How Surveillance Works

Dr Victoria Baines, IT Livery Company Professor of IT

8th April 2025

> *It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way – in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only.*

This is the memorable opening of Charles Dickens' *A Tale of Two Cities*. It's a fictional account of the French Revolution, written several decades later (1859), and by an Englishman at that. But it is worth mention here for its apparent understanding of surveillance and its impacts. It is permeated throughout by the language of the watchers and the watched (even the towers of Notre Dame are personified as watching), tensions between secrecy and transparency, and their capacity to be driven by various motivations and for various purposes - all of which have relevance for us today.

To some extent Dickens characterises the police state as an exotic Other, surveillance as a foreign practice of Britain's old arch enemy and therefore antithetical to its standards. This "universal watchfulness" finds its embodiment in the memorable character of Madame Defarge, one of the *tricoteuses* who took to knitting at the Guillotine. Her anti-aristocratic activities driven at least in part by her sister's experience of sexual violence at the hands of the elite, she comes to symbolise the most vengeful aspects of the Revolution in the novel. When we first meet her, she is described as "a stout woman…with a watchful eye that seldom seemed to look at anything, a large hand heavily ringed, a steady face, strong features, and great composure of manner." She is at once an agent of surveillance and totally inscrutable. Indeed, we later learn that she is also expert in counter-surveillance, encoding in her knitting the names of those to be condemned.

Twitching curtains, telling tales

When we report our observations about others to others, we are not always solely motivated by public interest. Dickens signposts this by nicknaming one of Madame Defarge's sisterhood The Vengeance. Further back in time, Ancient Rome lacked public prosecutors. In its stead, individuals brought cases against each other for criminal offences even when they were not the injured party. Cicero (*De Officiis* 2.14) argues that accusing others – as he himself did frequently – is not itself reprehensible (*reprehendendum*) so long as it is in the public interest:

> *If it shall be required of anyone to conduct more frequent prosecutions, let him do it as a service to his country; for it is no disgrace to be often employed in the prosecution of her enemies. And yet a limit should be set even to that. For it requires a heartless man, it seems, or rather one who is well-nigh inhuman, to be arraigning one person after another on capital charges. It is not only fraught with danger to the prosecutor himself, but is damaging to his reputation, to allow himself to be called a prosecutor.*

Cicero here alludes to how accusers motivated by personal interest might be viewed. Although he uses the word *accusator*, they came to be known in the Imperial period as *delatores*, denouncers or informers who might bring a prosecution or simply provide incriminating information for personal gain. This process was incentivised by the accuser's entitlement in law to a portion of the accused's property in the event of a conviction. In the reign of Augustus, this came to include prosecutions for adultery, and words or behaviour that threatened the majesty (*maiestas*) of the Emperor. Where there is money to be made from denunciation,

it is natural for people to move from what they happen to observe to what they can proactively gather through surveillance or intelligence. And in a dictatorship, accusers may be motivated as much by fear and self-protection as by the prospect of personal advancement: demonstrating loyalty to a regime by throwing heat on others can serve to reduce the risk to oneself, however temporarily.

Suetonius tells us that by the time of Nero's reign (54-68 CE), the tail was wagging the dog: "He ordained likewise that all words and actions upon which any informer could ground a prosecution, should be deemed treason" (*Nero* 32). If one could accuse someone of it, it was an insult to the regime, and therefore the Emperor. Thus, everything becomes treason. In the second century CE, the satirist Juvenal describes an unnamed *delator* who is so dangerous that even the most infamous informers from the reign of the 'bad' Emperor Domitian (81-96 CE) fear him (1.33). He also imagines a scene in which catching a massive turbot puts one in jeopardy of accusations of treason (4.45-8):

> *This monster the master of the boat and line designs for the High Pontiff [the Emperor Domitian]; for who would dare to put up for sale or to buy so big a fish in days when even the sea shores were crowded with informers?*

Philostratus' third century CE *Life of Apollonius of Tyana* (8.7) puts in the mouth of its subject a description of Rome under Domitian as a city in which no one and nowhere is safe from surveillance. In this striking passage, the philosopher mounts a robust defence against accusations made by informers that included human sacrifice, preforming magic, and conspiring against the Emperor:

> *The fact of my coming to Rome is in itself a disproof of the charge of revolutionary plotting; for to live in a city, where there are so many eyes to see and so many ears to hear things which are and are not, is a serious handicap for anyone who desires to play at revolution, unless he be wholly intent upon his own death. On the contrary, it prompts prudent and sensible people to walk slowly even when engaged in wholly permissible pursuits.*

We have no way of knowing whether Apollonius himself wrote or spoke these words. Philostratus claims they are based on memoirs of one of his companions, but this source material doesn't survive. But the depiction of Imperial Rome as a place where one is constantly watched is consistent with the work of our satirist Juvenal. His third satire contains particularly vivid descriptions of the dangers of life at Rome (3.268-277):

> *Now consider the various other dangers of the night. What a long way it is from the high roofs for a tile to hit your skull! How often cracked and leaky pots tumble down from the windows! What a smash when they strike the pavement, marking and damaging it! You could be thought careless and unaware of what can suddenly befall if you go out to dinner without having made your will. As you pass by at night, there are precisely as many causes of death as there are open windows watching you. So make a wish and a pathetic prayer as you go that they'll be content with emptying their shallow basins on you.*

Through personification, even the windows are engaged in surveillance. They are *vigiles* – watchful, vigilant. The noun form, *vigilantia*, is in fact the root of the modern word surveillance. And in Ancient Rome, *vigiles* was also the name of what was effectively the city's police force. Originally established as a fire brigade, they were formalised into a paramilitary unit of several thousand watchmen who were freed slaves. As well as maintaining public order, especially at night, the *vigiles* came to be associated with undercover surveillance, as described by Epictetus (*Discourses* 4.13.5):

> *A soldier, dressed like a civilian, sits down by your side, and begins to speak ill of Caesar, and then you too, just as you received from him some guarantee of good faith in the fact that he began the abuse, tell likewise everything you think and the next thing is – you are led off to prison in chains.*

We see personally motivated denunciations throughout history, with at times what we know now to be clearly fictitious testimony. As Gresham Professor of Divinity Ronald Hutton has explored in his lecture on Witch-Hunting in European and World History, accusations of witchcraft could be prompted by personal grievance, family rivalries, or a desire for revenge.[1]

Denunciation as an act of vengeance and expression of civic duty features repeatedly in the context of the French Revolution, where each commune had a Committee of Surveillance (perhaps better translated here as 'Vigilance') and failure to denounce was itself framed as grounds for suspicion, as in this proclamation issued in Lyon in 1793:

---

[1] https://www.youtube.com/watch?v=ucZrMm_4FIA

Denounce the crimes, denounce the criminals, a double reward awaits you: the voice of your conscience, for denunciation is a virtue: and a legitimate reward, for the National Convention is just and desires that each virtuous act should be a means by which the sans-culotte may improves his lot…

Friends, nothing can, nothing should constrain your ardour here: former servants must not forget that the Motherland is their sole mistress; nor relatives forget that it alone is their mother; nor citizens forget that they owe themselves utterly to this Motherland which rewards their zeal so effectively, but which would sanction without pity their negligence and punish their criminal silence.[2]

In this context, the inclusion of the Eye of Providence in French art of the time takes on particular significance. The state is all-seeing when everyone watches his or her neighbour. It is also around this time that the word surveillance first enters the English language. In his 1803 *Rough Sketch of Modern Paris* (xxix. 236) J. G. Lemaistre describes a visit to the Gobelins tapestry manufactory: "The workmen are not locked up within the walls of the manufactory, as was the case during the monarchy, but they are kept under the constant "surveillance of the police"."

"Smile, you're on CCTV"

Surveillance as a deterrent, as something that can manipulate someone's behaviour to achieve at least an outward semblance of compliance as Philostratus has Apollonius suggest, is proposed wholeheartedly by an English contemporary of the French Revolution. We have met Jeremy Bentham before, in my 2023 Gresham lecture on encryption.[3] One of the most prominent proponents of utilitarianism, and specifically that "it is the greatest happiness of the greatest number that is the measure of right and wrong", Bentham left instructions in his will that his 'auto icon' – a wax likeness of his head and his preserved skeleton dressed in his own clothes – should be put on display in perpetuity. He is still visible today, in University College London, although thankfully his now desiccated head has been removed from between his feet. In 1787 he published detailed proposals for a system of surveillance based on what he claimed were his brother Samuel's observations and designs in other countries including Russia. Brother Jeremy entitled his proposals as follows:

PANOPTICON;

OR

THE INSPECTION-HOUSE:

CONTAINING THE

IDEA OF A NEW PRINCIPLE OF CONSTRUCTION

APPLICABLE TO

ANY SORT OF ESTABLISHMENT, IN WHICH PERSONS OF

ANY DESCRIPTION ARE TO BE KEPT UNDER INSPECTION;

AND IN PARTICULAR TO

PENITENTIARY-HOUSES,

PRISONS, HOUSES OF INDUSTRY, WORK-HOUSES, POOR-HOUSES, LAZARETTOS, MANUFACTORIES, HOSPITALS, MAD-HOUSES, AND SCHOOLS:

WITH

A PLAN OF MANAGEMENT

ADAPTED TO THE PRINCIPLE:

Remembered largely as a design for a prison, it's worth noting here that it was in fact intended to be applicable to any institution in which large numbers of people needed to be watched – or feel as if they were being watched:

---

[2] Reproduced in Lucas, C. (1996) "The Theory and Practice of Denunciation in the French Revolution", *Journal of Modern History* 68.4: 768-785

[3] https://www.youtube.com/watch?v=sS-Epye4a_w

It is obvious that…the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose X of the establishment have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should conceive himself to be so.

The point of the Panopticon was to enable a handful of inspectors – or even a single inspector – to supervise a much larger number of inmates. It did so by making those inmates constantly visible, thereby feeling that they were under constant surveillance, or at the very least that any of their activities could be observed at any given moment.

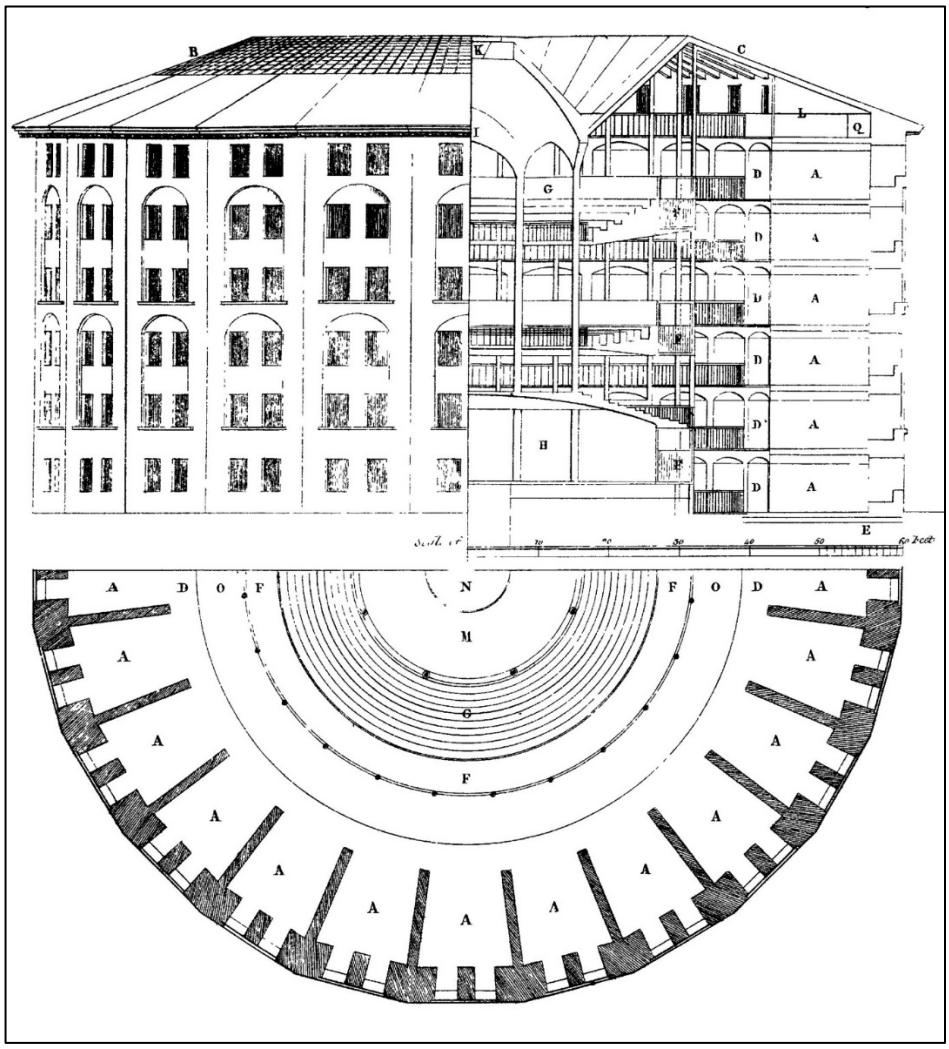

Fig. 1 Jeremy Bentham's Panopticon

Not unlike Madame Defarge, from the central tower (N), the inspector can see everything including all the inmates (A), without being seen. The effect is what Bentham celebrates as "a new mode of obtaining power of mind over mind." It has since been critiqued – perhaps most famously by 20th century historian and philosopher Michel Foucault in his work *Discipline and Punish* – as the ultimate illustration of surveillance as an instrument of power.

There are evident echoes of the design in Victorian institutional architecture. And yet it is clear from Bentham's original text that he saw this as a more humane solution to the overcrowded and insanitary conditions of 18th century prisons. For schools, he posits that "The youth of either sex might by this means sleep, as well as study, under inspection, and alone - a circumstance of no mean importance in many a parent's eye." For Bentham, the Panopticon presents a delightfully simple opportunity to improve society without violence:

What would you say, if by the gradual adoption and diversified application of this single principle, you should see a new scene of things spread itself over the face of civilized society? – morals reformed, health preserved, industry invigorated, instruction diffused, public burthens lightened, economy seated as it were upon a rock, the gordian knot of the poor-laws not cut but untied - all by a simple idea in architecture?

From a 21st century vantage point, however, it's difficult not to see it as Orwellian, and as a prototype for some of the worst excesses of authoritarian regimes. At the same time, we may spot parallels with our use of digital technology, not least the fact that our continual sharing of data about and of our lives makes us more visible than ever, more of the time.

21st century surveillance – democratic principles and safeguards

How does surveillance work now? In the UK, the Regulation of Investigatory Powers Act (RIPA) 2000 provides for the authorisation of covert surveillance by public authorities including police forces, the intelligence services, the Armed Forces, Revenue and Customs, and some government departments. It defines surveillance as "monitoring, observing or listening to persons, their movements, conversations or other activities and communications".[4] Surveillance is deemed to be covert if it is "carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place". Covert surveillance is further divided into directed and intrusive surveillance, as follows:

- Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under the 2000 Act);
- Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device).

The government's code of practice provides helpful examples of what would require directed surveillance authorisation due to reasonable expectation of privacy: the conversation of two people on the street or in a bus, the gathering of information about the pattern of a person's visits to a café, and recording someone providing their personal details to a shop assistant. In contrast, an example of intrusive surveillance would be the use of a zoom lens which "consistently achieves imagery of the same quality as that which would be visible from within the premises." The level of intrusion determines the authority required. For non-urgent requests, authorisation by a police Superintendent or equivalent rank is required; for intrusive surveillance in a private place, it's a Secretary of State, usually the Home Secretary.

Various safeguards are built into the application process. Twenty years ago, I was responsible for submitting applications for directed surveillance of drug dealers, and I can confirm first hand that we had to meet all these individual requirements. Authorisations are time limited – 3 months for the police, 6 months for the intelligence services (both renewable). The measures requested need to be necessary, on the grounds that they are:

- *in the interests of national security;*
- *for the purpose of preventing or detecting crime or of preventing disorder;*
- *in the interests of the economic well-being of the UK;*
- *in the interests of public safety;*
- *for the purpose of protecting public health;*
- *for the purpose of assessing or collecting any tax, duty, levy or other imposition,*
- *contribution or charge payable to a government department; or*
- *for any other purpose prescribed by an order made by the Secretary of State.*

[4] https://assets.publishing.service.gov.uk/media/5ba37401e5274a55cdb89bce/201800802_CSPI_code.pdf

My drug dealers fell very squarely under the second criterion. I also had to show that the surveillance requested was proportionate to the suspected offence and that the information we sought could not be obtained by other means.

It's my experience that these principles are not simply nice to have, they are enforced. When it emerged that some local councils were conducting directed surveillance to investigate activities such as dog-fouling and barking, use of disabled parking badges, and putting rubbish out on the wrong day, their powers were restricted: local councils can now only use directed surveillance to investigate offences which attract sentences of six months or more or relate to the underage sale of alcohol or tobacco, and subject to judicial approval[5]. Applications also need to demonstrate that they have assessed the risk of 'collateral intrusion' into the privacy of persons who are not the subject of the investigation – for example, the family of someone suspected of an offence – and that they have taken steps to limit that intrusion where possible. Those principles of necessity, proportionality, and minimising collateral intrusion are recognised as international good practice, and have featured prominently in efforts to standardise surveillance practices across the world such as the *International Principles on the Application of Human Rights to Communications Surveillance*.[6]

Twenty years ago, when I was submitting surveillance applications, we already had access (subject to due authorisation) to quite a lot of information about persons of interest: who was using a particular phone number, who was calling whom, where their car had been spotted by human observers or automatic number plate recognition (ANPR), their movements to and from their homes and workplaces, when they used a particular ATM or point of sale. Even if, as was often the case, drug dealers used prepaid mobile phones to avoid tracking, if we knew the phone number we could see when and where the credit was topped up. We could already to some degree track their movements and communications by the data they created.

Fast forward two decades, and two things are obvious: 1) We are generating so much more data and 2) It is being exploited by different actors for different purposes. Parking providers use ANPR to register your vehicle and fine you for non-payment. You are on CCTV on public and private property, whether you choose to 'smile' or not. And there is now a treasure trove of your private communications, geographical locations, photos and videos, thoughts and feelings – at least, those you have expressed.

Blurred lines – surveillance vs. data generation

The data you generate can be requested by public authorities with the relevant authorisation, and not all countries apply the same safeguards to surveillance. The companies who either generate this data on you, or to whom you volunteer it, use it for numerous purposes, from combatting fraud to market research to targeted advertising. As we saw in my previous lecture, data capture is used to profile us, to socially sort us into groups and types – and to manipulate what we see and experience, in this case for profit.[7] It's become fashionable to call this 'surveillance capitalism' after Shoshana Zuboff's book of the same name. Although it's useful shorthand for a particular set of practices in the Big Tech ecosystem, I find its impact and interpretation somewhat problematic. In the first instance, the sheer novelty of the concept can encourage us to forget that – as we have seen above - we have been 'surveillance societies' for millennia. My second, not unrelated, concern, is that the association of surveillance with capitalism may give the mistaken and paradoxical impression that the former is somehow contingent on the latter. Our knowledge of authoritarian and other regimes of course tells us that it is not. It's also worth noting that governments have been known to use the same online behavioural advertising techniques to 'nudge' users to change their behaviour.[8]

At this point it is important to acknowledge that in some disciplines, 'surveillance' is not a negative or sinister concept. In my previous lecture, we also saw how John Graunt's analysis of London's Bills of Mortality in the 16th century heralded the development of public health surveillance, monitoring the population for causes of death and disease with the aim of reducing both.[9] This kind of surveillance saves and improves countless lives, even though it is conducted at a 'mass' population level. Related to this is wastewater surveillance,

---

[5] https://www.theguardian.com/uk/2009/jul/21/local-authorities-spy-on-public; https://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public

[6] https://www.eff.org/files/necessaryandproportionatefinal.pdf

[7] https://www.youtube.com/watch?v=ce1CmaZ0qJQ

[8] https://www.theguardian.com/technology/2021/sep/08/study-finds-growing-government-use-of-sensitive-data-to-nudge-behaviour

[9] https://www.emro.who.int/health-topics/public-health-surveillance/index.html

which can detect the presence of contaminants in sewage, enabling the spread of virus pathogens to be tracked. With suitable safeguards, this seems to me to be a 'good' kind of surveillance. As with all data collection and analysis, safeguards need to apply not only to how this kind of surveillance is conducted, but also how the output is used. For example, it's been proposed that wastewater surveillance could be used to identify the level of psychoactive drugs in communities. Tests conducted corroborate information from international organisations – including my old agency EUROPOL – that the retail market for cocaine is expanding in Eastern Europe.[10] We might reasonably expect these findings to drive a policy response in those countries to assign more funds for education programmes and support for those with problematic drug use. But most of us would consider it disproportionate if the police were to profile more people in those regions as 'drug users' simply on the basis of this dataset and enforce against them accordingly. In an age of increasing use of AI, these are broadly the concerns of legislators such as those in the EU, where the AI Act now bans the use of automated profiling for predictive policing and criminal prediction systems (but provides a general exemption for national security).[11]

But it's not only Big Tech and retailers/advertisers monitoring our activity, tracking our online whereabouts (browsing habits): it's also prospective employers checking to see whether we are 'their kind of person'; it's our current employers, measuring our productivity in a much more granular fashion than 'clocking on' and time and motion men ever could. It's also each and every one of us. Digital technology turns us into voyeurs. Humans are naturally nosy. Which of us can honestly say that we have never Googled an ex-partner or former friend, or searched for them on social media, simply out of curiosity? The Even if we are not conducting our own directed surveillance, we see much further into other people's private lives than ever before. Some of this is staged, as in the case of public figures. Influencers create online content with an air of intimacy, blurring the lines between our traditional conceptions of public and private space. It's not covert surveillance if they invite us in and know we're watching – and yet it can nevertheless feel intrusive and voyeuristic. In the name of keeping our children safe, some of us may insist on monitoring their online activities and communications. The dark counterpart to that is stalkerware, publicly available apps that can be installed surreptitiously on someone's devices in order to track them and intercept their messages. Inevitably, this kind of surveillance technology is used by abusive partners in coercive relationships.

Private Eyes

The wealth of publicly available data on most, if not all, of us, has given rise to a new role in society – the Open-Source Intelligence (OSINT) amateur investigators. These are people who, for a range of motives, track targets across digital services. As the term "Open Source" suggests, the focus of this kind of data gathering is primarily public information. But what constitutes public information on the Internet is moot. We can safely say that data that someone publishes on their own website is open source. But what about a post on a social media platform, or any digital space for which a viewer would need to set up an account, and perhaps even conceal their identity with fictitious details in order to do so? For government authorities, conducting a targeted search on a specific individual even of open-source information can constitute directed surveillance and require due authorisation. Private OSINT investigators have no such constraints or legal protections.

And yet, the role of amateur groups is only increasing, particularly in relation to online safety. Digital vigilantism is embodied by the self-styled "paedophile hunters" who conduct citizen-led investigations that one would otherwise expect to be led by the police.[12] They often operate undercover, posing as children online in the hope that adults with paedophilic urges will engage with them and arrange to meet. This kind of 'sting' operation is heavily regulated with standard operating procedures, *if* conducted by law enforcement officers. No such rules apply to private individuals, and as a result there have been cases where evidence collected in this way has been inadmissible in court, interfered with legitimate operations, and even resulted in offences being committed by the vigilante groups. The last of these is particularly evident where the desire for vengeance and public humiliation can lead to violent assaults on individuals identified by the vigilantes as suspects.

At least some of these vigilante groups have something of the spirit of the *accusateurs* and Comités of the French Revolutionary era. Nevertheless, in the UK, their activities are so prevalent that their evidence is

[10] https://pmc.ncbi.nlm.nih.gov/articles/PMC7078280/pdf/41598_2020_Article_61628.pdf
[11] https://www.europeanlawblog.eu/pub/tbgfjobj/release/1
[12] https://journals.sagepub.com/doi/10.1177/17488958221136845?icid=int.sj-full-text.citing-articles.1

increasingly used in prosecutions, and the criminal justice system has had to issue guidance on their status in the law.[13] This is not the same as a member of the public simply reporting a crime that they happened to witness: it is citizen led digital investigation. This kind of amateur activity is prompted at least in part by what is perceived to be police inactivity. It highlights another key paradox: as much as digital technology now provides vastly superior means to surveil us, the result is very often too much information for the authorities to cope with.

21st century surveillance – automation and outsourcing

Two solutions have presented themselves in recent years. The first is an attempt to move away from targeted surveillance of suspected individuals in preference for automated profiling of 'bulk' datasets of all of our communications data. In 2014, this approach was summed up by the then Home Secretary Theresa May as follows: "If you are searching for the needle in the haystack, you have to have a haystack in the first place".[14] She told the same Parliamentary committee hearing, convened after Edward Snowden made public classified information on bulk data collection, that while citizens did not give their explicit consent to have their data harvested by the security services, there was an "unwritten agreement" that it was needed to "keep us safe".

I'm not sure everyone agrees. In fact, I would hypothesise that citizens are becoming increasingly privacy and security conscious. This appears to be borne out by steady growth in user numbers for privacy enhancing technologies (PETs) like encrypted messaging apps (Signal, Telegram) and anonymisers (Virtual Private Networks, Tor). When I worked as a cybercrime investigator, we called these counter-surveillance measures, because they obstructed identification and interception of criminals and their communications. They're now being used much more widely by the general population, which in turn suggests that we are all becoming more aware of surveillance by various actors, and ways to evade it.

Another approach has been to put the burden of surveillance onto tech companies. Following the logic that they are collecting vast amounts of our personal and private information in any case, effectively conducting their own mass surveillance, they can also conduct surveillance and enforcement that would otherwise be the remit of government authorities. This is particularly noticeable in emerging online safety legislation around the world, where the focus is less on prosecuting the humans who commit criminal offences using digital technology, and more on the responsibility of platforms to monitor for harmful content and remove it from our experience. The preferred solution, at least for now, is for platforms to surveil and modify what we see so that government authorities don't have to. It is a highly normative process that upholds a given community's desired morals, and which in turn interacts with growing self-censorship in digital spaces, sometimes known as chilling effects, apparently fuelled as much by fear of social alienation as by censure from the authorities.[15]

On the Internet, then, the risk is that awareness of surveillance – by governments, companies, and our fellow citizens – doesn't just deter 'bad' behaviour but also free expression. Where the notice "Smile, you're on CCTV" may make us self-conscious in a limited geographical area, digital technology exposes us to the gaze – and therefore judgement – of the entire world, depending on our privacy settings. Moreover, the Internet doesn't forget: witness the persistent trend for online communities and media to 'out' public figures for unpleasant or ill-advised comments they may have posted online as children.[16]

Popular resistance, countermeasures, and the Emergency Exception

At the same time, resistance is not inconsiderable to the use of technologies that are perceived to be engaged in surveillance without knowledge or consent. Over a decade ago, early adopters of Google's Glass Augmented Reality (AR) glasses found themselves branded as 'glassholes' and banned from establishments

---

[13] https://www.bbc.co.uk/news/uk-england-50302912; https://www.cps.gov.uk/legal-guidance/online-child-abuse-activist-groups-internet

[14] https://www.bbc.co.uk/news/uk-politics-29642607

[15] https://academic.oup.com/psq/article-abstract/138/3/361/7192889

[16] https://www.bbc.co.uk/news/av/uk-politics-22085693; https://www.independent.co.uk/news/education/education-news/nus-anti-semitism-national-union-students-offensive-tweets-jews-racism-adolf-hitler-israel-executive-council-malia-bouattia-a7696566.html

over fears that they were recording everyone in their sightlines.[17] More recently, a woman with whom Italy's Culture Minister is alleged to have had an extra-marital affair was banned from the Italian parliament for filming with a pair of Ray-Ban Stories smart-glasses.[18] It was only when the woman posted the filmed content on social media that the authorities became aware of it. There are, I think, two considerations contributing to hostile reactions to this kind of technology, over and above the annoyance or intrusion we may feel when someone holds up a smartphone in front of us: the fact that data may be captured surreptitiously by devices that look like ordinary sunglasses; and, the fact that these devices are perceived to be always capturing whatever the wearer sees, wherever they look.

Throughout history, we see evidence of the popular belief that one-to-one communication is and should remain private, and challenges to that privacy. For my 2023 lecture on encryption, The Sun newspaper very kindly ran an online poll on our behalf. In answer to the question, "Should the government have access to your online chats?", 84.02% (27,929 votes) responded "No, absolutely not". Throughout my three years of Gresham lectures, we have considered a millennia-old history of means to prevent interception of private correspondence, or at least its encryption to make it unreadable and therefore unusable: from the Caesar cipher, to John Wilkins' 1641 treatise *Mercury, or the secret and swift messenger* (featured in my lecture on Messaging and Signals[19]), and the kindred development by the military of technologies to prevent useful interception of sensitive communication, from ciphers to Enigma to channel hopping.

Cicero, our famous Roman prosecutor, was certainly aware of the potential for his personal correspondence to be intercepted. In a letter to his friend Atticus in Greece (XVIII (A I, 13)), written in 61 BCE, he cautions: "I don't venture to trust either Achaeans or Epirotes [i.e. Greek people] with a letter somewhat more outspoken than usual. Now some events have occurred since you left me worth my writing to you, but they must not be trusted to the risk of a letter being lost, opened, or intercepted." This was several decades before the Emperor Augustus introduced the *cursus publicus*, a public postal system for the whole empire.

Our French Revolutionaries initially baulked at the idea of reading people's private correspondence. In the summer of 1789, a committee was established to intercept and read aloud letters that were contained 'suspicious correspondence". As noted by Katlyn Marie Carter, the newspaper *Révolutions de Paris* gave sensational descriptions of interceptions and attempts to prevent them, including one messenger who swallowed the note in his charge.[20] But the idea of challenging the long-held belief that private correspondence was secret (*secret de la poste*) was controversial. A heated debate ensued in the General Assembly, with supporters arguing that interception was justified by the emergency circumstances[21]. In the words of a mysterious "Monsieur ***":

> *Although it is the unanimous wish of our cahiers [list of grievances] that postal secrecy should be inviolable, we cannot and should not believe that the intention of our constituents is that we should respect this inviolability at the cost of their safety and liberty. The most pressing of our duties is to secure these for them. Would it not be ridiculous and absurd, in fact, to believe that our constituents do not think and do not want progress in matters of safety and common and personal liberty above all else?*

This presumption to know the thoughts of citizens and to have their agreement to compromise their privacy is expressed in terms that are not dissimilar to Theresa May's explanation for bulk data collection. This is not to say that I believe the circumstances or the motivations to be identical: rather that - as I have explored more extensively elsewhere in relation to other aspects of safety and security rhetoric – emergency justifications for greater intrusion are not new, and they can be difficult to reverse.[22]

Belief in the sanctity of private correspondence was at the fore of another key moment in surveillance history, what has come to be known as the Post Office Espionage Scandal. As Marjorie Stone has observed (see Further Reading), it had a lasting impact on the British government's surveillance policy. On 14th June 1844, a petition was presented to the House of Commons that the Home Secretary, Sir James Graham, had

---

[17] https://edition.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions/index.html
[18] https://www.politico.eu/article/italy-minister-maria-rosaria-boccia-ray-ban-information/
[19] https://www.youtube.com/watch?v=SiXa6unIWlc
[20] Katlyn Marie Carter. 2018. "The Comités des Recherches: Procedural Secrecy and the Origins of Revolutionary Surveillance". *French History* 32.1; *Révolutions de Paris* 1.29.
[21] *Archives Parlementaires*, Tome VIII, 273ff. - https://archives-parlementaires.persee.fr/doc/743e3cc4-2a21-4625-b494-c4324f932ff0
[22] Victoria Baines. 2022. *Rhetoric of InSecurity: The Language of Danger, Fear and Safety in National and International Contexts*. Routledge. London.

authorised the interception of the letters of Giuseppe Mazzini, and exiled Italian nationalist living in London. Graham and the Foreign Secretary Lord Aberdeen shared information from Mazzini's letters with Austria, from whose empire Italian states were attempting to gain independence. As documented by F. B. Smith, we have an unusual amount of information for the time on tradecraft, on both sides, including broken and doubly impressed seals, altered time stamps, and surveillance detection measures such as inclusion of tiny grains that would betray evidence of tampering.[23] The public outcry at the time was considerable, amplified by radical politicians and notable intellectuals, among them the Scottish writer Thomas Carlyle in a letter to *The Times*:

> *Whether the extraneous Austrian Emperor and miserable old chimera of a Pope shall maintain themselves in Italy, or be obliged to decamp from Italy, is not a question in the least vital to Englishmen. But it is a question vital to us that sealed letters in an English post-office be, as we all fancied they were, respected as things sacred; that opening of men's letters, a practice near of kin to picking men's pockets, and to other still viler and far fataler forms of scoundrelism, be not resorted to in England, except in cases of the very last extremity. When some new Gunpowder Plot may be in the wind, some double-dyed high treason, or imminent national wreck not avoidable otherwise, then let us open letters: not till then. To all Austrian Kaisers and such like, in their time of trouble, let us answer, as our fathers from of old have answered:—Not by such means is help here for you. Such means, allied to picking of pockets and viler forms of scoundrelism, are not permitted in this country for your behoof. The right hon. Secretary does himself detest such, and even is afraid to employ them. He dare not: it would be dangerous for him! All British men that might chance to come in view of such a transaction, would incline to spurn it, and trample on it, and indignantly ask him, what he meant by it!*

Carlyle's letter is most often read as an outright rejection of interception of private communications. But in light of the arguments we have seen above for intrusion in the interest of public safety, the emergency exceptions for terrorism, treason, and national catastrophe seem rather more equivocal. Evidence was subsequently presented to the Commons that intercepted information had led directly to the arrest, torture and execution of Italian nationalists by Austrian authorities. In a series of cartoons, *Punch* ridiculed the Home Secretary, depicting him as 'Paul Pry at the Post Office', printing the (fictitious) contents of his own intercepted correspondence, and comparing him to – horror of horrors – French Police Minister Joseph Fouché. The magazine also featured spoof counter-surveillance devices, among them 'Anti-Graham Wafers' (envelope seals) with mocking slogans. According to Marjorie Stone, Charles Dickens also got in on the act – writing on the envelope flap of a letter to Thomas Beard on 28th June 1844, "It is particularly requested that if Sir James Graham should open this, he will not trouble himself to seal it again".

One of the functions of satire is to hold people to account, and accountability is likewise one of the key concerns for surveillance. This can take the form of what is sometimes known as sousveillance – watching the watchers, especially now that we all have cameras ready to hand and the means to broadcast live to the rest of the world. Civil society organisations play an important role here, especially for countries where there is low government accountability, and where citizen dissent is prohibited or otherwise dangerous. It can also take the forms of official oversight, by the judiciary or independent review bodies. To go back to the UK example, this is the remit of the Investigatory Powers Commissioner for directed and intrusive surveillance, and the Biometrics and Surveillance Camera Commissioner for CCTV in public places.[24] Unfortunately, it is not unusual for the regimes most in need of oversight to also display the least transparency.

Guarding the guards, watching the watchers

A phrase that we hear used often in this context is "Who will guard the guards themselves?", and this too originates in satire, and in fact in the work of our old friend Juvenal, where the question in the original Latin is *quis custodiet ipsos custodes* (*Satire* 6.347f., O29f.). The etymology of the word *custos*, meaning 'guard', isn't explicitly associated with watching as *vigil* is, but it comes to be used for watchmen, sentries, and overseers.[25] What we don't hear so often is the context for the question. Juvenal's sixth satire is a diatribe against women. It's incredibly graphic, arguably 'Not Safe For Work' (NSFW), and definitely not safe for children:

---

[23] F. B. Smith. 1970. "British Post Office espionage, 1844". *Historical Studies* 14.54: 189-203.
[24] https://www.ipco.org.uk/; https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner
[25] *Oxford Latin Dictionary*: "custōs ~ōdis"

> *I know what my old friends would say and advise: "lock her up and keep her indoors." But who will guard the guards who get paid in kind to keep quiet about your girl's dalliances; it's a conspiracy of silence. The savvy wife sees to it, and starts with them…"*

In 2025, this reads more like an incel complaint or the kind of misogynist soundbite we might expect to see/hear on social media from the likes of Andrew Tate and Laurence Fox. It demonstrates the importance of context in all our assessments of surveillance past and present. It also highlights the complex and problematic role of exposure. The speaker in Juvenal's sixth satire is letting us into the secrets of just how terrible women are, exposing what has previously been concealed. It's a recurrent feature of satire through the ages, but it's also similar to the drive for *publicité* seen in the French Revolution, where the desire to expose the secrets of the aristocracy and other traitors was paradoxically accompanied by – and arguably prompted – an expansion of covert surveillance. We can be thankful that the Revolutionary Comités didn't have access to the Internet.

Indeed, the history and current practice of surveillance is full of paradoxes and competing imperatives, often represented as 'trade-offs.' For society to be safe, we must accept intrusion into our privacy; those charged with conducting surveillance themselves enjoy a degree of secrecy; government authorities and Big Tech companies alike are bent on having access to huge amounts of data captured by digital technology that they can't make sense of without the help of automation and other digital tools.

Until now, surveillance has presupposed a person watching and a person watched, and our terms for its related concepts reflect those different ways of seeing. And yet, as surveillance increasingly entails automated data collection and processing, it would seem that it is less a business of seeing and more one of profiling. Transparency and accountability are certainly still of utmost importance. But as we have discovered, telling people that they are under surveillance can change their behaviour, and this can be precisely the aim.

We might find ourselves tempted to update the opening paragraph of *A Tale of Two Cities* thus:

> *It was the best of times, it was the worst of times, it was the age of safety, it was the age of insecurity, it was the epoch of transparency, it was the epoch of opacity, we were more human than ever, we were more datafied than ever, we all strove to watch without being seen, we had nothing to hide, but everything to fear, in short, the period was so far like the previous period, that some of its noisiest surveillance 'experts' insisted on its being received, for good or for evil, in the superlative degree of comparison only.*

If I were having one of my more arrogant moments, I might even wager that Dickens – as a fan of societal paradoxes and the imagery of surveillance – wouldn't mind all that much.

Further Reading

Gordon Corera. 2015. *Intercept: The Secret History of Computers and Spies*. Weidenfeld & Nicholson. London.

Simon Schama. 1989. *Citizens: a chronicle of the French Revolution*. Random House. New York.

Bruce Schneier. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton. New York

Rose Mary Sheldon. 2005. *Intelligence Activities in Ancient Rome*. Routledge. London & New York.

Marjorie Stone. 2012. "Joseph Mazzini, English Writers, and the Post Office Espionage Scandal: Politics, Privacy, and Twenty-First Century Parallels". *Britain, Representation, and Nineteenth-Century History* (*BRANCH)* - https://branchcollective.org/?ps_articles=marjorie-stone-on-the-post-office-espionage-scandal-1844

Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books. London.