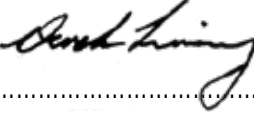




Postgraduate Dissertation coversheet & feedback form:

<i>For completion by student:</i>		
Student Name Derek Linney		
Student University Email: 2218467@student.uwtsd.ac.uk		
Module code: HPPH7014	Student ID number: 2218467	Educational support needs: No
Dissertation title: The dichotomy between private and public spaces has lost its relevance as an arbiter of legitimate expectations of privacy.		
Supervisor: Tristan Nash		Word count: 14,320
I confirm that this is my original work and that I have adhered to the University policy on plagiarism. Signed  Email submission: if you are submitting this form via email, please tick this box ☒ (as a substitute for your signature) to confirm that you agree to the above declaration.		

For completion by the first marker:

Comments:

First Marker's Mark:

Date:

Signature:

For completion by the second marker:

Comments:

Comments:

Second Marker's Mark:

Signature:

Signature:

Date:

Agreed internal mark:

Signature 1st marker:

Signature 2nd marker:

Signature 1st marker:

Signature 2nd marker:

Date _____

Comments (for completion by the internal markers which indicate how the agreed internal mark has been arrived at):

NB. All marks are provisional until confirmed by the final examination board.

For completion by the External Examiner:

Comments:

Proposed Mark:

Signature of External Examiner:

Final Agreed Mark:

Comments (to indicate how the final agreed mark has been arrived at):

**The dichotomy between private and public spaces has lost its
relevance as an arbiter of legitimate expectations of privacy.**

Derek Linney

Submitted in partial fulfilment for the award of the degree of MA in
Philosophy

University of Wales Trinity Saint David

January 2026

Supervisor: Tristan Nash



Master's Degrees by Examination and Dissertation

Declaration Form

1. This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Name.....Derek Linney

Date 29th January 2026.....

2. This dissertation is being submitted in partial fulfilment of the requirements for the degree of MA in Philosophy

Name.....Derek Linney

Date 29th January 2026.....

3. This dissertation is the result of my own independent work/investigation, except where otherwise stated.

Other sources are acknowledged by footnotes giving explicit references.

A bibliography is appended.

Name.....Derek Linney

Date 29th January 2026.....

4. I hereby give consent for my dissertation, if accepted, to be available for photocopying, inter- library loan, and for deposit in the University's digital repository

Name.....Derek Linney

Date 29th January 2026.....

Supervisor's Declaration.

I am satisfied that this work is the result of the student's own efforts.

Signed:

Date:

Abstract

There has been a traditional distinction in both philosophical and legal discussion between the different expectations of privacy that apply in public spaces and private spaces. This dissertation argues that this dichotomy has always been more ambiguous than commonly presumed and has become even less relevant as technology impacts privacy in both spheres. Privacy is much more than the difference between simple observation of an individual in a public space and that person being hidden from view in a private space. Privacy primarily involves one having control over one's personal data, where the term "data" is used in the most general sense to include information about one's image, physical presence, identity and actions. Through philosophical and legal literature analysis and a combination of hypothetical and real-world examples I demonstrate that infringements of privacy arise not only from observation itself but also from how the information gained is processed, stored, accumulated, disseminated and used. Technology itself is blurring the boundaries between public and private space. Formerly private space becomes less private as we introduce information technology into our homes. At the same time, CCTV and facial recognition systems diminish privacy in public spaces. Technologies, such as mobile phones, track our movements and activities whether they occur in our homes, our offices, on the street or in a public park. While consent practises appear to give the individual control over what data about them is collected and how it is used, the protection this provides is largely illusory given the asymmetry of power and knowledge in the consent process. I conclude that effective philosophical and legal debate regarding privacy protection requires moving beyond consideration of spatial boundaries.

CONTENTS

Abstract	vii
1. Introduction	1
2. Definitions of Privacy	4
2.1 Models of Privacy	6
2.2 Proposed Model	9
3. Accumulation, Enrichment and Correlation of Data.....	14
3.1 An example regarding data enrichment	18
4. Public and Private Spaces	20
5. Privacy in Public Spaces	24
5.1 The Traditional Approach to Privacy in Public Places	25
5.2 The Arguments for Not Expecting Privacy in Public Spaces	29
5.3 Respecting The Privacy of Others in Public Spaces	30
6. The Impact of Technology on Privacy.....	31
6.1 Technology in Public Spaces	32
6.2 Technology in Private Spaces	34
6.3 Technology and Privacy in the Workplace	36
6.4 Future Technologies and Privacy.....	37
7. The Impossibility of Making Rational Decisions Regarding Consent.....	41
8. The Nothing to Hide Argument	44
9. Legal Approaches to Privacy	48
10. Conclusion	52
Bibliography.....	55

1. INTRODUCTION

“The UK is sleepwalking towards the end of privacy in public. The spread of insidious Facial Recognition Technology (FRT) in public spaces across the country will mean we can no longer walk down our local highstreets without being subject to constant monitoring and identification by dystopian surveillance technology.”

Privacy International (2025)¹

There has been a traditional distinction in both philosophical and legal debate between the different expectations of privacy that apply in public spaces and private spaces. Traditionally, privacy was thought to depend on physical boundaries: what occurred in private spaces, such as the home, was protected, while activities in public spaces were presumed to be open to observation. Many observers cite Aristotle’s distinction between the *polis* and the *idios* as locating the political sphere in public and the private sphere in the household.² Swanson disputes this, arguing that Aristotle’s use of “private” is not location specific.³ I will argue that such distinctions were never historically as clear cut as often presumed and become even less relevant as technology impacts privacy in both spheres. Closed Circuit Television (CCTV) and Facial Recognition Technology in public spaces destroy privacy, while smart speakers and browser cookies threaten privacy in our homes and smartphones track our activities across all locations.

The key argument I put forward is that privacy is much more than the difference between simple observation, for example in the street, and being hidden from potential observation in a private space. I maintain that privacy primarily involves you having control over your personal data, where *data* is used in the most general sense to include your image, physical presence, identity and actions. The threat to

¹ Privacy International, "The End of Privacy in Public," 2025, <https://privacyinternational.org/campaigns/end-privacy-public>.

² See Hannah Arendt, *The Human Condition*, 2nd ed. (Chicago: University of Chicago Press, 1998). p.29 and Beate Roessler and Judith DeCew, "Privacy," *The Stanford Encyclopedia of Philosophy* (2023). <https://plato.stanford.edu/archives/win2023/entries/privacy/>.

³ Judith A. Swanson, *The Public and the Private in Aristotle's Political Philosophy* (Ithaca: Cornell University Press, 1992). p.3

privacy arises not simply from observation but how the information gained from observation is processed, stored, accumulated, disseminated and used. In this dissertation I am concerned primarily with *informational privacy* as distinct from *decisional privacy*. Decisional privacy is the right of an individual to make choices and decisions about intimate and personal matters without interference or undue influence from others and includes topics such as a woman's rights to her own body when discussing abortion.⁴

I argue that technology itself is blurring boundaries between public and private space. Formerly private space becomes less private as we introduce smart speakers into our home and conduct business over Zoom meetings from our living rooms. Our browsing and other online activity is constantly monitored and recorded. Our phones and our cars increasingly record information about our location and activities. At the same time facial recognition systems, whether in the hands of organisations or private individuals, through their smartphones, are eroding the anonymity that we might previously have enjoyed in public spaces. As Nissenbaum argues:

‘[While] the private/public dichotomy is not in itself problematical it is not useful as the foundation of a normative conception of privacy’ especially in the world of modern information technology.⁵

A key factor in assessing the degree to which your privacy is affected by observation is the extent to which multiple items of data – captured at different times and/or places and/or by different agents – are accumulated. A series of data points, none of which of themselves threaten your privacy, may in combination represent a serious intrusion into that privacy. I discuss this issue at some length as it relates to privacy both in public and private places and indeed may make the boundary between these spaces irrelevant as personal information is accumulated from observations made across both types of location.

⁴ See, for example, Roessler and DeCew, "Privacy." pp.11-14

⁵ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, Calif.: Stanford Law Books, 2010). pp.116-7

I discuss how technology advances, such as Artificial Intelligence (AI), both increase the existing threats to privacy but also introduce entirely new categories of danger to personal privacy.

A major issue in controlling one's privacy is that when there is a trade-off between disclosing information – either explicitly, for example, when agreeing to cookies on a website, or implicitly when, for example, entering a shopping mall with CCTV cameras - one does not have available the full information on what data will be collected and how that data will be used. One cannot make an informed, economically or socially sound trade-off. While consent practises appear to give the individual control over what data about them is collected and how it is used, the protection this provides is largely illusory given the asymmetry of power and knowledge in the consent process

A common justification of technologies such as CCTV cameras is the *Nothing to Hide* argument: only those with something to hide need fear surveillance. I refute the Nothing to Hide argument both in terms of its simplistic approach to privacy and the way that it tends to conflate the ideas of *secret* and *private*.

While there is insufficient space for a full discussion of privacy in a legal context, I provide some examples of different legislative regimes regarding privacy. These suffice to illustrate that legal systems have difficulties with defining privacy, that historical and cultural differences are reflected in different legal treatments of privacy, and that legal systems have generally been unable to keep pace with the rapidly changing technological landscape.

I argue that failure to recognise that there are aspects of privacy that are relevant in public spaces creates an environment in which the use of invasive technologies such as CCTV cameras and facial recognition can go unchecked. At the same time, technology is making traditionally private spaces far less private. Compartmentalising privacy issues into public, private and online spaces hinders rather than helps attempts to maintain individuals' rights to privacy.

2. DEFINITIONS OF PRIVACY

“Privacy is a very complex concept, and scholars and others have struggled for centuries to define it and articulate its value”

Daniel Solove.⁶

While it is notoriously difficult to define privacy, or more specifically what constitutes an infringement of privacy, an understanding of what one is dealing with clearly affects any deeper discussion on how it may vary between private and public spaces. While a comprehensive survey of all definitions of privacy is beyond the scope of this dissertation, this section highlights the key factors relevant to consideration of the public/private dichotomy.

Since much surveillance in public spaces is covert, it is relevant to consider the consequentialist question as to whether an activity, e.g. the act of a voyeur, needs to cause one harm or distress to be an infringement of one’s privacy.⁷ Lowry Pressly discusses at length the case of Gerald Foos who opened a hotel specifically to spy on the guests.⁸ The ‘victims’ were unaware of the voyeurism and hence were also unharmed by its presence. Foos himself argued that his activities brought no harm to anyone and, because his guests were unaware of his voyeurism, they were not affected by it. He reasoned, ‘There’s no invasion of privacy if no one complains.’ Pressly argues that despite there being no apparent harm or distress to the people spied upon their privacy had nonetheless been violated; a moral harm had been done.

Suppose a hacker, sitting in his bedroom in Tokyo has hacked into hundreds of personal computers, including mine, and for each targeted computer his system records everything that is viewed or written on the computer and everything the webcam can see. Even if he never looks at the data for my computer, I would argue

⁶ Introduction to Alan F. Westin, *Privacy and Freedom* (New York: Ig Publishing, 2015). p.viii

⁷ Even where CCTV cameras are visible I would argue that the surveillance is essentially covert since the individual has no idea what the cameras are capturing, what is being recorded and how that data is being used.

⁸ Lowry Pressly, *The Right to Oblivion: Privacy and the Good Life* (Cambridge, Massachusetts: Harvard University Press, 2024). pp.58-77.

that he has infringed my privacy. This is true even though I am unaware of the activity and that the data collected is not seen by anyone; the mere presence of the data interception is a violation of my privacy.

However, if I am told that my computer is being constantly monitored then one could argue that I cannot, from then on, regard the recording of information as infringing upon my privacy. It would only be if the information were disseminated or used in a way I hadn't been told about, and implicitly or explicitly accepted, that my privacy was violated. When I use Google, I know that my data is being intercepted and used to feed me "relevant" ads when I use other websites or social media platforms. I know this, not from reading the voluminous Terms & Conditions (T&Cs), but from practical experience: I research a topic and I start seeing adverts related to that topic. Since I now know this is happening does it mean my privacy is not being invaded when Google does this since I should now have no reasonable expectation of privacy?

There is discussion as to whether the motive behind an activity, for example the collecting of data about one's movements, affects whether it is a breach of privacy. If the street photographer captures you crossing the street and uses the image as an illustration of city life does this represent a lesser invasion of privacy than an image he captures of a homeless person in distress that he posts on social media to gain likes? If he uses the latter to highlight the social issues of homelessness, is this any less an invasion of the subject's privacy?

Is there a difference between something being *private* and it being *secret*, and what does the answer tell us about privacy? Has an erroneous conflation of the two resulted in a distorted view of there being a distinction between privacy in public and private space: i.e. that one's presence in a public space cannot be secret so this means that one's activities in that public space cannot be private?

The next section discusses some of the models used to identify and categorise privacy.

2.1 MODELS OF PRIVACY

There is debate as to whether privacy is a primary right or whether it is derivable from other, more fundamental, longer established rights such as property rights. I will argue that it is a primary right and that it mainly flows from considerations of personal autonomy and the control of personal information. As such, this represents a deontological approach to privacy, although there are also consequentialist arguments that are discussed below.

Appeals to autonomy, of Kantian *Ends not Means* rights or to more fundamental rights could remove the need for a specific distinct *right to privacy*.⁹ This line of reasoning – *reductionism* - is followed by philosophers such as Judith Jarvis Thomson.¹⁰ Such arguments, while typically valid for certain specific types of privacy, do however each tend to narrow the definition of privacy to too great an extent or apply to only one type of privacy.¹¹ Nagel distinguishes instrumental rights of privacy which may be derivable from other established rights from intrinsic rights to privacy which are not.¹²

Consequentialist arguments in favour of privacy, range from the necessity of privacy if we are to be able to maintain differentiated social relationships to the necessity for privacy in a functional democracy. While secret ballots may be the norm in Western democracies, it is not clear that they are essential, per se, to democratic government: ancient Greece was considered democratic, but elections were held by a public vote and many “democratic” organisations, such as the United Nations or UK Parliament, have open voting. However, Westin holds that political organisations require privacy if they are to be able to operate freely in democratic

⁹ Bell explores the ethics of street photography through a Kantian perspective in Macalester Bell, "Wronging Persons Through Photographs: On Photographic Front Incursions," *Journal of ethics & social philosophy* 30, no. 4 (2025). Pp.578-81

¹⁰ Judith Jarvis Thomson, "The Right to Privacy," in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984). and Roessler and DeCew, "Privacy." pp.14-16

¹¹ Carissa Véliz, *The Ethics of Privacy and Surveillance*, Oxford philosophical monographs, (Oxford: Oxford University Press, 2024). pp.65-69

¹² Thomas Nagel, "Personal Rights and Public Space," *Philosophy & public affairs [e journal]* (1995). p.86.

societies.¹³ Philosopher James Rachels makes the case for the need for privacy to maintain social relationships and, similarly, sociologist Erving Goffman sees it as essential to enable the different personal and professional roles we play in life.¹⁴

There is a good argument that privacy is not a single thing but a family (in the Wittgensteinian sense) of related concepts.¹⁵ While privacy itself is very hard to define, activities that threaten privacy are perhaps easier to categorise. Approaching privacy through the processes by which it is compromised also helps negate arguments that privacy is not a “right” as such but is derivable from other more fundamental rights. For example, if you read someone else’s private letter then this is clearly a privacy issue - you are gathering information - but it is not really a theft of property. Stealing the letter would however be a breach of property rights. Stealing something breaches property rights because it deprives the owner of his property - i.e. that which is stolen - whereas reading the letter without permission doesn’t deprive the owner of the letter. What it does do is deprive the owner of his privacy regarding its contents.

Gavison, while primarily focussed on how privacy is handled in legislation, provides a set of more generally applicable concepts of privacy which she maintains are distinct but coherent:¹⁶

- Our accessibility to others
- The extent to which we are known to others
- The extent to which others have physical access to us
- The extent to which we are the subject of others' attention

For Gavison, this multi-dimensional nature of privacy offers an argument against reductionism.¹⁷

¹³ Westin, *Privacy and Freedom*. pp.46-47.

¹⁴ Rachels makes the case for the need for privacy to maintain social relationships in James Rachels, "Why Privacy is Important," in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984). Goffman is referenced in Daniel J. Solove, *On Privacy and Technology* (Oxford: Oxford University Press, 2025). p.32

¹⁵ Véliz, *The Ethics of Privacy and Surveillance*. pp.70-73

¹⁶ Ruth Gavison, "Privacy and the Limits of Law," *The Yale law journal* 89, no. 3 (1980). p.423

¹⁷ Ibid. pp.460-467

Clarke proposes a taxonomy of privacy, derived in part from consideration of Mazlow's *Hierarchy of Needs*:¹⁸

- Privacy of the person
- Privacy of personal behaviour
- Privacy of personal communications
- Privacy of personal data

Of these, we are primarily concerned with the last two as these relate more to *informational privacy* as opposed to *decisional privacy*.

Finn expands Clarke's list to seven, largely to encompass the changing technological landscape.¹⁹ They are:

- Privacy of the person
- Privacy of behaviour and action
- Privacy of communication
- Privacy of data and image
- Privacy of thoughts and feelings.
- Privacy of location and space
- Privacy of association

Again, the first two do not concern us here, but the informational privacy items have been expanded.

By contrast, Solove proposes a model based more upon the processes by which information is gathered, processed and used.²⁰ His four-part model involves:

- Information Collection
- Information Processing
- Information Dissemination
- Invasions

He then breaks each of these areas down further to provide a "taxonomy" of privacy. While he is primarily focussed on how privacy is treated in law, his

¹⁸ Roger Clarke, "What's 'Privacy'?", (2006). <https://www.rogerclarke.com/DV/Privacy.html>.

¹⁹ Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer Netherlands, 2013).

²⁰ Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania law review* 154, no. 3 (2006).

approach is useful in the wider ethical and philosophical debate. Solove's approach clearly equates privacy issues with the access to and use of data.

Pressly explicitly criticises this trend towards considering privacy purely in information terms as he feels that this encourages an economic model which is at odds with the true value of privacy.²¹ He believes this plays into the hands of the technology giants: that privacy becomes something to trade.²² Posner, however, supports the view that privacy should be assessed in economic terms.²³ For example, asking what is the economic cost of maintaining a right to information privacy.

2.2 PROPOSED MODEL

There is not room here to explore or critique each of these models, but instead I propose to use an *observe, store, process, distribute, use* model of personal information which has proved appropriate while exploring the public-private space dichotomy. While derived from Solove, the proposed model varies from it in simplifying the processes of Solove's model. It is also more concerned with the privacy infringement itself rather than consequential harm from that infringement.

The privacy of the individual may be impacted by any or all stages of the model:

- The act of observation
- The storing of data (including accumulation)
- The processing of data (including enhancement such as facial recognition or correlation among accumulated data)
- The distribution of data (including publishing the data, whether through traditional channels or online, and sharing data with other parties)
- The use made of the data

²¹ Pressly, *The Right to Oblivion*. pp.5-11

²² Ibid. p.7

²³ Richard A. Posner, "The Economics of Privacy," *The American economic review* 71, no. 2 (1981).

This essay concentrates on the first four parts of this model. These stages in the model provide a framework for identifying activities that represent a potential moral harm from the loss of privacy. The *use* stage crystalises any related instrumental harm that may arise: the effect and cost of that loss of privacy. Any consequentialist analysis of the result of a loss of privacy needs to explore the use to which the obtained personal data is put. Such analysis also needs to balance that cost against any benefits derived from the data. This is relevant when assessing, for example, the balance between security and surveillance.²⁴ The instrumental harm/benefit element is also vital to legal debates about privacy since it is fundamental to many justifications for collecting personal information including the *legitimate interest* defence for keeping or sharing online data. Such analysis is largely outside the scope of the current essay which focusses instead on identifying those situations where privacy is breached and particularly where this is done without the knowledge of the individual affected. Society needs to be fully aware of the scale, location and nature of such infringements of privacy if it is to have a rational debate about the trade-offs between privacy, security and convenience.

The greater the extent to which the individual can control the stages of the model, the greater the degree of privacy. The essence of privacy is that you decide how much of the information about you is made available to third parties. Now clearly, there are differences in the availability of information about your actions when you are alone in your own home compared with when you are in a public space such as the centre of the village where you live. When you're in your own home then by default you have privacy because information about what you're doing is only known to you unless you choose to disclose that information, for example, during a video call to a friend. When you're walking in the street then your activities will be visible to anyone else in the street. The information gained may be, for example to a stranger, simply where you are and which direction you're walking, or, if it's someone you know, will include your identity.

²⁴ Véliz, *The Ethics of Privacy and Surveillance*. pp.120-140

There are three categories within the information that is made visible by your location and activities:

1. Information that arises simply because of the circumstances, i.e. it is an inevitable byproduct of your location and activity, for example walking down the street.
2. Information that may need to be disclosed as part of a transaction: e.g. when withdrawing money from a bank then the bank needs to verify your identity.
3. Information that is collected but which is not necessary for the activity, and which is not an inevitable byproduct of that activity. This can range from data collected for law enforcement – e.g. speed cameras – to private organisations collecting your purchase data for marketing purposes. It may be gathered either with or without your explicit consent.

It is in this third category that the major intrusions and infringements of your right to privacy lie. If the speed camera captures everyone's number plate, irrespective of whether they were speeding, just to have that information available raises the question as to whether that is a legitimate and justifiable form of data collection.

To explore the lack of real difference between public and private space consider the following examples from both private and public spaces which illustrate how privacy or its violation can occur in either setting. If you invite someone into your home then you are allowing them a certain access to some data about you and your circumstances and how you live, but, if while you are making them a cup of coffee, they go wandering off into the bedroom and start looking through the drawers in your bedroom, then you would regard that as an infringement of your privacy. They have moved beyond the boundaries of the informational space to which you have given them access.

Similarly, if you are out shopping and come across an acquaintance then, as previously explained, the fact of your identity and the fact that you are shopping is obvious to that person. Therefore, the disclosure of that information cannot be seen as an invasion of privacy because it is an inevitable consequence simply of the actions you are taking. However, if that person sees the shopping bag you're carrying and then starts looking, uninvited, inside the shopping bag, you will clearly

regard that as a breach of your privacy. Irrespective of whether you are in a private or public space you desire control, in the interests of privacy, over the extent of data sharing beyond that which is a byproduct of the activity itself.

To give another example: suppose you go into a furniture shop and purchase a chest of drawers for delivery to your home then the shop not only needs to identify you to the extent needed for the sales transaction and your payment but it also needs to know your home address because that is necessary information for it to fulfil its side of the bargain of delivering the furniture. However, if you are buying a table lamp which you are taking home with you, then whilst the shop still has the legitimate need to know sufficient about you to verify payment it does not need to know your address. It might ask you, but if you refuse to give that information then it would be regarded as an infringement of your privacy for it to try and obtain that address information surreptitiously.

There have been reports in the USA from users of the Square payment system that if they use their bank card to purchase an item at a store that is using a Square payment device and as part of that transaction there is a legitimate need for the store to have additional information about them - for example their email address because the store needs to email them the warranty information of the item they have purchased – then that information is retained by Square.²⁵ If they then go into another store which also has a Square point of sale system and proffer their bank card then their email address and other information, that Square may know such as their phone number, will be made available to the shopkeeper. This is a breach of privacy since there is no legitimate need for them to have it, the shopper is not volunteering that information and he has not given consent. Bizarrely, Block Inc., who own Square, post a privacy notice on their website which dictates T&Cs for customers who shop at a store using the Square POS system and which says:

‘If you are a consumer shopping at a business that uses Square, this privacy notice applies to you. It explains what data we collect about

²⁵ The details are unverified but reported by Reddit users: Reddit, "Square POS "Send receipt to phone/email" creates a shadow profile linked to your card number," (2024). https://www.reddit.com/r/privacy/comments/1gdqv02/square_pos_send_receipt_to_phoneemail_creates_a/.

you, what we do with it, when and why we share it with others, how long we keep it, how we secure it, what cookies are and what they (and similar technologies) do, what data is collected about you by third party service providers, and what choices you have to control your data. By using our services you consent to these data practices.’²⁶

So, by buying something in a store equipped with a Square POS device you, the customer, are accepting T&Cs you know nothing about.

In general, gathering information about an individual, or about that individual’s activities, should be limited to that which is appropriate to the circumstances, where “appropriate” is the minimum needed for the transaction or activity to take place. The individual may be asked for more information but may decline to provide it on the grounds of *privacy*.

While the privacy model adopted is agnostic regarding location, what may vary between different locations is the justification needed to override the right to privacy by other considerations such as security. For example, in the UK, in public areas:

‘a police officer might stop you and ask your name, ..., but you do not have to stop or answer any questions. If you do not and there’s no other reason to suspect you, then this alone cannot be used as a reason to search or arrest you.’²⁷

In other words, you have a right to privacy unless the police officer has reason to suspect you. However, when you are in a private home then, with exceptions, the police require a greater justification for the infringement of privacy: enough to be granted a search warrant to enter the property.²⁸

²⁶. Block Inc, "Privacy Notice for Users Who Do Not Apply or Sign Up for a Square Account or Other Services," 2023, https://squareup.com/us/en/legal/general/privacy-no-account?country_redirection=true.

²⁷ UK Government, "Police powers to stop and search: your rights," 2025, <https://www.gov.uk/police-powers-to-stop-and-search-your-rights/police-powers-stop-question>.

²⁸ UK Government, "Crime and Policing Bill: police powers factsheet," 2025, <https://www.gov.uk/government/publications/crime-and-policing-bill-2025-factsheets/crime-and-policing-bill-police-powers-factsheet>.

3. ACCUMULATION, ENRICHMENT AND CORRELATION OF DATA

*“If you give me six lines written by the hand of the most honest of men,
I will find something in them which will hang him.”*

Cardinal Richelieu (1585–1642) ²⁹

Suppose that as you leave your house your neighbour is standing at her window, and she observes you walking down the road. This clearly is not infringing your privacy. But suppose that every time that you leave the house she is at the window, and you see that she has a notebook and appears to be recording your movements. Despite the individual observations not threatening your privacy the repeated observations and the accumulation of data over time do seem to do so.³⁰

Your purchases at a shop are recorded on the till as is your debit card. But suppose the shop accumulates data over multiple visits using your payment card as the identifier, does the picture it builds up of your purchases start to invade your privacy? If you have a loyalty card, and use it, then you have probably agreed to such accumulation of data so cannot regard this as a breach of privacy.³¹ But, if you have no such loyalty card and have never agreed to the store keeping data about you then it would seem that the action of accumulation is infringing your privacy.

Solove gives a simple, but powerful example of how accumulation of data can threaten privacy: consider a person who buys a book about cancer.³² This could be for a wide variety of reasons, for example they may be a health professional or have

²⁹ Susan Ratcliffe, "Cardinal Richelieu," in *Oxford Essential Quotations* (Oxford University Press, 2017).

³⁰ I use the term *accumulation* rather than *aggregation* as the latter, while often used by non-technical writers on privacy to mean accumulation, more normally refers to adding together data from different subjects or events to arrive at a single overview – e.g. consolidating outcomes of a medical procedure to gain a view of its overall effectiveness and safety. Most technical authors on the privacy of data, when writing about *aggregation*, are concerned with whether the aggregated data which, while anonymised, might contain gender, age and demographic data that could allow individuals to be identified. This is different from processing accumulated data on an individual where events from different locations and times are compared and joined to give new information about or insights into that individual.

³¹ However, as I discuss in Chapter 7 it is not at all clear that you can fully understand the full impact of the *consent* you may have given.

³² Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (New Haven Conn.: Yale University Press, 2011). p.27

a relative they are caring for who has cancer. But, if that same person then buys a wig then one can make the inference that it is highly likely that they are not only suffering from cancer but are undergoing chemotherapy.

Accumulation not only happens within organisations collecting data – such as a specific online retailer - but data can be enriched through the merging of data from other, usually commercial, sources. For example, Experian advertises its services in this area:

‘Business and marketing data enrichment allows brands and businesses to learn more about their users and customers, whether business or consumer. Enrichment also helps to increase the value of data by enhancing it with additional information and intelligence.’³³

Experian is, in effect, providing the same service today, and using today’s technologies, as Lotus/Equifax offered in 1990 with a consumer database of 120 million households on multiple CD’s: *The Lotus Marketplace: Households*. The offering was withdrawn after a public backlash.³⁴ However, public victories regarding privacy tend to be short lived.³⁵ Even at the time, industry insiders commented that the Lotus offering was no more than most of the marketing data industry was doing, it simply became known to the public.³⁶

Accumulation can refer to data collected at different locations, such as from different CCTV cameras as you walk round the town centre, and/or at different times; for example, each time you buy an item on Amazon.³⁷ It is clear that while an individual action – the observation and possibly recording of your activity at a particular place and time – may not infringe your privacy, the accumulation of such

³³ Experian, "Data enrichment and enhancement," 2025,
<https://www.experian.co.uk/business/data-quality/solutions/data-enrichment>.

³⁴ Nissenbaum, *Privacy in Context*. pp.8-9

³⁵ Ibid. p.9

³⁶ Mary J. Culnan, "The Lessons of the Lotus MarketPlace: Implications for Consumer Privacy in the 1990's" (paper presented at the Computers, Freedom & Privacy, Burlingame CA, March 26–28 1991).

³⁷ Facewatch, the leading facial recognition CCTV system used by UK retailers, promotes itself with the feature that “A database is shared by geography with every Facewatch subscriber....” Facewatch, "The Trusted Name in Retail Crime Prevention," 2025,
<https://www.facewatch.co.uk/>.

data can do so. Interestingly, this scenario – where an individual occurrence of an action is lawful while the repeated occurrence may be unlawful – is recognised in law when dealing with issues such as stalking or harassment.³⁸

Correlation occurs when data from multiple individuals is cross-referenced and from this knowledge of occurrences - such as the frequency, regular timing and location of meetings – a relationship between those individuals can be inferred. Or the correlation may show that while two or more individuals may not have met one another, they do meet, on separate occasions, with a third party.

The observe/store/process/distribute/use model of privacy implicitly has the ability to handle this effect - multiple occurrences of a legitimate action becoming illegitimate – through the store/process dimensions. Models of privacy that simply concentrate on the observe and distribute data aspects of privacy struggle to handle the issue of accumulation.

This is particularly relevant in the consideration of privacy in public spaces. Your image captured on a CCTV camera may not seem particularly significant nor any real infringement of your privacy. However, if that CCTV camera links to a facial recognition system which can identify you and link your movements to every other time you have been captured on CCTV cameras, either directly managed by the same agency or to which that agency, e.g. the police, have access, then your privacy is certainly under threat. CCTV cameras in public places are generally either controlled by official organisations – police, local authorities etc. – or by commercial organisations such as shopping precinct operators. Widespread distribution of the images is therefore not the primary concern but rather how such data is used and particularly how it is accumulated. An example of the dangers is that of shoppers falsely blacklisted across multiple retailers as a result of errors in facial recognition systems.³⁹ The Home Office recently admitted that false-positive rates, in facial recognition systems, were significantly higher among Asian and

³⁸ See e.g. Ursula Smartt, "The Stalking Phenomenon: Trends in European and International Stalking and Harrassment Legislation," *European journal of crime, criminal law, and criminal justice* 9, no. 3 (2001). p.218

³⁹ Big Brother Watch, "Stop Facial Recognition," 2025,
<https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>.

black people and were up to 9.9% in the case of black women, compared to 0.04% for white subjects.⁴⁰ This bias could result in false arrests or stop and search among ethnic minorities when in public places.

On the other hand, private image capture devices such as smartphones, dashcams and video doorbells can lead to rapid, widespread dissemination of one's image taken in a public space. Rapidly developing technologies such as facial recognition, or even simple tagging within images on social media, lead to one being identifiable and hence open to the indexing and accumulation of such images.⁴¹

Any satisfactory account of privacy, whether in public or private spaces, needs to account for the accumulation effect. As Nissenbaum states:

‘If so many of the individual incursions, taken by themselves, cause only tiny, even imperceptible breaches – a camera here, a tagged image there, one's clickstream sold to an ad agency – how is it possible to address the big, truly worrisome totality with policies targeted to any one of these?’⁴²

In the digital age, the accumulation and analysis of data can expose individuals in ways they neither anticipate nor consent to, making the protection of privacy an ever more complex and urgent challenge. A particular risk from accumulation of data is that it enables technology companies to go beyond simple, moderately personalised adverts and content into more intrusive persuasive technologies exploiting our anxieties and weaknesses.⁴³ As such it represents a threat to our autonomy.

⁴⁰ Rajeev Syal, "Home Office admits facial recognition tech issue with black and Asian subjects," *The Guardian*, 5th December 2025.

⁴¹ I use the term *indexing* to refer to the process by which an image or any piece of data about an individual or an item is tagged with an identifier (the index) which enables multiple discrete pieces of data about that person or object to be correlated.

⁴² Nissenbaum, *Privacy in Context*. p.242

⁴³ James Williams, "Ethical Dimensions of Persuasive Technology," in *Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford University Press, 2023).

3.1 AN EXAMPLE REGARDING DATA ENRICHMENT

An example of data enrichment, that I believe goes beyond simple targeted marketing, is a charity – the Marie Curie organisation which provides palliative and end of life care – using “wealth analysis” to determine whether their supporters could be donating more than they currently do:

‘We may conduct donor wealth analysis. Donor wealth analysis involves us assessing information about you to understand whether you have the capacity and/or affinity to support Marie Curie at a higher level (such as making a major donation). To conduct donor wealth analysis efficiently, we may use trusted third-party wealth analysis companies that undertake profiling to collate and analyse information we provide together with information from public registers alongside statistical social-economic data. This helps us to understand more about your interests and level of potential engagement or donation.’⁴⁴

And, as they themselves state:

‘... we may use data analysis to interpret your data and predict how likely you are to be interested in or responsive to a particular campaign or fundraising message.’⁴⁵

As well as using a specialist wealth analysis companies they obtain data from:

‘...company resources, public registers, public record databases and documents which provide information on ownership of assets, trade and industry references, professional directories, print and broadcast media, company websites and any data that you choose to make public on LinkedIn such as your professional memberships and networks. We may also use any publicly available data that you share on social media. We may use additional information such as geographical information for measures of affluence where available.’

⁴⁴ Marie Curie, "Supporters Privacy Notice," 2025, <https://www.mariecurie.org.uk/privacy/supporters-privacy-notice>. ‘Donor Wealth Analysis’

⁴⁵ Ibid. ‘How we combine and analyse the information we collect about you.’

This approach is lauded by CACI, one of Marie Curie's data enrichment partners:

‘Mark Lumby, Head of Fundraising Insight at Marie Curie, shared the charity's motivation for embarking on a data enrichment journey: the necessity of understanding more about their supporters beyond basic demographics. The more data charities have access to, the more robust their engagement strategies can be shaped, resulting in more income from supporters. By partnering with CACI, Marie Curie aimed to gain these deeper, necessary insights into supporter profiles, affluence, interests and behaviours.’⁴⁶

I have quoted this example at length to illustrate the issue of data accumulation and enrichment. A charity which I support with donations is exploiting information about me by profiling that goes far beyond anything I expected, or believe I consented to, when I started supporting them. While building profiles of their supporter base to identify target audiences is commonplace among marketers, the idea that they are trying to estimate my individual wealth, to see if I should be targeted to contribute more, is an unwelcome intrusion into my privacy.

⁴⁶ Harsh Tandon, "How Marie Curie use data & insights to improve supporter engagement & increase income," CACI, updated 27th May, 2025, <https://www.caci.co.uk/insights/how-marie-curie-use-data-insights-to-improve-supporter-engagement-increase-income/>.

4. PUBLIC AND PRIVATE SPACES

“Public Space is for living, doing business, kissing and playing. Its value can’t be measured with economics or mathematics; it must be felt with the soul.”

Enrique Peñalosa (2001).⁴⁷

Defining what constitutes private and public spaces is itself problematical. As Hylen, discussing the Early Roman Period, comments:

‘... it is correct to say that ‘the ancients distinguished between a public and private sphere’, but not that ‘the private sphere was located in private houses’ and the public sphere included everything outside. Rather, a good deal of ‘public’ activity took place inside of houses, while many functions that were considered ‘private’ occurred outside them. The overlap between public and private functions and space makes the neat divisions of modern scholarship untenable.’⁴⁸

And Scanlon, discussing the contractualism implicit in behaviour and privacy in public, comments:

‘People need to be able to conduct parts of their lives protected from the scrutiny of others whom they have not chosen to admit ... even within a given society there are many different ways in which these needs can be provided for ... different ways of defining the boundaries between ‘private’ and ‘public’ space.’⁴⁹

For the purposes of the examples and arguments in this paper, I will use a simplified model that treats “public” in terms of free public access rather than physical property ownership. Hence, I will include streets, parks, countryside and shopping malls within the realm of public spaces, and largely exclude homes, workplaces and

⁴⁷ Enrique Peñalosa, "Speech to the Urban Land Institute" (paper presented at the Urban Land Institute Annual Meeting, Boston, Massachusetts, 3rd October 2001 2001).

⁴⁸ Susan E. Hylen, "Public and Private Space and Action in the Early Roman Period," *New Testament studies* 66, no. 4 (2020). p.536

⁴⁹ Thomas Scanlon, *What We Owe to Each Other* (Cambridge, Mass.: Belknap Press of Harvard University Press, 1998). p.339

commercial venues with restricted access. While not definitive this should not significantly affect my conclusions about privacy in public spaces.

There have been attempts to more formally define the nature of public spaces, but such attempts tend to place too much emphasis on ownership.⁵⁰ They also struggle with locations that may fall into multiple categories: consider a university campus which may simultaneously be a space open to the public, a workspace and a residential community space and which is most likely on privately owned land. While ownership is clearly important in terms of who has the legal authority to erect and operate, for example, surveillance cameras, it doesn't act as a clear arbiter of private vs. public space.

There is a view that in many Western countries there has been a capitalisation of public space, with a greater proportion of publically accessible space falling under private ownership. Compare the traditional public street with shops, restaurants and offices accessible from the street to today's shopping malls, food courts and office complexes where access to the individual units is through privately owned concourses.⁵¹ Miles, discussing photography in public in Australia, comments on confusion as to which spaces are private and which are public caused by the privatisation of formerly public spaces such as shopping centres and railway stations.⁵²

There are three fundamental sources of surveillance in public spaces:

- Official bodies – national and local authorities, police and security forces
- Commercial and institutional organisations – shopping malls, offices, carpark operators, university authorities etc.
- Private individuals – through cameras, smartphones, dashcams, video doorbells etc.

⁵⁰ Bert-Jaap Koops and Masa Galic, "Conceptualising Space and Place," in *Privacy in public space: conceptual and regulatory challenges* (Cheltenham, UK: Edward Elgar Publishing, 2017).

⁵¹ Tjerk Timan, "Conclusion: The Need for Privacy in Public Space," *ibid.* pp.278-283.

⁵² Melissa Miles, "Photography, Privacy and the Public," *Law, culture and the humanities* 11, no. 2 (2015). p.282

Although official and commercial surveillance may represent a serious threat to our freedoms as citizens, the surveillance material is not generally widely circulated outside the realm within which it is captured. However, photography and video captured by ordinary persons creates, through the growth of social media, an environment in which the widespread circulation of images, taken without the individual's consent, becomes pervasive.

What generally constitutes "private" space is perhaps somewhat simpler to define than "public" space. It is space where access is controlled and limited to specific individuals. For example, a personal residence: 'an Englishman's home is his castle'.⁵³ Private spaces have traditionally been regarded as providing a high degree of privacy.⁵⁴

However, the issue is not as clear cut as it may appear. Consider a private house with a driveway running from the public road to the front of the house. Is the driveway "private". If the driveway is gated and requires the owner to open the gate to allow access, then it is easy to see that it might be considered "private". But if it's not gated and anyone can walk up the driveway to the front door then, as far as access is concerned, it becomes "public". This becomes relevant when, for example, the owner has a smart doorbell installed that videos and records anyone entering the driveway and approaching the front door. The owner could argue it is private property so he can record anyone approaching the house and, if he feels like it, could post that video to social media.⁵⁵ But the postman might regard it as public space and that he has a right for the image of him going about his lawful business of delivering letters not to be distributed online.

⁵³ There are many attributions for the phrase but the earliest seems to be "*.. but the house of one is to him his castle and his defence*" from a ruling made by the King's Bench in 1505. Word Histories, "Origin of 'An Englishman's home is his castle'," 2017, <https://wordhistories.net/2017/07/26/englishmans-home-castle-origin/>.

⁵⁴ There are anomalies such as to the degree of privacy enjoyed by the upper classes in their homes, surrounded as they were by servants, or whether the working classes living in overcrowded tenements had any privacy at home.

⁵⁵ This discussion is independent of the situation where smart doorbells, because of their field of view, record neighbours on their own property – clearly infringing privacy - or passers-by in the street - arguably an invasion of privacy. For a legal view see; Information Commissioner's Office, "Home CCTV systems," For the public, 2025, <https://ico.org.uk/for-the-public/home-cctv-systems/>.

Feminists have also criticised the traditional model of public space and private space as different realms, and maintain that women have, under the cover of privacy, been subjected to repression and physical harm in the private space of the home.⁵⁶ This view is however partially culturally/religiously determined as in Muslim communities, where the private space is largely female dominated, women may regard public space as the male-dominated space.⁵⁷

Private places can be divided, roughly, into those that are private dwelling spaces and those that are owned and occupied by commercial or administrative bodies. In the former where there has, until recently, generally been a high degree of privacy, it can be argued that recent reductions in privacy have been “self-inflicted” by the homeowners introducing technology, albeit without realising the implications, into their own homes. By contrast offices have never provided a great deal of privacy, but what privacy they had is being eroded by surveillance technologies deliberately introduced by the owning or management organisation.⁵⁸

⁵⁶ Roessler and DeCew, "Privacy." pp.18-21

⁵⁷ Ariane Pereira and Emília Malcata Rebelo, "Women in public spaces: Perceptions and initiatives to promote gender equality," *Cities* 154 (2024). Section 2.2

⁵⁸ Isabel Ebert, Isabelle Wildhaber, and Jeremias Adams-Prassl, "Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection," *Big data & society* 8, no. 1 (2021).

5. PRIVACY IN PUBLIC SPACES

“Tourists who have loaded themselves with rolls of films for use in Europe this summer will have to be careful when they go to Germany. In that thoroly regulated country a new law goes into effect July 1st prohibiting the photographing of any person or his property without his express permission.”

The Independent (1907)⁵⁹

If, when walking along a London Street, someone takes my photograph, without my consent, and publishes it on social media then I may be irritated, but have my fundamental rights been infringed? Prosser would say they have not:

‘On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of privacy to do no more than follow him about. Neither is it such an invasion to take his photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which any one person would be free to see.’⁶⁰

Similar views to Prosser’s were expressed as early as 1907 in an editorial in The Independent magazine which proclaims that:

‘As regards photography in public it may be laid as a fundamental principle that one has a right to photograph anything that he has the right to look at.’⁶¹

This was in response to news that the German Government had just enacted legislation to prohibit the photographing of any person without their consent.⁶²

However, Westin is clear that privacy in public spaces is an essential requirement to wellbeing:

⁵⁹ The Independent, "The Ethics and Etiquet of Photography," *The Independent*, 11th July, 1907. pp.107-8

⁶⁰ William L. Prosser, "Privacy," *California law review* 48, no. 3 (1960). pp.391-2

⁶¹ Independent, "The Ethics and Etiquet of Photography." pp.107-8

⁶² See epigraph at the start of this chapter.

‘Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.’⁶³

Until large scale urbanisation and advanced transportation one could argue that there was little idea of privacy within public spaces; in the village or small town everyone knew everyone, and one could not expect privacy within public spaces. With large scale urbanisation we started to enjoy the opportunity of anonymity and privacy whilst in public spaces. However, in recent times, the advent of technology-based surveillance coupled with unparalleled opportunities for this material to be widely disseminated by electronic communication has rapidly diminished the opportunity for anonymity and privacy in public spaces.

Surveillance of public spaces has also been seen as a step towards totalitarianism and a threat to democracy:

‘The CCTV camera is the synecdoche of potentially totalitarian state and corporate superintendence. Public space, in turn, is the basic ingredient of democracy. From the Greek polis to the town square to the rough and open culture of contemporary urban streets, public space is a resource, a commons, the crucial platform of popular democratic tradition. How many revolutions, including our own, were catalyzed on the public stage of the street or the commons? Destroying or controlling these public spaces has always been a political tool by which rulers battle restive populations....’⁶⁴

5.1 THE TRADITIONAL APPROACH TO PRIVACY IN PUBLIC PLACES

Traditional approaches to privacy, in both ethical debate and law, have tended to treat privacy differently between privacy in “private” spaces and in “public” spaces. Private spaces have been regarded, generally, as spaces where there is a physical barrier between the subject and the outside world – e.g. within a person’s house – and within which a person is entitled to privacy. Anywhere where the subject can

⁶³ Westin, *Privacy and Freedom*. p.34

⁶⁴ Christian Parenti, *The Soft Cage: Surveillance in America, From Slavery to the War on Terror* (New York: BasicBooks, 2003). p.110

be observed, whatever its actual ownership – such as a town square, a shopping mall or a theatre, is a “public” space. Even in a public space there has, generally, been some degree of a right of privacy: the physical “bubble” around the person which prevents the observation of artifacts, for example a document in a jacket pocket or goods within a shopping bag, provides the basis of privacy. It would be a breach of privacy to invade this physical space. One reason that Stop and Search powers given to the police are controversial is precisely because they intrude upon this privacy.

It is also indicative of there being some expectation of privacy in public spaces, or at least semi-public spaces such as theatres, that early concerns regarding infringements of privacy, in late 19C America, corresponded to the advent of photography and the publishing of photographs of individuals taken in such locations without their consent.⁶⁵

Goffman developed a theory of “territories” that are created by individuals and groups when in public places and which may be spatial – e.g. the implicitly negotiated spacing on a park bench between strangers – through to an informational space – what one chooses to share.⁶⁶ Individuals are constantly assessing and making claims on such territories as they negotiate public spaces. Individuals may also, through for example reading on a train or wearing headphones while walking along the street, signal that they wish to be treated as in a private space.⁶⁷ As Vincent Jackson commented back in 1994: ‘The experience of listening to your Walkman is intensely singular. It signals your desire to cut yourself off from the rest of the world.’⁶⁸

⁶⁵ See: Amy Gajda, *Seek and Hide: the Tangled History of the Right to Privacy* (New York: Viking, 2022). pp.ix-xi and Pressly, *The Right to Oblivion*. p.45.

⁶⁶ Robin James Smith, "Interaction in Public Spaces," in *The Routledge International Handbook of Goffman Studies*, ed. Gregory W. H. Smith and Michael Hviid Jacobsen (London: Routledge, 2022). pp.103-5

⁶⁷ Adriana De Souza e Silva and Jordan Frith, "Locational Privacy in Public Spaces: Media Discourses on Location-Aware Mobile Technologies," *Communication, culture & critique* 3, no. 4 (2010). pp.505-6

⁶⁸ Vincent Jackson, "Menace II Society," in *Doing cultural studies : the story of the Sony Walkman*, ed. Paul Du Gay and et al (London: SAGE in association with The Open University, 1997). p.144

In public spaces, one can argue that there is loss of privacy from the mere observation of the person and which is available to anyone passing by, and hence there should be no expectation of privacy. But, this has traditionally been limited by several factors:

- Unless you are known personally to the observer then your identity remains private: you are anonymous
- The information available is limited to the outwardly observable details
- Any dissemination of information by the observer is limited by their sparse communication channels
- Any dissemination of information by the observer will take a lengthy period of time
- Any aggregation of information across sources or time is severely limited.

It may get reported by the local gossip in the pub that you have been seen twice in the High Street in a state of apparent intoxication, but that information is likely to remain highly localised.

Also, even in public spaces, there are areas which traditionally have provided a degree of privacy: e.g. a secluded part of a public park. Social norms have also contributed to a degree of privacy: a courting couple on a park bench are usually ignored by passers-by. Indeed, it can be argued that public places have historically often afforded greater privacy than private locations such as dwelling spaces or workplaces. As well as the courting couples, those park benches may also be occupied by spies having clandestine meetings or an office worker seeking a brief interlude of privacy for her own thoughts away from the pressure of her office environment.⁶⁹

When walking down the street in my village I pass another person; depending upon my relationship – close friend, acquaintance or stranger – I may or may not, but usually will, offer a simple greeting. Whether this develops into a dialogue depends not only upon my relationship with the other person but also whether I and they are

⁶⁹ Spies really have chosen to meet in public parks; this is not simply the imagination of spy thriller writers. For example, Kim Philby met his Russian handler in Regents Park. Kim Philby, "The day I was recruited as a Russian spy, by Kim Philby," *The Observer*, 15th August 1999.

both in the mood to stop and talk. There are subtle - e.g. body language - and less subtle - “sorry I’m late for an appointment” - ways that we signal this to each other.⁷⁰ If I signal my lack of desire for conversation then I will take any further exchange, such as questions about what I am about, by the other person as not only annoying but starting to infringe upon my privacy. Effectively I create a “private” space around me, even though I am in public.⁷¹ This can be described as *personal space* which transcends the public or private nature of my physical location.⁷²

Nissenbaum quotes from a detective novel to illustrate the anonymity of public places:

‘Conversation between the detective and the suspect:

“Where were you when Talbot was killed?”

“Jogging. In Central Park”

“Witnesses?”

“Hundreds”

“So you have an alibi.”

“Not exactly” Resnicow, *The Gold Solution* (1983)

i.e. seen by hundreds, noticed by none.’⁷³

She also illustrates how individual human observations of someone in public give rise to information which is ‘sparse and disjointed’ and hence, unlike digital information which ‘can be stored and conjoined’, does not threaten privacy.⁷⁴

As will be discussed in the next chapter, technology, and particularly surveillance technology, changes the privacy and anonymity of public spaces. At the same time, technologies are rapidly being introduced into our homes, cars and phones that break through the physical barrier of *private* spaces.

⁷⁰ These interactions primarily are studied in sociological research. Goffman was influential in this area: see Smith, “Interaction in Public Spaces.”

⁷¹ Veliz calls this our *autopos*: Carissa Veliz, “In the Privacy of Our Streets,” in *Surveillance, Privacy and Public Space*, ed. Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops (Oxford: Routledge, 2020). p.20

⁷² See for example; Ali Madanipour, *Public and Private Spaces of the City* (London: Routledge, 2003). Chapter 1: pp.5-34

⁷³ Nissenbaum, *Privacy in Context*. p.117

⁷⁴ Ibid. pp.117-8

5.2 THE ARGUMENTS FOR NOT EXPECTING PRIVACY IN PUBLIC SPACES

There seems to be a widespread view that we don't have a right to privacy in public spaces. This position unfortunately sanctions everything from the proliferation of CCTV cameras to our image being captured on strangers' mobile phones.

There are two similar, but distinct, arguments that appear to underline this position:

The "Privacy = Lack of Observation" argument:

- i. Privacy = Not being observed
- ii. Being in a public space => You can be observed
- iii. Therefore: Being in a public space => You cannot expect privacy

The "Private = Secret" argument:

- iv. Privacy = Keeping information secret
- v. Being in a public space => What you are doing cannot be secret
- vi. Therefore: Being in a public space => You cannot expect privacy

These arguments can be challenged on a number of grounds:

- Privacy is more than simply not being observed.
- What constitutes "being observed" is not a simple, well-defined activity.
- Privacy is not synonymous with secrecy

Compare:

- a) A person while walking down the street sees you walking along the opposite pavement and "observes" you.
- b) A person sees you sitting at a table outside a café and then stands for 30 minutes "observing" you by staring at you.

Surely the nature of "observe" is different between the two cases and in a) clearly doesn't invade your privacy while in b) clearly does? Yet, both are examples of you being observed in a public space.

- c) If the person in b) starts writing down in a notebook everything he sees you doing, then this would qualify as an even greater invasion of my privacy.

Likewise, if

- d) He takes out his mobile phone and starts live-streaming images of you on Instagram; your privacy is even further invaded.

These examples show that privacy is concerned with far more than simple observation. Many discussions of privacy in the philosophical literature use the example of a peeping Tom and how his actions breach one's privacy through the act of observing one without one's knowledge. Unfortunately, the widespread use of such examples tends to reinforce the view that having privacy simply means not being observed.

5.3 RESPECTING THE PRIVACY OF OTHERS IN PUBLIC SPACES

While much of the foregoing discussion has related to intrusions into privacy in public spaces one should also consider the role of the individual in their interaction with others when in public. Valiz discusses the duty we have to respect other's privacy.⁷⁵ She talks about having a *duty of ignorance* – refraining from seeking personal information – and a *duty of silence* – not divulging personal information. The former includes:

- Looking away
- Not asking invasive questions
- Refraining from collecting personal data
- Refraining from making invasive inferences

While these are primarily concerned with the analogue world of physical contact and interaction, the same principles could apply to the use of digital technology, for example mobile phone cameras and social media.

⁷⁵ Véliz, *The Ethics of Privacy and Surveillance*. pp.160-173

6. THE IMPACT OF TECHNOLOGY ON PRIVACY

“Our attention, our activities, our locations, our desires—everything about us that we revealed, knowingly or not, was being surveilled and sold in secret, so as to delay the inevitable feeling of violation that is, for most of us, coming only now. And this surveillance would go on to be actively encouraged, and even funded by an army of governments greedy for the vast volume of intelligence they would gain.”

Edward Snowden (2019)⁷⁶

Technology advances have impacted all aspects of the informational privacy sphere. Observation capabilities have proliferated with CCTV, smartphones, smart doorbells, car GPS, dashcams, police bodycams, fitness trackers, smart speakers, browser trackers and cookies. Storage costs have consistently dropped such that ever-greater amounts of data can be stored at diminishing cost.⁷⁷ Processing costs have reduced dramatically, and capacity increased through parallel processing technologies. Facial recognition technology enables anonymous data from CCTV or photographs to be indexed and to be accumulated for an individual.⁷⁸ Artificial Intelligence makes the scanning of large quantities of information to gain insights more practicable on a large scale. Network capacity and interchange standards such as XML and JSON enable sharing of data across disparate systems and organisations.⁷⁹ Data distribution capabilities have grown: high speed global data connections between data centres and to peoples’ homes are the norm. Platforms such as Instagram, Facebook and X provide for near instantaneous transmission across the globe.

⁷⁶ Edward J. Snowden, *Permanent Record* (London: Macmillan, 2019). Preface.

⁷⁷ The Amazon example, discussed later in this chapter, highlights how storage costs are no inhibitor to organisations storing vast amounts of personal data.

⁷⁸ Facial recognition technology does not appear in books or papers about privacy until about 2000 and significant concern dates from the 2010s and active opposition in the 2020s – see e.g. Big Brother Watch, “Stop Facial Recognition.”
On transaction costs of facial recognition see Evan Selinger and Brenda Leong, “The Ethics of Facial Recognition Technology,” in *Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford University Press, 2023). pp.603-4

⁷⁹ As early as 1965 Westin identified data sharing as a key threat to privacy: Westin, *Privacy and Freedom*. p.117

Veliz argues that the very fact of digitisation leads to surveillance; for example, when you use a digital map compared with an analogue map a trace of your activity and location is captured.⁸⁰

6.1 TECHNOLOGY IN PUBLIC SPACES

Timan describes the way that a multitude of emergent technologies coupled with increased private ownership or management of public space is leading to a loss of privacy in public spaces.⁸¹

CCTV has been in use for many years but has proliferated in recent years. There has also been a change in usage from what could be called passive monitoring where CCTV footage is stored for subsequent analysis, for example in the case of a crime, to active real-time use of the systems coupled with facial recognition to actively identify individuals.⁸² This is being used in by official bodies during demonstration monitoring and by private companies tracking potential shoplifters.⁸³

The concept of Goffman “territories” was mentioned earlier: spaces – both physical and informational – that are claimed by individuals as they move around public places such as parks and streets or semi-public areas. Technologies such as CCTV, a stranger’s smartphone photography or a police bodycam disrupt the rules or conventions that previously enabled privacy within such territories.

Street photography involving the taking and distribution of photographs of people in public without their consent is contentious. The legal position varies by country, as discussed in a later section, but the moral position is also disputed and supporters of the right to take such photographs often fall-back on the *no right to privacy in public places* argument. Critics of the genre often reference autonomy or respect

⁸⁰ Véliz, *The Ethics of Privacy and Surveillance*. pp.182-4

⁸¹ Timan, "Conclusion: The Need for Privacy in Public Space."

⁸² Big Brother Watch, "Biometric Britain," (2023). <https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf>.

⁸³ Danielle Herbert, "Man 'branded a thief' after shop's facial recognition error," (2025). <https://www.bbc.co.uk/news/articles/c3vn4p1lwqno>.

for the individual to support their view that artistic freedom arguments don't trump individuals' rights to privacy.⁸⁴

A recent movement in the UK tried, unsuccessfully, to get legislation enacted to force retailers to accept cash payments and prohibit card-only operations.⁸⁵ Their motivation was a mixture of concerns about sections of the population being disenfranchised through to a concern about state control. An ongoing movement is lobbying against government plans for digital currencies.⁸⁶ One key aspect of the cash-less society is that it makes anonymity in public harder to achieve and makes it almost impossible to go "off-grid".

Individuals are also directly contributing to a reduction of their own privacy in public spaces by their use of devices that include location tracking technology such as smartphones, fitness trackers and satnav in cars.⁸⁷ Location tracking of individuals blurs further the distinction between public and private space; the technology is agnostic as to whether the user is at home, at work, at a leisure centre or on a public street.⁸⁸

Veliz stresses the importance of privacy on public streets and the threat to this privacy from technology.⁸⁹ In addition, she makes the point that rising house prices in many cities have forced the younger generation into either living at home with

⁸⁴ See John Hadley, "Street Photography Ethics," *Ethical theory and moral practice* 25, no. 4 (2022). and Bell, "Wronging Persons Through Photographs: On Photographic Front Incursions." (2025)

⁸⁵ Hansard, "Cash Acceptance - Volume 730: debated on Monday 20 March 2023," 2023, <https://hansard.parliament.uk/commons/2023-03-20/debates/187CA19F-E3A9-48B1-B40A-869CB673F4A1/CashAcceptance>.

⁸⁶ Cash is Freedom, "Join Our Campaign Against Programmable Digital Currency," 2025, <https://www.cashisfreedom.uk/>.

⁸⁷ An example of data derived from fitness trackers was the location of military bases. Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases," *The Guardian* (28 Jan 2018). <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>.

⁸⁸ The Chinese state seems to have gone farthest in accumulating data across multiple platforms and locations to track people's movements See Brian Spegele, "China's Surveillance State Pushes Deeper Into Citizens' Lives," *Wall Street Journal* (New York), Oct 19th 2022.

⁸⁹ Veliz, "In the Privacy of Our Streets."

parents or sharing accommodation with others and therefore they have a greater need for the ‘privacy of the streets’.⁹⁰

6.2 TECHNOLOGY IN PRIVATE SPACES

Technology is breaking down the traditional privacy that an individual had while in their private residence. The messages and emails they are sending, the eBook they are reading, the website they are visiting, the TV programme they are watching, the items they are perusing in an online store are all visible to the technology providers and much of this information is also shared with third parties. Smart speakers are constantly monitoring conversations to identify commands.

Smart Heating systems link to one’s mobile phone to automatically recognise when one is away from one’s home and when approaching it again to set the thermostat temperature accordingly: potentially a benefit in convenience, comfort and heating costs but at the expense of an external system/organisation knowing whether anyone is home.⁹¹ This is a technology that is focussed on private space, the home, but also monitors one’s whereabouts in public space.

I recently downloaded all of the data that Amazon holds about me.⁹² I have been a customer for 25 years and it holds details of:

- Every product I have purchased, added to my basket but removed, or returned
- Every audiobook I have purchased and whether I finished listening to it
- Every piece of music I have listened to via music streaming
- Every eBook I have purchased and the start and end times of every reading session
- Every request I have made to my smart speakers (both the audio and the transcripts are stored)
- Every photo I have taken with my smartphone⁹³

⁹⁰ Ibid. p.30

⁹¹ A technology called “geofencing”. See Lab43, "Geofencing: The Smart Home Game Changer," 2025, <https://lab53.uk/geofencing-the-smart-home-game-changer/>.

⁹² A service that online organisations must by law provide if requested. It is usually available within the privacy section of the account settings for a website. The total volume of information held about me by Amazon was over 3GB of data.

⁹³ Amazon services involved are: Amazon shopping, Audible, Amazon Music, Kindle, Echo and Amazon Photos.

And for each of these it records when and on which device (computer, phone, tablet etc.) the activity occurred.⁹⁴ The detail of the picture that this wealth of data draws about me, my life and my preferences is frightening.⁹⁵ Whilst it can be argued that I must have consented, at some time, to this data being held, I was not aware of the full extent of data being collected and stored: for example I had no idea that every exchange with my Alexa smart speakers was recorded and stored indefinitely.

Even for someone like myself who is relatively concerned about privacy and is highly technologically literate the sheer power of data analysis, sharing and use constantly surprises me.⁹⁶ In 2024, I was diagnosed with diabetes and naturally researched the topic online. It was only days before my Instagram feed was featuring books, diets and quack remedies related to diabetes. My only surprise is that I haven't been inundated with adverts for stomach remedies given my grandchildren's predilection to ask the Alexa smart speakers to "make fart noises" or to sing "poo songs".⁹⁷

Technology in private spaces can break down the physical barriers of those spaces and open up your activities to public view without you being directly involved in the process by which this happens. Consider the situation where you are attending an event, such as a party, at a private venue or in a private home. Another attendee captures pictures on their phone and posts this on social media. While you are clearly exposing part of your personal space to the other attendees by being present at the event, you have not consented to that information being broadcast to the world at large. Not only are the photographs now public but it is likely that someone may have *tagged* you in them such that your identity is also broadcast without the need

⁹⁴ To give an idea of the detail held, I can tell that: on 19th January 2018 between 00:09 and 00:23 my wife read an eBook - *Pachinko* by Min Jin Lee - on her Kindle (Kindle Paperwhite 7th Generation) and during that time turned over 32 pages.

⁹⁵ A similar data dump from Google revealed not only every search I had made but included, amongst other items, every location I had looked up on Google Maps or asked for directions to during the last 15 years. I subsequently restricted Google to only store data for the last 90 days.

⁹⁶ In the 1990's the author worked as an IT Consultant specialising in Customer Relationship Management in the global retail sector and his work included leading a team analysing data on customer purchases at a large UK high street retailer which had launched a highly successful loyalty card.

⁹⁷ The data held by Amazon allows me to see one such interaction during the 2022 Christmas holidays: 'Request: "alexa play poo in your pants", response: "Here's Poo in the Pants, by Lil Young Old Man, on Amazon Music." Alexa transcript; 28/12/2022 11:39:56'

for technologies such as facial recognition. People are becoming so used to sharing images that they often don't stop to think whether the subjects may not want their image shared.⁹⁸

A surveillance review as far back as 2015, a long time in information technology terms, reported that up to 95% of intelligence collected by intelligence agencies originated from open, rather than closed, sources; an indication of the amount of information that can be gleaned from calls, texts and social media data generated by individuals.⁹⁹ Even when individuals are vigilant in their security settings, the fact that these vary from platform to platform and are regularly subject to change means that more personal data is made available than most users think is the case.¹⁰⁰

6.3 TECHNOLOGY AND PRIVACY IN THE WORKPLACE

While the emphasis has been on privacy in either public or private residential spaces, there is a third type of space not discussed so far: the workplace. This differs from the former two in that there has always been less expectation of privacy in workplace settings. Even here, however, technology has reduced privacy even further.¹⁰¹ There is not room here to fully explore this area, but there are two major concerns regarding digital technologies in the workspace:

- Surveillance
- Automated, algorithmic performance assessment¹⁰²

The first is clearly similar to the privacy issues discussed earlier but the second represents a different category of technology impact, i.e. upon personal autonomy. As well as performance assessment, there is increasing use of AI systems, often

⁹⁸ Kaspersky, "Social Media Privacy and Prevention," 2025, <https://www.kaspersky.com/resource-center/definitions/social-media-privacy>.

⁹⁹ Royal United Services Institute, "A Democratic Licence to Operate: Report of the Independent Surveillance Review," (13 July 2015). https://static.rusi.org/20150714_whr_2-15_a_democratic_licence_to_operate.pdf. 3.16

¹⁰⁰ Lilian Edwards and Lachlan Urquhart, "Privacy in public spaces: what expectations of privacy do we have in social media intelligence?," *International journal of law and information technology* 24, no. 3 (2016). p.296

¹⁰¹ John Weckert, *Electronic Monitoring in the Workplace: Controversies and Solutions* (Hershey, PA: Idea Group Publishing, 2004).

¹⁰² Ebert, Wildhaber, and Adams-Prassl, "Big Data in the workplace."

with ethnic or gender biases, for recruitment screening.¹⁰³ Potential employees now also, routinely, have their social media histories screened by employers. Experian, for example, offer this as a service.¹⁰⁴

‘Almost every applicant, for every job role, has a sizeable social media presence. Spanning everything from well-known platforms like Facebook, YouTube, Twitter and TikTok, to more niche services like gaming sites. These accounts provide a wealth of information about an applicant’s beliefs, attitudes and behaviours.’

6.4 FUTURE TECHNOLOGIES AND PRIVACY

One of the biggest challenges in discussing both the ethical and the legal aspects of privacy related to data collection, processing and distribution is the speed with which technologies can evolve from concepts, through prototypes to widespread adoption. Reading Westin’s 1967 work *Privacy and Freedom* one is struck by the almost quaint nature of the technology discussed in this seminal, but pre-PC pre-Internet pre-smartphone, work.¹⁰⁵ Despite this, he clearly sees the emerging dangers to privacy from technologies ranging from large scale databases to the expanding use of credit cards.¹⁰⁶ Oscar Reubhausen, chairman of the committee that sponsored Westin’s work, remarked that:

‘The rapidly developing capability to observe, record, and broadcast observations that are conventionally assumed to be private was thought to signal some problems of potential concern. Of paramount importance was the challenge perceived to individual privacy.’¹⁰⁷

¹⁰³ Jennifer King and Caroline Meinhardt, "Rethinking Privacy in the AI Era," *Human Centered Artificial Intelligence* (February 2024). <https://hai.stanford.edu/assets/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf>. p.26

¹⁰⁴ Experian, "Social media checks – what are they and why are they important?," updated Jan, 2021, <https://www.experian.co.uk/blogs/latest-thinking/background-checks/social-media-checks-what-are-they-and-why-are-they-important/>.

¹⁰⁵ He does discuss the threats to privacy of the then emerging technology of “TV Eyes” (CCTV) and videotape recorders. Westin, *Privacy and Freedom*.pp.75-77

¹⁰⁶ Ibid. pp.176-184.

¹⁰⁷ Ibid.pp.xii-xiv

The rapid rise of Artificial Intelligence poses many concerns regarding privacy but, in many ways, the biggest threat is that it makes the analysis of vast reams of data economically viable. The exponential growth of data held about individuals by technology companies perhaps itself partially protected the privacy of the individual; there was simply too much data for even the best algorithms to digest beyond simple segmentation for target marketing and personalised advertisements. With AI the large volume of data is an aid rather than a hinderance and the insights that can be derived by the combination of AI and the data repositories threaten a much deeper profiling of individuals whether for marketing or for political manipulation.¹⁰⁸ Data analysis, aided by AI developments, is starting to affect privacy in public areas through, for example, automated profiling of people observed on CCTV in areas such as shopping malls.¹⁰⁹

A rare case of a technology seemingly being held back by privacy concerns was that of wearable smart glasses incorporating cameras, recording information and presenting information to the wearer in real-time. *Google Glass* had widespread publicity back in 2012-14 but didn't make it into full production.¹¹⁰ Only a version developed for selected workplace use was developed into a commercial product.¹¹¹ However, that victory for privacy may be short lived; there has been an explosion of product announcements and releases of similar technology in the last couple of years. Examples come from Oakley, Rayneo and a partnership between RayBan and Meta. The latter is advertised with the promise that you can:

¹⁰⁸ The Cambridge Analytica scandal illustrates this only too well. Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian*, 17 March 2018.

¹⁰⁹ Olivia Campbell, "Using AI to Detect Suspicious Behavior in Shopping Malls," Arcadian.ai, 2024, <https://www.arcadian.ai/blogs/blogs/using-ai-to-detect-suspicious-behavior-in-shopping-malls>.

¹¹⁰ The implications of Google Glass for privacy are explored in Olya Kudina and Melis Bas, "The end of privacy as we know it," in *Surveillance, Privacy and Public Space*, ed. Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops (Oxford: Routledge, 2020).

¹¹¹ Charles Arthur, "Google Glass: is it a threat to our privacy?," *The Guardian*, 6th March 2013.

‘Capture exactly what you see and hear with the new ultra-wide 12 MP camera and five-mic system. Take high-quality photos and immersive videos and share it all to Facebook and Instagram. Toggle between your phone and glasses camera when you videocall or livestream, so that everyone can experience your unique view of the world.’¹¹²

Another potential privacy concern relates to the gathering of DNA. In particular, the rapidly reducing costs of DNA analysis may make it possible for law enforcement or government officials or private commercial interests to identify and track individuals through the DNA traces they leave everywhere they go. Albert Scherr, an authority on forensic DNA evidence, discusses the privacy and legal issues raised by this “out-of-body” DNA analysis.¹¹³ Not only can the DNA identify individuals, but it can also provide extensive information, such as medical conditions, about them. Apart from DNA records kept by law enforcement agencies there are large databases of individuals’ DNA in the records of companies offering ancestry tracing: *23andMe*, *AncestryDNA* and *MyHeritage* together hold some 50 million individuals’ DNA records:¹¹⁴

There are optimists who believe that technology may evolve in a way that enables individuals to protect their privacy. Back in 2005, Doyle and Bagaric argued that:

‘As to the threats posed by the monitoring capabilities of the new information technologies, it is now becoming apparent that technology itself can provide the means to counter them.’¹¹⁵

¹¹² RayBan Meta, "Ray-Ban | Meta Wayfarer," 2025, <https://www.ray-ban.com/uk/electronics/RW4006ray-ban%20%20meta%20wayfarer-black/8056597988377>.

¹¹³ Albert Scherr, "Privacy in Public Space: The Problem of Out-of-Body DNA," in *Privacy in public space: conceptual and regulatory challenges* (Cheltenham, UK: Edward Elgar Publishing, 2017).

¹¹⁴ Megan Prictor, "A giant biotechnology company might be about to go bust. What will happen to the millions of people's DNA it holds?," *The Conversation* (2024). <https://theconversation.com/a-giant-biotechnology-company-might-be-about-to-go-bust-what-will-happen-to-the-millions-of-peoples-dna-it-holds-241557>.

¹¹⁵ Carolyn Doyle and Mirko Bagaric, "The right to privacy: appealing, but flawed," *The international journal of human rights* 9, no. 1 (2005).

Likewise, in 2009, Holvast discussed the benefits of *Privacy Enhancing Technologies*.¹¹⁶ However, I tend to agree with Cohen who, while wishing such developments were going to be effective, regards it as very unlikely.¹¹⁷ The developments of the last 15-20 years do not seem to be on the side of the optimists.

An invidious aspect of many of the technologies discussed in this chapter is how easily we can be bribed to agree to the collection of data. As well as the many examples of loyalty cards or acceptance of cookies on websites there are less obvious ones: for example, by agreeing to a black box in your car that monitors and reports your driving habits you may get a reduced car insurance premium. Nissenbaum raises the apparent paradox that people, when asked, consistently say they are concerned or very concerned about privacy, but then 'In almost all situations where people must choose between privacy and just about any other good, they choose the other good.'¹¹⁸ She counters with the argument that most of the time the choices are either not truly choices or we don't have the full picture of what data is collected and how it will be used.

The following section discusses how we are ill-equipped to make judgements regarding the trade-offs between convenience and privacy that are implicit in the use of many technologies

¹¹⁶ Jan Holvast, "History of Privacy" (paper presented at the The Future of Identity in the Information Society, Berlin, Heidelberg, 2009// 2009). pp.34-5

¹¹⁷ Julie E. Cohen, "Privacy, ideology, and technology: A response to Jeffrey Rosen," *The Georgetown law journal* 89, no. 6 (2001). p.2042

¹¹⁸ Nissenbaum, *Privacy in Context*. p.105

7. THE IMPOSSIBILITY OF MAKING RATIONAL DECISIONS REGARDING CONSENT

“Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others...”

Alan Westin (1967).¹¹⁹

Karsten Mause makes an interesting point about technologies such as surveillance, but applicable to many other technologies, in that we make, consciously or subconsciously, economic trade-offs during decision making.¹²⁰ In privacy terms this can mean that we judge the benefit we receive against the cost associated with divulging information. Unfortunately, if we do not know the extent of, in the cited case, surveillance and how the information so obtained is being used then we cannot make rational judgements about our actions.

As a student in the 1980s you could make a rational decision about buying a risqué magazine: what were the chances of someone who knew you seeing you buy the magazine from the newsagent set against the benefit you would gain from the purchase? In the modern online world, a current-day student visiting a soft porn website or sharing a nude photograph on Instagram has no way of judging the risks they are taking: from identity theft through to blackmail. They are unable to rationally make the risk-reward decisions that are fundamental to many of our activities.

Solove argues that existing mechanisms fail to provide the user with real control.¹²¹ Consent and Opt In/Out terms on websites and applications often seem designed to make the user simply accept the use of their data, or the T&Cs are so voluminous that few users will bother to read them all. In any case, the T&Cs may be frustratingly opaque, despite regulations such as the *General Data Protection*

¹¹⁹ Westin, *Privacy and Freedom*. pp.5-6.

¹²⁰ Karsten Mause, "A politico-economic perspective on privacy in public spaces," in *Privacy in public space : conceptual and regulatory challenges* (Cheltenham, UK: Edward Elgar Publishing, 2017).

¹²¹ Daniel J. Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law," *Boston University law review* 104, no. 2 (2024).

Regulation (GDPR). When a website asks if it may share data with selected third parties, one has no idea whether that is one or two or scores of organisations and whether they are related to the focus of the original site or are simply any organisation that will pay them referral fees. GDPR type regulations can also backfire: by making users opt in/opt out so frequently they become inundated and cannot realistically assess each request on its merits.¹²² There also seems to be a trend for websites to adopt an ‘allow all use of data’ or ‘pay for access’ approach. In other words, agree to everything or else pay to access the site.

As Edwards notes:

‘Even in the simplest case, where the data subject themselves has knowingly disclosed substantive, personal data about themselves, it is simply not credible to argue that accepting standard terms and conditions on a social media site, typically buried under an obscurely placed hyperlink, negates any kind of expectation of privacy. such “consent” to fixed unilaterally imposed terms and conditions is neither free, specific nor informed ... and has become effectively illusory.’¹²³

Although initiatives such as GDPR do make some steps towards giving the user (the consumer) protections and controls on what data is collected and how it is used, the asymmetries in the consumer-organisation relationship significantly reduce the effectiveness of such legislation.¹²⁴ Solove argues that all attempts to manage privacy through what he call ‘privacy self-management’ are ultimately doomed to fail and that privacy law needs to ‘focus on regulating the architecture that structures the way information is collected, used, and transferred.’¹²⁵

Veliz makes the point that even if I read and understand the T&Cs and consent then that consent should only apply to the data that is strictly relevant to me alone.¹²⁶ By

¹²² King and Meinhardt, "Rethinking Privacy in the AI Era."

¹²³ Edwards and Urquhart, "Privacy in public spaces." p.306

¹²⁴ Peter J. van de Waerd, "Information asymmetries: recognizing the limits of the GDPR on the data-driven market," *Computer Law & Security Review* 38 (September 2020), <https://www.sciencedirect.com/science/article/pii/S0267364920300418>.

¹²⁵ Solove, *On Privacy and Technology*. pp.90-91

¹²⁶ Véliz, *The Ethics of Privacy and Surveillance*.p.207

sharing material that includes personal data about my friends or family – stories, photographs, location information etc.- then I am giving that data to a third party without the consent of the person who is the subject of the data. This is also discussed by Edwards and Urquhart: ‘For intelligence purposes, one of the most useful pieces of data that can be extracted from a social media profile is the network of friends or ‘social graph’¹²⁷

Veliz further discusses that data accumulation can lead to correlations and inferences that I cannot foresee when I consent to the sharing of individual items of data.¹²⁸ Elsewhere, she observes that the extent of data collection on individuals through today’s technology far exceeds anything the Stasi collected on East Germany citizens during the Cold War era.¹²⁹

A shopping centre may have a sign up saying that CCTV is operational within the location. But, I have no way of knowing what they may be doing with the captured footage: how long they storing it for, if they are using facial recognition, or whether they are sharing data with others? I have no data on which to assess whether the benefit of entering the centre offsets the potential loss of privacy. The lack of data about who is capturing data and what is being captured also means I cannot make decisions about how to moderate, or not, my behaviour.¹³⁰

Many commentators describe the loss of privacy as *Orwellian* and recall the world of *Big Brother*. A key difference between the world of 1984 and our world is that in Orwell’s novel the citizens knew that they were being observed and that there was no escape from that observation and that Big Brother knew everything about their activities. The modern, real world is more *Kafkaesque* (as in *The Trial*): we don’t know what is being observed, or by whom, or how that information is being used and that makes us powerless to take control of the situation.¹³¹

¹²⁷ Edwards and Urquhart, "Privacy in public spaces."

¹²⁸ Véliz, *The Ethics of Privacy and Surveillance*. p.207

¹²⁹ Carissa Véliz, "The Surveillance Delusion," in *Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford University Press, 2023). p.557

¹³⁰ Benjamin J. Goold, "Privacy rights and public spaces: CCTV and the problem of the "unobservable observer"," *Criminal justice ethics* 21, no. 1 (2002). p.24

¹³¹ Solove, *Nothing to Hide*. pp.25-6

8. THE NOTHING TO HIDE ARGUMENT

“If these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing.”

Henry James (1888).¹³²

It is often argued that if one has nothing to hide then one has nothing to fear from surveillance techniques such as CCTV cameras.

This ignores two important aspects of privacy:

- The complex nature of privacy
- Private information is different from secret information.

Solove argues that the *Nothing to Hide* argument ‘represents a singular and narrow way of conceiving of privacy’.¹³³

Something can be private without it being secret.¹³⁴ Suppose I send an e-mail to my brother saying how pleased I was to see him last month. This is not secret. I am not concerned to encrypt it. I do not regard it as a secret. However, if that e-mail is intercepted by a hacker who is monitoring my e-mail system, then I would regard my privacy as having been infringed.

My health data is not secret; it is widely available to medical professionals by whom I have been treated and by the administrative staff at my GP's surgery who handle prescription renewals. If my garage mechanic asked me for that information I wouldn't reply “It's secret” I would reply “It's private, it's none of your business”. If a close friend asks about my medical condition, then I may or may not choose to share the information. If I don't wish to share the information, I am likely to say that “I prefer to keep the information private” not “It's a secret”. This not only

¹³² Henry James, *The Reverberator* (New York: Macmillan, 1888). p.209.

¹³³ Solove, *Nothing to Hide*.

¹³⁴ For a discussion of the semantic distinctions between privacy and secrecy see: Roessler and DeCew, "Privacy." pp. 22-23

shows there is a distinction between secrets and private information but also highlights how disclosure of the latter is dependent upon context.

Suppose I go shopping and buy my wife a birthday present. I am walking back to my car and meet a neighbour who, seeing my shopping bag, asks if I have bought anything special. I exercise my right to keep my shopping habits private and don't disclose what I have bought. It is private information. However, when I get home my wife sees I have been shopping and asks what I have bought, but this time my response isn't to say it's "private" but rather to say that it is "a secret".

In general, a desire for secrecy is more directly related to the consequential impacts of disclosure while desire for privacy is about autonomy and control of personal information. The *Nothing to Hide* argument is essentially a consequential argument about the individual: disclosure has no harms if you have nothing to hide. It is more about secrecy than about privacy and therefore doesn't, of itself, justify invasions of personal privacy.

Also, even when looked at from a consequentialist point of view there are societal benefits from privacy: Rachels argues that control of our personal data and control of with whom and when we share such data is fundamental to the maintenance of the many different relationships we have in life: from family, through close friends, acquaintances, co-workers, doctor, strangers etc.¹³⁵ A German Federal Court ruling makes a similar point:

‘A societal order, and its underlying legal order, would not be compatible with the right to informational self-determination if citizens were no longer able to tell who knows what kind of personal information about them, at what time and on which occasion’¹³⁶

Roessler and DeCew express a similar summary of writings by Erving Goffman and Anita Allen:

¹³⁵ Rachels, "Why Privacy is Important."

¹³⁶ Federal Constitutional Court, *Judgment of 15 December 1983*, Bundesverfassungsgericht (Germany, 1983), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Section 146.

‘The social freedom to play different roles is dependent on being able to present oneself differently to neighbors, students, one’s spouse. It is dependent on the protection of privacy.’¹³⁷

On surveillance technology in general and the *Nothing to Hide* argument in particular, the UK Surveillance Camera Commissioner’s Office says:

“Of the many arguments deployed in the defence of surveillance technology there is one that doesn’t just miss the point: it misses all of them. Beguilingly simple, the expression “if you’ve done nothing wrong you’ve nothing to worry about” is, of course, not the answer to legitimate public concern over surveillance; it’s not even an answer. There are many reasons why - the absence of logical merit, ethical legitimacy and legal validity being but three.”¹³⁸

Despite the arguments against the *Nothing to Hide* defence of surveillance it is all too often used in public debate and seems to strike a chord with the public:

‘These results certainly indicate a British leaning towards the line of “nothing to hide, nothing to fear”, and perhaps towards seeing online law enforcement as essentially akin to offline. In a question on which statement best describes current surveillance law, 47% said it “generally makes us all safer and is only something to worry about if you are doing something illegal”.’¹³⁹

and

‘The most common retort against privacy advocates - by those in favor of ID checks, cameras, databases, data mining and other wholesale

¹³⁷ Roessler and DeCew, "Privacy." p.33

¹³⁸ Surveillance Camera Commissioner’s Office, ““If you’ve done nothing wrong...”: 5 Reasons Why This is No Defence for Surveillance,” UK Government, updated 27 May, 2021, <https://videosurveillance.blog.gov.uk/2021/05/27/if-youve-done-nothing-wrong-5-reasons-why-this-is-no-defence-for-surveillance/>.

¹³⁹ Dr Joel Rogers de Waal, "Security Trumps Privacy in British Attitudes to Cyber-Surveillance," YouGov, 2017, <https://yougov.co.uk/politics/articles/18362-Security-Trumps-Privacy>.

surveillance measures - is this line: "If you aren't doing anything wrong, what do you have to hide?"¹⁴⁰

¹⁴⁰ Bruce Schneier, "The Eternal Value of Privacy," 2006,
https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.

9. LEGAL APPROACHES TO PRIVACY

“One of the most difficult questions facing English courts ... is whether and, if so, when a person might have a reasonable expectation of privacy in a public place.”

Moreham (2006) ¹⁴¹

When analysing how the Law regards privacy, one is faced with the fact that there is a diversity of different national legal frameworks. This suggests there is no simple answer to the underlying ethical considerations of privacy in public spaces. For example, considering *street photography*: in the USA one can generally publish people’s photographs taken in public spaces without their consent while in France such actions are, with exceptions, against the law.

UK Law is inconsistent in its approach to the distribution of data obtained in public spaces: if I record a video of you in the street and publish it I am generally not breaching the law (unless the video contains sexual or intimate content) but if I make an audio recording of you and publish that without your consent then I could be breaking the law.¹⁴²

The American legal system generally treats activities taking place in public as not being protected by privacy considerations unless material gathered, such as photographs, is used for commercial purposes. There is a view that, in general, the law in the USA has a greater focus on decisional privacy rather than informational privacy.¹⁴³

German law tends to support privacy, as a 1983 judgement, describing *informational self-determination*, illustrates:

¹⁴¹ N. A. Moreham, "Privacy in Public Spaces," *Cambridge law journal* 65, no. 3 (2006). p.606.

¹⁴² Information Commissioner's Office, "How can we comply with the data protection principles when using surveillance systems?," 2025, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/>.

¹⁴³ Roessler and DeCew, "Privacy." pp.11-13

‘If individuals cannot, with sufficient certainty, determine what kind of personal information is known to certain parts of their social environment, and if it is difficult to ascertain what kind of information potential communication partners are privy to, this could greatly impede their freedom to make self-determined plans or decisions.’¹⁴⁴

Legislation can support the view that an activity which is not illegal as a single instance could be illegal if repeated if it thereby constitutes harassment or stalking. This is parallel to the view that observing a single activity of mine may not be a breach of privacy but recording multiple activities over time could be. However, when it comes to privacy, legislation generally tends to only consider whether each one-off capture of data is legitimate.¹⁴⁵

A particular problem for legal systems is that it is difficult for laws, and the law-making process, to keep up with the pace of technology developments.¹⁴⁶ It is difficult to define laws that are general enough to apply to new technologies without them being too vague to be useful and more specific laws tend to fall behind the changes in technology.

There are also anomalies that result from the way that laws are developed and adapted to changing circumstances. For example, in the USA, there are less stringent laws regulating government access to your emails residing on Google’s servers compared with while they are in transit over the phone lines.¹⁴⁷ This derives from laws regarding wiretapping applying in the latter case but not the former.

Solove comments how the law tends to treat privacy in a ‘simplistic, binary way: personal data is either secret or exposed’ – what he terms the *secrecy paradigm*.¹⁴⁸

¹⁴⁴ Federal Constitutional Court, *Judgment of 15 December 1983*. Section 146

¹⁴⁵ Solove, *On Privacy and Technology*. p.37

¹⁴⁶ Philip Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape* (Cambridge, Mass.: MIT Press, 1997). p.213

¹⁴⁷ Solove, *Nothing to Hide*. pp 167-8.

¹⁴⁸ Solove, *On Privacy and Technology*. p.30

He sees privacy as more complex than this and rather than people keeping personal data *secret* it is more about them setting boundaries that ‘modulate the flow of data’.

Data protection laws such as GDPR are useful in curtailing some of the worst abuses of the collection and use of personal data but have limited overall success; partly because of the problems with consent-based approaches discussed earlier and partly because they struggle with the impact of new technologies. Even the European Data Protection Board, who administer GDPR, concedes that consumers suffer from fatigue from multiple consent requests:

‘In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing This results in a situation where consent questions are no longer read.’¹⁴⁹

Even if strong legal constraints or regulations govern the use of personal data, and organisations follow both the letter and the spirit of such legislation, there is the ever-present danger of data breaches exposing that data.¹⁵⁰ As well as large scale publicised incidents, such as that at NPD in 2024, there are numerous often unreported smaller scale breaches.¹⁵¹ In 2024, 5,000 customers’ banking details were accessed by a breach of London Transport’s systems and in another incident, data on 25,000 former BBC employees, including National Insurance numbers,

¹⁴⁹ European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679," V1.1 (4th May 2020).
https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Sect. 88-89

¹⁵⁰ There are reports that data on 1 billion Chinese citizens was hacked from government databases. Karen Hao, "China Has a Problem With Data Leaks. One Reason Is Its Surveillance State," *Wall Street Journal* (New York), July 21st 2022.

¹⁵¹ "National Public Data, an online background check and fraud prevention service, experienced a significant data breach. This breach allegedly exposed up to 2.9 billion records with highly sensitive personal data of up to 170M people in the US, UK, and Canada". Microsoft, "National Public Data breach: What you need to know," 2024,
<https://support.microsoft.com/en-gb/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535>.

were stolen.¹⁵² The UK Information Commissioners Office received notification of over 12,000 breaches of data security in 2024.¹⁵³ While the single largest category was a result of emails being sent to the wrong recipient, “unauthorised access” accounted for 12% of breaches. In 2025, notifications of breaches are running 6% up on 2024.

¹⁵² James Warren, "Boy arrested over London transport cyber hack," BBC, updated 12 September, 2024, <https://www.bbc.co.uk/news/articles/c4gqg2elkj4o>.

and
Josh Halliday, "Data breach exposes details of 25,000 current and former BBC employees," *The Guardian*, 29th May 2024.

¹⁵³ Information Commissioner's Office, "Data security incident trends," 2025, <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/>.

10. CONCLUSION

“Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules—not just for governments but for private companies.”

Bill Gates (2013)¹⁵⁴

The distinction between public and private spaces regarding expectations of privacy has always been somewhat artificial with many examples of privacy being enjoyed in public spaces. Pervasive technology, from CCTV to smartphones, together with the storage, processing and distribution of data from these technologies has further blurred the boundaries. Traditionally private places, such as the home, enjoy less privacy. Public spaces, which once provided the opportunity for anonymity no longer do so. Shopping, whether in physical stores or online now leaves an identity trail of the individual shopper. Your movements in a vehicle are captured on ANPR systems, congestion charge and road toll systems and car parking apps and your movements are recorded by the vehicle itself. Social media platforms could be said to be virtual public spaces, but they contain much private information.

New and emerging technologies further threaten the individual's ability to keep personal data private. While there is much discussion about online privacy, the technologies that intrude upon public spaces get far less attention. The simplistic assumption that we don't have the right to expect privacy in public spaces allows technologies such as CCTV and Facial Recognition to be expanded, apparently without limits in public spaces from high streets to shopping precincts.

Discussions and legislation regarding the capture, storage, processing, distribution and use of personal data need to be based upon considerations of privacy independent of where the “capture” – i.e. observation – takes place. Nissenbaum cautions against regarding “online” as a distinct space as regards privacy since it is

¹⁵⁴ Steven Levy, "Bill Gates and President Bill Clinton on the NSA, Safe Sex, and American Exceptionalism," (Nov 12th 2013). <https://www.wired.com/2013/11/bill-gates-bill-clinton-wired/>.

integrated into our social lives.¹⁵⁵ Solove argues that “privacy is rarely lost in one fell swoop” but is gradually eroded slowly, imperceptibly and only then do we notice it has gone.¹⁵⁶ A similar sentiment is echoed in a 2024 article that discusses how Germany, a country with some of the strongest privacy protection legislation and which opposed *Google Street View* in the early 2010s, has now succumbed to this technology:

‘Like the famous allegory about a frog being slowly boiled alive, privacy violations don’t seem so upsetting when delivered bit by bit over time. One of the world’s most private societies was a longtime holdout to the behemoth that is Google, but it, too, has been boiled.’¹⁵⁷

While we tend to be suspicious of manual recording and accumulation of data we seemingly accept it when considering technology systems. In the earlier example of the neighbour recording your movements their actions seem to be both unacceptable and rather creepy. However, we accept online systems are doing this kind of tracking most of the time. If you visited a physical bookshop and the owner followed you around noting down which sections you visited, which books you took down and how long you spent looking at those books then you probably wouldn’t want to patronise that shop in the future. However, that is precisely the information captured and recorded by online stores such as Amazon and which we accept as normal and acceptable; even if we are uneasy about the level of data captured we seem to regard it as inevitable.

While much of this paper has discussed the threats to privacy from governments and commercial organisations it has also described how the behaviour of individuals can compromise the privacy of both themselves and others. Allen goes

¹⁵⁵ Helen Nissenbaum, "A Contextual Approach to Privacy Online," *Daedalus* 140, no. 4 (2011). p.38

¹⁵⁶ Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide'," *The Chronicle of Higher Education* 57, no. 37 (2011). p.5

¹⁵⁷ PetaPixel, "Germany vs Google: How Street View Won the Privacy Battle in Europe’s Most Private Country," updated March 8th, 2024, <https://petapixel.com/2024/03/08/germany-vs-google-how-street-view-won-the-privacy-battle-in-europes-most-private-country/>.

so far as to suggest that we have, as the title of her lecture describes, ‘An Ethical Duty to Protect One's Own Information Privacy?’.¹⁵⁸

This paper has concentrated upon the threats to privacy and the moral harms arising from them. It has not discussed at any length the instrumental harms caused as a result of those compromises of privacy. Neither has it addressed the potential benefits from, for example, surveillance. A more instrumental, consequential analysis is required to determine whether the price of loss of privacy is outweighed by the personal and societal benefits arising from how personal data is used: whether that is your smartphone map getting you to a meeting place on time or surveillance preventing terrorist acts. What is clear is that partitioning the world into public and private spaces when discussing privacy issues and their trade-offs has, in the information technology age, been rendered largely irrelevant.

On a personal level I have found myself following the same pathway as Carissa Veliz: starting out with an academic interest in the philosophical issues around privacy but with only a moderate personal concern regarding privacy issues but then, as I researched the topic, developing a strong recognition of the growing threats to our privacy and recognising the importance of that privacy.¹⁵⁹ Of course, it may already be too late to reverse the tide of technological intrusion into our lives; we have become too dependent upon smartphones, satnavs, Google, social media etc. to readily give them up in the interest of privacy. In a Lockean sense we, by our very acts of using such technologies, have given tacit consent to the owners and operators of such technology to observe, store, accumulate and use our data. Lobbying groups trying to reverse the trend in CCTV and facial recognition systems have had relatively limited success thereby allowing governments free rein to expand such systems.¹⁶⁰ We may however look back in future years and ask how little we actually gained by giving up so much of our privacy in both public and private spaces.

¹⁵⁸ Anita Allen, "An Ethical Duty to Protect One's Own Information Privacy?," *Meador Lecture in Morality* (2013). https://scholarship.law.upenn.edu/faculty_scholarship/451/.

¹⁵⁹ Véliz, *The Ethics of Privacy and Surveillance*. p.215.

¹⁶⁰ Lewis Lewis Adams and Kathryn Armstrong, "Facial recognition could be used more widely by police under plans," BBC, 2025, <https://www.bbc.co.uk/news/articles/c3r7pwpgeeweo>.

BIBLIOGRAPHY

- Agre, Philip, and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, Mass.: MIT Press, 1997.
- Allen, Anita. "An Ethical Duty to Protect One's Own Information Privacy?" *Meador Lecture in Morality*. (2013). Accessed 18th March. https://scholarship.law.upenn.edu/faculty_scholarship/451/.
- Arendt, Hannah. *The Human Condition*. 2nd ed. Chicago: University of Chicago Press, 1998.
- Arthur, Charles. "Google Glass: Is It a Threat to Our Privacy?" *The Guardian*, 6th March 2013. <https://www.theguardian.com/technology/2013/mar/06/google-glass-threat-to-our-privacy>.
- Bell, Macalester. "Wronging Persons through Photographs: On Photographic Front Incursions." *Journal of ethics & social philosophy* 30, no. 4 (2025).
- Big Brother Watch. "Biometric Britain." (2023). <https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf>.
- . "Stop Facial Recognition." 2025, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>.
- Block Inc. "Privacy Notice for Users Who Do Not Apply or Sign up for a Square Account or Other Services." 2023, https://squareup.com/us/en/legal/general/privacy-no-account?country_redirection=true.
- Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, 17 March 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- Campbell, Olivia. "Using Ai to Detect Suspicious Behavior in Shopping Malls." Arcadian.ai, 2024, <https://www.arcadian.ai/blogs/blogs/using-ai-to-detect-suspicious-behavior-in-shopping-malls>.
- Cash is Freedom. "Join Our Campaign against Programmable Digital Currency." 2025, <https://www.cashisfreedom.uk/>.
- Clarke, Roger. "What's 'Privacy'?" (2006). <https://www.rogerclarke.com/DV/Privacy.html>.
- Cohen, Julie E. "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen." *The Georgetown law journal* 89, no. 6 (2001): 2029.
- Culnan, Mary J. "The Lessons of the Lotus Marketplace: Implications for Consumer Privacy in the 1990's." Paper presented at the Computers, Freedom & Privacy, Burlingame CA, March 26–28 1991.

- De Souza e Silva, Adriana, and Jordan Frith. "Locational Privacy in Public Spaces: Media Discourses on Location-Aware Mobile Technologies." *Communication, culture & critique* 3, no. 4 (2010): 503–25.
- de Waal, Dr Joel Rogers. "Security Trumps Privacy in British Attitudes to Cyber-Surveillance." YouGov, 2017, <https://yougov.co.uk/politics/articles/18362-Security-Trumps-Privacy>.
- Doyle, Carolyn, and Mirko Bagaric. "The Right to Privacy: Appealing, but Flawed." *The international journal of human rights* 9, no. 1 (2005): 3–36.
- Ebert, Isabel, Isabelle Wildhaber, and Jeremias Adams-Prassl. "Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection." *Big data & society* 8, no. 1 (2021).
- Edwards, Lilian, and Lachlan Urquhart. "Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?" *International journal of law and information technology* 24, no. 3 (2016): 279–310.
- European Data Protection Board. "Guidelines 05/2020 on Consent under Regulation 2016/679." V1.1. (4th May 2020). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
- Experian. "Data Enrichment and Enhancement." 2025, <https://www.experian.co.uk/business/data-quality/solutions/data-enrichment>.
- . "Social Media Checks – What Are They and Why Are They Important?", Updated Jan, 2021, <https://www.experian.co.uk/blogs/latest-thinking/background-checks/social-media-checks-what-are-they-and-why-are-they-important/>.
- Facewatch. "The Trusted Name in Retail Crime Prevention." 2025, <https://www.facewatch.co.uk/>.
- Federal Constitutional Court. *Judgment of 15 December 1983*. Bundesverfassungsgericht (Germany: 1983). https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.
- Finn, Rachel L., David Wright, and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet, 3–32. Dordrecht: Springer Netherlands, 2013.
- Gajda, Amy. *Seek and Hide: The Tangled History of the Right to Privacy*. New York: Viking, 2022.
- Gavison, Ruth. "Privacy and the Limits of Law." *The Yale law journal* 89, no. 3 (1980): 421–71.
- Goold, Benjamin J. "Privacy Rights and Public Spaces: Cctv and the Problem of the "Unobservable Observer"." *Criminal justice ethics* 21, no. 1 (2002): 21–27.

- Hadley, John. "Street Photography Ethics." *Ethical theory and moral practice* 25, no. 4 (2022): 529–40.
- Halliday, Josh. "Data Breach Exposes Details of 25,000 Current and Former Bbc Employees." *The Guardian*, 29th May 2024.
<https://www.theguardian.com/media/article/2024/may/29/data-breach-exposes-details-of-25000-current-and-former-bbc-employees>.
- Hansard. "Cash Acceptance - Volume 730: Debated on Monday 20 March 2023." 2023, <https://hansard.parliament.uk/commons/2023-03-20/debates/187CA19F-E3A9-48B1-B40A-869CB673F4A1/CashAcceptance>.
- Hao, Karen. "China Has a Problem with Data Leaks. One Reason Is Its Surveillance State." *Wall Street Journal* (New York), July 21st 2022.
https://www.wsj.com/world/china/china-has-a-problem-with-data-leaks-one-reason-is-its-surveillance-state-11658410752?mod=article_inline.
- Herbert, Danielle. "Man 'Branded a Thief' after Shop's Facial Recognition Error." (2025). <https://www.bbc.co.uk/news/articles/c3vn4p1lwqno>.
- Hern, Alex. "Fitness Tracking App Strava Gives Away Location of Secret Us Army Bases." *The Guardian*. (28 Jan 2018).
<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>.
- Holvast, Jan. "History of Privacy." Paper presented at the The Future of Identity in the Information Society, Berlin, Heidelberg, 2009// 2009.
- Hylen, Susan E. "Public and Private Space and Action in the Early Roman Period." *New Testament studies* 66, no. 4 (2020): 534–53.
- Independent, The. "The Ethics and Etiquet of Photography." *The Independent*, 11th July, 1907. https://archive.org/details/sim_independent_1907-07-11_63_3058/page/108/mode/2up.
- Information Commisioner's Office. "Data Security Incident Trends." 2025, <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/>.
- . "Home Cctv Systems." For the public, 2025, <https://ico.org.uk/for-the-public/home-cctv-systems/>.
- . "How Can We Comply with the Data Protection Principles When Using Surveillance Systems?", 2025, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/>.
- Jackson, Vincent. "Menace Ii Society." In *Doing Cultural Studies : The Story of the Sony Walkman*, edited by Paul Du Gay and et al. London: SAGE in association with The Open University, 1997.
- James, Henry. *The Reverberator*. New York: Macmillan, 1888.
- Kaspersky. "Social Media Privacy and Prevention." 2025, <https://www.kaspersky.com/resource-center/definitions/social-media-privacy>.

- King, Jennifer, and Caroline Meinhardt. "Rethinking Privacy in the Ai Era." *Human Centered Artificial Intelligence*. (February 2024).
<https://hai.stanford.edu/assets/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf>.
- Koops, Bert-Jaap, and Masa Galic. "Conceptualising Space and Place." Chap. 1 In *Privacy in Public Space: Conceptual and Regulatory Challenges*, 19–46. Cheltenham, UK: Edward Elgar Publishing, 2017.
- Kudina, Olya, and Melis Bas. "The End of Privacy as We Know It." Chap. 7 In *Surveillance, Privacy and Public Space*, edited by Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops, 119–40. Oxford: Routledge, 2020.
- Lab43. "Geofencing: The Smart Home Game Changer." 2025,
<https://lab53.uk/geofencing-the-smart-home-game-changer/>.
- Levy, Steven. "Bill Gates and President Bill Clinton on the Nsa, Safe Sex, and American Exceptionalism." (Nov 12th 2013).
<https://www.wired.com/2013/11/bill-gates-bill-clinton-wired/>.
- Lewis Adams, Lewis, and Kathryn Armstrong. "Facial Recognition Could Be Used More Widely by Police under Plans." BBC, 2025,
<https://www.bbc.co.uk/news/articles/c3r7pwpgeweo>.
- Madanipour, Ali. *Public and Private Spaces of the City*. London: Routledge, 2003.
- Marie Curie. "Supporters Privacy Notice." 2025,
<https://www.mariecurie.org.uk/privacy/supporters-privacy-notice>.
- Mause, Karsten. "A Politico-Economic Perspective on Privacy in Public Spaces." Chap. 4 In *Privacy in Public Space : Conceptual and Regulatory Challenges*, 91–111. Cheltenham, UK: Edward Elgar Publishing, 2017.
- Microsoft. "National Public Data Breach: What You Need to Know." 2024,
<https://support.microsoft.com/en-gb/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535>.
- Miles, Melissa. "Photography, Privacy and the Public." *Law, culture and the humanities* 11, no. 2 (2015): 270–93.
- Moreham, N. A. "Privacy in Public Spaces." *Cambridge law journal* 65, no. 3 (2006): 606–35.
- Nagel, Thomas. "Personal Rights and Public Space." *Philosophy & public affairs [e journal]* (1995).
- Nissenbaum, Helen. "A Contextual Approach to Privacy Online." *Daedalus* 140, no. 4 (2011): 32–48.
- . *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif.: Stanford Law Books, 2010.
- Parenti, Christian. *The Soft Cage: Surveillance in America, from Slavery to the War on Terror*. New York: BasicBooks, 2003.
- Peñalosa, Enrique. "Speech to the Urban Land Institute." Paper presented at the Urban Land Institute Annual Meeting, Boston, Massachusetts, 3rd October 2001 2001.

- Pereira, Ariane, and Emília Malcata Rebelo. "Women in Public Spaces: Perceptions and Initiatives to Promote Gender Equality." *Cities* 154 (2024): 105346.
- PetaPixel. "Germany Vs Google: How Street View Won the Privacy Battle in Europe's Most Private Country." Updated March 8th, 2024, <https://petapixel.com/2024/03/08/germany-vs-google-how-street-view-won-the-privacy-battle-in-europes-most-private-country/>.
- Philby, Kim. "The Day I Was Recruited as a Russian Spy, by Kim Philby." *The Observer*, 15th August 1999. <https://www.theguardian.com/theobserver/1999/aug/15/featuresreview.revi7>.
- Posner, Richard A. "The Economics of Privacy." *The American economic review* 71, no. 2 (1981): 405–09.
- Pressly, Lowry. *The Right to Oblivion: Privacy and the Good Life*. Cambridge, Massachusetts: Harvard University Press, 2024.
- Pricitor, Megan. "A Giant Biotechnology Company Might Be About to Go Bust. What Will Happen to the Millions of People's DNA It Holds?" *The Conversation*. (2024). <https://theconversation.com/a-giant-biotechnology-company-might-be-about-to-go-bust-what-will-happen-to-the-millions-of-peoples-dna-it-holds-241557>.
- Privacy International. "The End of Privacy in Public." 2025, <https://privacyinternational.org/campaigns/end-privacy-public>.
- Prosser, William L. "Privacy." *California law review* 48, no. 3 (1960): 383–423.
- Rachels, James. "Why Privacy Is Important." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, 290–99. Cambridge: Cambridge University Press, 1984.
- Ratcliffe, Susan. "Cardinal Richelieu." In *Oxford Essential Quotations*: Oxford University Press, 2017.
- RayBan Meta. "Ray-Ban | Meta Wayfarer." 2025, <https://www.ray-ban.com/uk/electronics/RW4006ray-ban%20%20meta%20wayfarer-black/8056597988377>.
- Reddit. "Square Pos "Send Receipt to Phone/Email" Creates a Shadow Profile Linked to Your Card Number." (2024). https://www.reddit.com/r/privacy/comments/1gdqv02/square_pos_send_receipt_to_phoneemail_creates_a/.
- Roessler, Beate, and Judith DeCew. "Privacy." *The Stanford Encyclopedia of Philosophy*. (2023). <https://plato.stanford.edu/archives/win2023/entries/privacy/>.
- Royal United Services Institute. "A Democratic Licence to Operate: Report of the Independent Surveillance Review." (13 July 2015). https://static.rusi.org/20150714_whr_2-15_a_democratic_licence_to_operate.pdf.
- Scanlon, Thomas. *What We Owe to Each Other*. Cambridge, Mass.: Belknap Press of Harvard University Press, 1998.

- Scherr, Albert. "Privacy in Public Space: The Problem of out-of-Body DNA." Chap. 9 In *Privacy in Public Space: Conceptual and Regulatory Challenges*, 211–41. Cheltenham, UK: Edward Elgar Publishing, 2017.
- Schneier, Bruce. "The Eternal Value of Privacy." 2006, https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.
- Selinger, Evan, and Brenda Leong. "The Ethics of Facial Recognition Technology." In *Oxford Handbook of Digital Ethics*, edited by Carissa Véliz: Oxford University Press, 2023.
- Smartt, Ursula. "The Stalking Phenomenon: Trends in European and International Stalking and Harrassment Legislation." *European journal of crime, criminal law, and criminal justice* 9, no. 3 (2001): 209–32.
- Smith, Robin James. "Interaction in Public Spaces." In *The Routledge International Handbook of Goffman Studies*, edited by Gregory W. H. Smith and Michael Hviid Jacobsen. London: Routledge, 2022.
- Snowden, Edward J. *Permanent Record*. London: Macmillan, 2019.
- Solove, Daniel J. "Murky Consent: An Approach to the Fictions of Consent in Privacy Law." *Boston University law review* 104, no. 2 (2024): 593–639.
- . *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven Conn.: Yale University Press, 2011.
- . *On Privacy and Technology*. Oxford: Oxford University Press, 2025.
- . "A Taxonomy of Privacy." *University of Pennsylvania law review* 154, no. 3 (2006): 477–564.
- . "Why Privacy Matters Even If You Have 'Nothing to Hide'." *The Chronicle of Higher Education* 57, no. 37 (2011).
- Spegele, Brian. "China's Surveillance State Pushes Deeper into Citizens' Lives." *Wall Street Journal* (New York), Oct 19th 2022. <https://www.wsj.com/articles/xi-china-surveillance-covid-11666187151>.
- Surveillance Camera Commissioner's Office. "'If You've Done Nothing Wrong...': 5 Reasons Why This Is No Defence for Surveillance." UK Government, Updated 27 May, 2021, <https://videosurveillance.blog.gov.uk/2021/05/27/if-youve-done-nothing-wrong-5-reasons-why-this-is-no-defence-for-surveillance/>.
- Swanson, Judith A. *The Public and the Private in Aristotle's Political Philosophy*. Ithaca: Cornell University Press, 1992.
- Syal, Rajeev. "Home Office Admits Facial Recognition Tech Issue with Black and Asian Subjects." *The Guardian*, 5th December 2025. <https://www.theguardian.com/technology/2025/dec/05/home-office-facial-recognition-tech-issue-black-asian-subjects>.
- Tandon, Harsh. "How Marie Curie Use Data & Insights to Improve Supporter Engagement & Increase Income." CACI, Updated 27th May, 2025, <https://www.caci.co.uk/insights/how-marie-curie-use-data-insights-to-improve-supporter-engagement-increase-income/>.

- Thomson, Judith Jarvis. "The Right to Privacy." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, 272–89. Cambridge: Cambridge University Press, 1984.
- Timan, Tjerk. "Conclusion: The Need for Privacy in Public Space." In *Privacy in Public Space: Conceptual and Regulatory Challenges*, 269–90. Cheltenham, UK: Edward Elgar Publishing, 2017.
- UK Government. "Crime and Policing Bill: Police Powers Factsheet." 2025, <https://www.gov.uk/government/publications/crime-and-policing-bill-2025-factsheets/crime-and-policing-bill-police-powers-factsheet>.
- . "Police Powers to Stop and Search: Your Rights." 2025, <https://www.gov.uk/police-powers-to-stop-and-search-your-rights/police-powers-stop-question>.
- van de Waerdt, Peter J. "Information Asymmetries: Recognizing the Limits of the Gdpr on the Data-Driven Market." *Computer Law & Security Review* 38 (September 2020): 105436. <https://www.sciencedirect.com/science/article/pii/S0267364920300418>.
- Veliz, Carissa. "In the Privacy of Our Streets." Chap. 2 In *Surveillance, Privacy and Public Space*, edited by Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops, 16–32. Oxford: Routledge, 2020.
- Véliz, Carissa. *The Ethics of Privacy and Surveillance*. Oxford Philosophical Monographs. Oxford: Oxford University Press, 2024.
- . "The Surveillance Delusion." In *Oxford Handbook of Digital Ethics*, edited by Carissa Véliz, 0: Oxford University Press, 2023.
- Warren, James. "Boy Arrested over London Transport Cyber Hack." BBC, Updated 12 September, 2024, <https://www.bbc.co.uk/news/articles/c4gqg2elkj4o>.
- Weckert, John. *Electronic Monitoring in the Workplace: Controversies and Solutions*. Hershey, PA: Idea Group Publishing, 2004. doi:10.4018/978-1-59140-456-9.
- Westin, Alan F. *Privacy and Freedom*. New York: Ig Publishing, 2015.
- Williams, James. "Ethical Dimensions of Persuasive Technology." In *Oxford Handbook of Digital Ethics*, edited by Carissa Véliz, 0: Oxford University Press, 2023.
- Word Histories. "Origin of "an Englishman's Home Is His Castle"." 2017, <https://wordhistories.net/2017/07/26/englishmans-home-castle-origin/>.