Francis Online*, https://doi.org/10.1080/24751979.2025.2474706.

Lazaro, Christophe, and Daniel Le Métayer. "Control over Personal Data: True Remedy or Fairy Tale?." *SCRIPTed*, vol. 12, no. 1, June 2015. *SCRIPTed*, https://doi.org/10.2966/scrip.120115.3.

Leslie, D. "Understanding bias in facial recognition technologies: an explainer." *The Alan Turing Institute*, 2020. https://doi.org/10.5281/zenodo.4050457. PDF download.

Liu, Jing, Marko M. Skoric, and Chen Li. "Disentangling the relation among trust, efficacy and privacy management: A moderated mediation analysis of public support for government surveillance during the COVID-19 pandemic." *Behaviour & Information Technology*, vol. 43, no. 3, 2024: 551-570. *Taylor & Francis Online*, https://doi.org/10.1080/0144929X.2023.2178830.

Löfstrand, Cecilia H. "From privacy to protection: The reframing of integrity in Sweden's camera surveillance politics." *Nordic Journal of Criminology*, vol. 27, no. 1, 10 Jun. 2025: 1-17. *Scandinavian University Press*, https://doi.org/10.18261/njc.27.1.2.

Madden, Mary. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Research Center*. 12 Nov. 2014, www.pewresearch.org/internet/2014/11/12/public-privacyperceptions/.

McCullen, Aidan. "Panopticon States and the Hawthorne Effect – Eye Am Watching". *The Innovation Show*, 7 Dec. 2022, theinnovationshow.io/panopticon-states-and-the-hawthorneeffect-eye-am-watching/.

Moor, James H. "Towards a theory of privacy in the information age." *ACM SIGCAS Computers and Society*, vol. 27, no. 3, 01 Sept. 1997, 27-32. *ACM Digital Library*, https://doi.org/10.1145/270858.270866. PDF download.

Murray, Darag, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, and Amy Stevens. "The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe". *Journal of Human Rights Practice*, vol. 16, no. 1, February 2024: 397-412. *Oxford Academic*, https://doi.org/10.1093/jhuman/huad020.

Newell, Bryce C., Tjerk Timan, and Bert-Jaap Koops. *Surveillance, Privacy, and Public Space*. Routledge, 2018. api.pageplace.de/preview/DT0400.9781351780193_A37413164/preview-9781351780193_A37413164.pdf. Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, November 2009. www.sup.org/books/law/privacy-context.

Oswald, David, Fred Sherratt, and Simon Smith. "Handling the Hawthorne effect: The challenges surrounding a participant observer". *Review of Social Studies*, vol. 1, no. 1, 2015: 53-73. *ROSS Journal*, www.rossjournal.co.uk/wp-content/uploads/2016/12/RoSS-Vol1-No1-Oswald-et-al-53-73.pdf.

Penney, Jonathon W. "Understanding Chilling Effects". *Minnesota Law Reveiw*, vol. 106, 2022: 1451-1530 minnesotalawreview.org/wp-content/uploads/2022/04/6-Penney_Web.pdf.

Perlin, Paulina. "ACLU v. NSA: How Greater Transparency Can Reduce the Chilling Effects of Mass Surveillance". *Yale Law School*, 6 Dec. 2017, law.yale.edu/mfia/case-disclosed/acluv-nsa-how-greater-transparency-can-reduce-chilling-effects-mass-surveillance.

Priks, Mikael. "The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway." *The Economic Journal*, vol. 124, November 2015: 289-305.https://doi.org/10.1111/ecoj.12327.

Richards, Neil and Woodrow Hartzog. "Privacy's Trust Gap: A Review." *The Yale Law Journal*, vol. 126, no. 1, 28 Feb. 2017, yalelawjournal.org/review/privacys-trust-gap-areview.

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review*, vol. 126, no. 7, May 2013, harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/.

Richards, Neil, and Woodrow Hartzog. "Taking Trust Seriously in Privacy Law". *Stanford Technology Law Review*, vol. 19, 2016: 431-472. *Stanford Law School*, law.stanford.edu/wpcontent/uploads/2017/11/Taking-Trust-Seriously-in-Privacy-Law.pdf.

Slobogin, Christopher, and Sarah Brayne. "Surveillance Technologies and Constitutional Law." *Annual Review of Criminology*, vol. 6, January 2023. *Annual Reviews*, https://doi.org/10.1146/annurev-criminol-030421-035102.

Solove, Daniel J. *Understanding Privacy*. Harvard University Press, 2008. books.google.co.nz/books?id=eSrnEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false.

Spencer, EA, and Mahtani K. "Hawthorne effect". *Catalogue of Bias*, 2017, catalogofbias.org/biases/hawthorne-effect/.

Thompson, Nik, Tanya McGill, Anna Bunn, and Rukshan Alexander. "Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance". *Journal of the Association for Information Science and Technology*, vol. 71, no. 9, 2020: 1129-1142. *Vavuniya University*, drr.vau.ac.lk/bitstream/handle/123456789/530/Cultural%20Factors%20and%20the%20Role%20of%20Privacy%20Concerns%20in%20Acceptance%20of%20Government%20Surveillance%20-%20Rukshan%20Alexander.pdf?sequence=1.

"Trusted transparency - Connecting the dots between what you say and what you do." *Simply Privacy*. Simply Privacy. simplyprivacy.co.nz/trusted-transparency-connecting-the-dotsbetween-what-you-say-and-what-you-do/. Accessed 21st Jan. 2026.

Ucchwas, Elman. "Negative Effects of Employee Monitoring & Smart Ways to Avoid Them". *Apploye*, 30 Dec. 2025, apploye.com/blog/employee-monitoring-negative-effects/.

United Nations, General Assembly. Universal Declaration of Human Rights. Resolution 217 A, 10 Dec. 1948. *United Nations*, www.un.org/en/about-us/universal-declaration-of-humanright. PDF download.

Wacks, Raymond. Privacy: *A Very Short Introduction (2nd edn)*. "The death of privacy?" Oxford University Press, March 2015. https://doi.org/10.1093/actrade/9780198725947.003.0006.

Waldman, Ari E. *Privacy as Trust: Information Privacy for an Information Age*. Cambridge University Press, 7 Mar. 2018. books.google.co.nz/books?id=v81MDwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

Walker, Isabelle. "The evolution of surveillance technology." *International Bar Association*. 23 Jul. 2025, www.ibanet.org/The-evolution-of-surveillance-technology.

Warren, Samuel D., and Louis D. Brandeis. "The right to privacy." *Harvard Law Review*, vol.4, no. 5, 15 Dec. 1890, groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Welsh, Brandon C., and David P. Farrington. *Making Public Places Safer: Surveillance and Crime Prevention*. Oxford University Press, 2009.books.google.co.nz/books?id=lALLlGzyD24C&printsec=frontcover#v=onepage&q&f=false.

Wheatley, Mary C. "Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age." *Premier Journal of Data Science, 2024. Premier Science*, https://doi.org/10.70389/PJDS.100001.