

1

THE CASE OF THE DISAPPEARING BODY

... he that increaseth knowledge increaseth sorrow.

Ecclesiastes 1.18

THE BODY DISAPPEARS

In the words of the poem, ‘Yesterday upon the stair, I met a man who wasn’t there.’ This was meant to be humorous: we can presume its author (one Hughes Mearns, since you ask) wasn’t expecting it to be prescient. Nonetheless, it was.

A century after the lines were composed, we live in a society where *all the time* we meet men and women who aren’t there. Acquaintance used to be face-to-face, a firm handshake, getting the cut of someone’s jib. Trust was a matter of direct, personal acquaintance.¹ But the needs of a complex society, and a set of new technologies, changed all that.

The proportion of significant face-to-face contacts is falling all the time, in what has been called by sociologists the ‘disappearance of the body’. We communicate by phone, email, letter, text; increasingly many of the contacts that make up our society are mediated through technology. Technological representations of ourselves do the interacting.

Mearns' poem has a very intriguing third line: 'He wasn't there again today.' The man who wasn't there makes a reappearance. But how can the narrator of the poem know that the man who wasn't there today was *the same* man who wasn't there yesterday? A nonsensical question? Hardly. If the man in the poem *was* there yesterday and today, it would be a trivial matter of memory to check whether he was the same on each day. Of course, the narrator can be fooled, by identical twins or a master of disguise. But the procedure is simple – recognising the same face, voice and mannerisms. Our brains have evolved over millions of years to do precisely that. And our society has augmented these methods with others to deal with less familiar persons – signatures, seals and passwords.

But a man who *isn't* there? None of these standard high-bandwidth methods will work for the absent presence. Instead, our mysterious bodiless fellow must work through some technologically-constructed version of himself or 'avatar'. Some trace must be left behind which leaves a trail back to the person whose body has disappeared, and those traces can be compared. Having met a man on the stair who wasn't there twice running, we might ask him a question about his mother's maiden name, or demand a digital signature, or get him to key in a digital password or PIN number.

PLENTY OF EVIDENCE

This leads to a strange paradox. A physical presence leaves behind few signs; a handshake in a closed room leaves no trace, except in the memory. Information, on the other hand, persists. In the case

of the physical meeting, if something can be converted into information – via a bug, CCTV, or even DNA – then it could be established that the meeting really took place. Nevertheless, that is always an *extra* procedure, which could in principle be dodged by the people involved. But the man who isn't there must present some tangible piece of information to assure everyone else about his identity, which will remain as a semi-permanent testimony. With the disappearing body, the trace is intrinsic to the meeting taking place at all. No information, no meeting.

Each time a new technology appears that allows people to communicate without an immediate physical presence, a new abstraction is created. It may be an email log, a digital representation of non-verbal communication, a certificate of trustworthiness or whatever. But the abstraction has a concrete form in which the interaction lives on. As our bodies disappear, we leave more of these representations behind. It becomes harder to conceal what we have been doing. The technology boosts our privacy in the present (we don't have to meet people face to face), but it threatens the privacy of our past.

A number of technologies have affected the value, function and feasibility of privacy directly. In a wholly oral culture, spying requires someone to be within earshot of a conversation while simultaneously being concealed. Certain types of behaviour can only be performed in private if there are appropriate spaces protecting privacy. Even very simple technologies such as writing, walls and glass windows have effects on the private space; some give privacy, while others take it away.

The serious academic and legal interest in privacy² really began with the development of portable photographic cameras. With their invention, one could be wandering down the street, in

public, but find one's image captured, and possibly printed using new printing techniques in journals. Although nothing in the situation took place in private before the technology appeared, there was a powerful intuition that one's privacy had somehow shrunk. In the nineteenth century, this was new and serious; nowadays, it is an issue only for those unfortunate enough to be of interest to tabloid newspapers. We are all used to our images being plundered, either by photographers or CCTV cameras, and we probably act accordingly. We are perhaps somewhat less likely to spit, pick our noses or urinate in the street, for instance, if we believe that we might be seen doing so (although a quick search through video-posting site YouTube will show many instances of unusual or noteworthy behaviour captured and preserved forever). And the whole point of a CCTV camera is to make us less likely to commit assaults or thefts, crimes which (if we are to avoid capture) have to be performed to some extent in privacy.

In this book, we want to explore the effects of new digital technologies on our privacy. There is no doubt that those technologies have the potential to be very injurious. It is hard to generalise – in individual cases the gains and losses, costs and benefits have to be weighed in the balance, and we shouldn't prejudge. Sometimes society benefits more than the individual loses. Sometimes the individual gains enough to justify the sacrifice of privacy. Sometimes the loss of privacy translates into a loss for society and a gain only for the state or the corporation. Very rarely is the effect catastrophic. And the costs and benefits vary; all governments misuse some data, and all governments use other data wisely, but one would be sensible to take different precautions depending on where one was. The demands of, say, the United States, France, Iran, China, Russia and North Korea are not the

THE CASE OF THE DISAPPEARING BODY

5

same, and each government has different aims, different ideologies, different dogmas and different scruples in dealing with its citizens.

Costs and benefits are the nub of the classic type of privacy problem – there are many tangible benefits to be gained by allowing intrusions into one’s life, but there is also the intangible worry. We simply find it hard, as humans, to balance the tangible benefits and the intangible costs. In an evil dictatorship, one has a good idea of how personal information will be used, and so can plan accordingly. But in a capitalist democracy, it is much harder to decide how information will be used in the future. The benefits are there for all to see; the costs are not. This may be why our defences are so often down when our privacy is threatened.

Legislation is rarely the answer to our online problems. The law is intended to constrain technologists, but equally the technological capabilities constrain what the lawyers and the legislators can achieve. This rapidly evolving and unstable situation affects our understanding of privacy itself.

Applying apparently well-understood political principles is surprisingly hard in cyberspace, where we often find ourselves having to approve or disapprove of an outcome we never anticipated, or alternatively find ourselves having to decide about a principle that never seemed controversial or even relevant before.³ Where do our rights to free speech end? Do you have an inalienable right to deliver an online lecture in the US to an audience in China? Do the disadvantages incurred by those who lack computer literacy or training fatally undermine their rights to just treatment by society? How far is a society justified in promoting computer literacy? To what extent is it reasonable for a technophobic refusenik to opt out of an information society? Is there a

difference in kind between unauthorised exposure of, say, a photograph by hand to a few dozen people, and uploading a digital image to a website that receives thousands of visits a day?

Important questions of principle appear suddenly from nowhere as a result of technological development, and one either has to reinterpret old principles radically in the new space, or start to think anew. Google is responsible for about half the Web searches made worldwide; finishing low down in Google's page rankings can dramatically reduce visits to a site. What responsibilities does Google have for ensuring equitable treatment? Google's PageRank algorithm works by analysing the eigenvectors of the Web's link matrix – are any principles of fair and equitable treatment somehow breached in the design of the algorithm? Did any moral philosopher ever wonder about the rights and wrongs of eigenvector analysis (our guess: an emphatic no)? What about the methods Google needs to use to ensure that the ranking isn't rigged? There have always been recommendation systems with consequences for those being recommended – financial analysts picking stock market winners, for instance – but none so central to a space or activity as Google is to the Web.

Is privacy a private good or a public good? If an individual cedes his privacy, for example by keeping an explicit blog, is that a free choice of a sovereign individual, or a betrayal of an important principle? Do we have duties not to give our information away, in order not to weaken the idea that one's identity and personality should be inviolable? Should we refrain from using credit cards, joining loyalty schemes, using e-government websites? All of these constitute a semi-permanent record of our business.

There are no right or wrong answers, except to say that the study and science of the Web has to be deeply interdisciplinary,

involving lawyers, technologists, sociologists, policing and security experts and philosophers reasoning and cooperating together to try to discern and understand the new world we are creating. The consequences of principles are important evidence in judging their fitness, and these can be very different online than offline; we may have to rethink our principles, although the basic premises of the arguments remain the same.

WHAT IS ON THE HORIZON?

Privacy often clashes with other values that we consider important. In particular, information that may erode our privacy could also promote efficiency. For instance, in many major cities, particularly in crowded Europe and Asia, traffic congestion is a serious and expensive problem. Lives are constantly put at risk, not only from the pollution that idling engines cause but also from delays in getting emergency services to their destinations. Knowing where cars are is clearly important for traffic control, and technology has a role to play. This is hardly science fiction – in 2006 a committee of Members of the European Parliament recommended adoption of the eCall in-car system which logs accidents and locates the nearest emergency vehicles, which they claimed could save 2,500 lives per year.⁴ IntelliOne, an American company, has developed a traffic monitoring system that locates mobile phones in cars twice per second, from which it can work out how fast the car is travelling, and therefore where the traffic snarl-ups are. It can even tell the difference between a traffic jam and a red light.⁵

It is helpful for an organisation to know what information its employees need, and so monitoring the webpages that they

download is useful. Similarly, monitoring emails via keywords is also valuable; particular queries can be sent to the people who can best deal with the problem. But do we really want our bosses to know what we are looking at, and reading our conversations?

Electronic tagging, of animals, children, property or criminals is becoming increasingly popular (for different reasons) in order to keep track of their whereabouts. But for the law-abiding, tagging could compromise privacy; taking the dog for a walk, going for a day out with the children or even carrying around tagged valuables would tell some sort of database where one is. The criminal is tagged to prevent the breaking of a curfew or condition of release, which is all very well, except that there may be a legitimate yet private purpose in travelling somewhere. The presumption that criminals forfeit *all* rights to privacy as a result of their crimes is a very harsh one unsupported in most jurisdictions. And suppose the crime in question was a political crime?

The information involved can be extremely mundane, but in the right context and the wrong hands very useful indeed. And it may be hard in advance to realise what potential there is for undermining privacy. You don't need supercomputers.

Our homes are host to many small, relatively stupid, relatively powerless computing devices, embedded in household goods. Such gadgets, linked together, can create surprisingly intelligent and flexible behaviour, to keep heating costs and environmental damage down, or to deploy resources intelligently to save money. Five minutes before it goes off, the alarm clock could send a message to the kettle to switch on, and the toilet seat and towel rail to warm up. Activating the shower might start the toaster. The coffee machine might sense when coffee had been poured and then send a message to the car ignition. In the car the seat belt might tell the

THE CASE OF THE DISAPPEARING BODY

9

garage door to open, while the garage door turns the central heating down. Nothing in that chain of systems is doing anything more complex than sensing things about their own use, and sending basic messages to other gizmos. Out of all that simple activity comes a sort of cleverness in the arrangement of the house.

Probably no-one would want an intelligent house; rather, the point is that information is being created that can be monitored, and the systems around you could be telling the world what is going on in your home. Domestic activity usually leaves little trace; snoopers are often reduced to relatively coarse methods of detection, such as scrabbling through litter bins. But a coffee machine that tells other household devices about itself could potentially be used to tell observers how many pots of coffee are made during the day, a much finer-grained detail of household life which, together with other details could be used to paint quite an accurate picture. Your coffee machine could be used to spy on you.

Computers are getting smaller and smaller, and can be made of, or fitted into, many new and interesting materials. The possibilities are endless, but so are the dangers. For instance, the field of electronic textiles or 'washable computing' provides all sorts of fascinating futures. Fabrics that can monitor vital signs, generate heat or act as switches suggest limitless possibilities, from the ridiculous – clothes that change colour constantly – to the useful – a jacket that recharges your mobile phone. Textronic's 'textro-polymer' is made of fibres that change their resistance as they are deformed or stretched, and so can detect pressure.⁶ Very handy – but imagine a bedsheet that was able to detect, and broadcast, the number of people lying on it.

The information gathered by such devices has many important, interesting and genuinely useful purposes, and so they will

continue to proliferate. But as they do, so will the dangers. The spy of the future will not be a shabby man with binoculars or a telephoto lens; tomorrow's spies will be coffee machines, bed linen and clothes.

And we shouldn't assume that we will spot the dangers in advance. If the short term benefits of technology are good enough, we tend not to question them. Had the government demanded that we all carry around electronic devices that broadcast our whereabouts to a central database, that the information should be stored there indefinitely, and that the police should be able to access it with relatively minimal oversight, there would have been an outcry. But in the real world most if not all of us carry such devices around voluntarily, in the shape of our mobile phones. The benefits, we generally reckon, outweigh the costs – which they probably do, but that is merely luck. Precautions against misuse were not discussed widely. We sleepwalked into the danger.

CROOKS AND NANNIES: CRIME AND SURVEILLANCE IN THE REAL WORLD

This is all hypothetical so far; are there any specific examples of apparent threats to privacy from digital technologies? Here are a couple of instances where computing systems provide a new source of worry about our shrinking private space, one patently dangerous, the other less obviously so. Both examples were taken from a particular newspaper from a date late in 2005 chosen at random.

THE CASE OF THE DISAPPEARING BODY

11

The first concerns identity theft. The article in question, subtitled 'Privacy laws gain support in America, after a year of huge violations',⁷ begins by drawing a disturbing analogy between the industrial revolution and our own IT-driven development.

In the industrial age, factories spewed out soot and sludge that polluted the environment; in the information age, companies leak data that can also expose the public to harm. When it came to pollution, politicians and even industrialists eventually agreed on the need for regulation to keep factories in check. This is now happening for privacy regulation in America.

Identity theft cost the US upwards of \$50 billion a year as early as 2002. This has been an obvious danger for some years now, and the European Union, with its more careful, less swashbuckling politico-legal culture, has traditionally taken it much more seriously. Indeed, 1998 nearly saw a trade war break out between the US and the EU over the EU's supposedly over-Draconian privacy directive which demanded companies allow their customers to alter incorrect data held about them. But American business is now coming round to the European point of view.

What changed in the interim is the discovery of the size of the problem, but even that was something of an accident. California, more liberal and namby-pamby than most American states, pioneered a privacy law demanding that individuals had to be notified whenever a company discovered that data about those individuals had leaked. Until then, a company compromised by hackers did not have to inform anyone, not even victims or law-enforcement agents, of the breach. Opponents of the measure complained that it would create a bad environment for business, and businesses would flee for other states. What actually happened was that the law began to bite.

February 2005 saw ChoicePoint, a large data collection agency which holds nineteen billion records, 'fess up. It told 145,000 people that it had inadvertently given personal data away to fraudsters, including social security numbers (the basic identifier of the individual for the American government). Even then it waited five months after the discovery of the problem to inform those affected, of whom 750 had already spotted some fraudulent activity.⁸ Later that month the Bank of America admitted it had lost data tapes with personal information about one million government employees, including some members of the Senate (this at least was accident and not fraud).⁹ In June came the revelation that information about forty million credit card accounts had been stolen.¹⁰ Small wonder that by the end of the year, businesses themselves were begging Congress to pass a federal privacy law.

Firms routinely collect more data than they need, keep it unencrypted and without even basic password protection, and for too long. Security is not the answer to this; it is of course necessary, but not sufficient. As privacy expert Charles Raab memorably put it:

... it is no comfort to a privacy-aware individual to be told that inaccurate, outdated, excessive and irrelevant data about her are encrypted and stored behind hacker-proof firewalls until put to use by (say) a credit-granting organization in making decisions about her.¹¹

The temptations for crooks are immense, because even though the data is potentially valuable in itself (which is why firms keep it), it has other uses. Most obviously, knowledge of credit card or bank details can be used to extract money from an account.

THE CASE OF THE DISAPPEARING BODY

13

The scary part is that such data plays the extra and important role of identifying its subject. An identification system needs to pick on some aspect of an individual that will be very hard for other people to fake. Identity theft involves the thief extracting enough knowledge about the victim's confidential affairs to plausibly pass as the victim; the thief can then behave illegally or suspiciously, all the while understood by the system as being someone else. This is an inevitable consequence of, and made easier by, the disappearance of the body. Such illegal behaviour might not harm the victim directly; for example, a money launderer might open a bank account in a victim's name to deposit ill-gotten gains and withdraw them in a harder-to-trace form. Technically, such a scam actually makes the victim richer, at least temporarily.

Identify theft is a worry because it is comparatively hard to prove, as it is the victim's identity that is in question. Furthermore, the crime can happen without anyone being aware of it for a while; even something as basic as unauthorised use of credit card details may not be discovered until the thief bumps up against your credit limit, or you get your credit card bill some weeks later, in which time you or your bank could have lost an awful lot of money. Finally, because the behaviour that identity thieves indulge in reflects badly on you, you may gain a bad record or reputation as a result of the theft. You may find yourself inconveniently on a credit blacklist, or dangerously on an FBI wanted list, and yet it is hardly possible to check. Someone with a bad credit record can take years to regain their good name, while someone who is thought to be a terrorist might be blissfully unaware of the danger until they are surrounded at gunpoint by highly-trained agents at JFK Airport. At a time when law enforcement and habeas corpus measures are evolving rapidly as part of the War on

Terror, the end result might be weeks or even years in prison with precious few ways of establishing innocence. After all, it is not a case of proving that you are who you say you are; you have to prove that there is another person who has been masquerading as you, a much harder task.

Identity theft is a great concern to many people, and is a well-known example of what can happen when private data falls into the wrong hands. The invasion of privacy is the means to a criminal end: the main aim is something else, be it straightforward theft, money laundering, fraud, creating a disguise, illegal immigration, terrorism or what have you. But our second news story shows that the invasion of privacy may sometimes be exactly the point.

The rapidly greying population of Japan is trying to cope, technologically, with its demographic shift.¹² Average life expectancy, currently eighty-two, is growing by 2.5 years each decade while the Japanese birth rate is one of the smallest in the world. Add to that the Japanese aversion to immigration to produce the spectre of a society, in not many years' time, with an unusually large number of elderly citizens and relatively few younger people to provide care. The Japanese solution, we should not be surprised to hear, is to provide incredible techno-gadgets to take on some of the burden. The *Economist* highlights a number of products, of which three in particular are of interest to us.

Synclayer has a system with which elderly people can monitor vital signs such as blood pressure and temperature, and send them at a constant rate to the health services for automatic monitoring. Any indications of danger can then be acted upon immediately. Another system by Synclayer provides a sensor that detects particular movements, for instance, the opening of the fridge door.

Every time the elderly person opens his or her fridge, a message is sent over a Local Area Network (LAN) that the door has opened, and the time is stored in a database. Relatives or health workers can then monitor activity and check up if things are too quiet. Zojirushi, NTT DoCoMo and Fujitsu have developed the iPot, an electric kettle that keeps water hot all day for the making of tea or miso soup (and a gadget emphatically not to be confused with the marijuana-scented MP3 player¹³). Such kettles are common in Japan, but this one transmits a message to a server by wireless whenever the kettle is used, and a twice-daily report is sent to a designated mobile phone or email address of a relative or carer.

The Spy in the Coffee Machine was chosen as the title of this book, based on the coffee machine scenario from the previous section, as used in an invited talk given by one of the present authors. The scenario was technologically plausible, if perhaps unlikely as a serious attempt to invade privacy. Yet while we were pitching the proposal to Oneworld publishers, something very similar was actually reaching the market. Of course, the iPot is an extremely creative solution to a serious problem, and the invasion of the privacy of the elderly people involved will be with their permission. The information gathered will be used for their benefit; if they are incapacitated for any reason, then their inactivity should be detectable within a few hours, which may make the difference between life and death. We certainly do not wish to suggest Synclayer or Zojirushi have sinister intentions.

But look at the technology to monitor mundane activity. Tiny computers and sensors, wireless networks and the Internet all come together to enable information about making coffee or opening the fridge to be transferred instantly to a remote observer, who need not even be in the same country.

And it should not be assumed that one can merely avoid using such applications. One can, of course, not allow one's carers to install an iPot. But so effective is miniaturisation that one can be spied upon by all sorts of people in all sorts of ways. For instance, in the United Kingdom, microchips capable of assessing the weight of rubbish have been fitted to thousands of the wheelie bins that are used to store household waste before it is picked up by dustcarts run by local councils. A number of councils have distributed bins that can transmit information to a central database about the disposal practices of individual families. The chips are fitted to the lip of the bin and scanned as the bin is tipped into the dustcart. In theory, the idea is to monitor the number of bins that dustmen have emptied, and to judge disputes between neighbours. But if the dustcart also contains weighing equipment (and some do), then the weight of rubbish disposed of could be linked to an individual household.¹⁴

When the story broke, some raised civil liberties concerns, but they have to be balanced against monitoring waste disposal and improving Britain's poor recycling record. Health care, the environment and, of course, security against crime and terrorism are perennial reasons for introducing privacy-invading technology. It is extremely difficult for someone to evade this sort of monitoring. Merely residing in South Norfolk or St Helens makes you liable to be snooped on by your own bin.

THE THREAT OF THE DIGITAL

Why do digital technologies in particular threaten privacy? Much has to do with the ways that information is represented, and how

it is communicated. Digital information lasts a long time, effectively forever if it is periodically copied, backed up and stored using up-to-date formats. Copying is simple and accurate, and transfer from one person to another trivial. Searching through digital information is fast; discovering a tiny number of references to a person in a large database, virtually impossible to spot with the human eye, is a simple matter with a computer. Information that is harmless on its own can be placed in significant new contexts. While from the subject's point of view, it is hard to know when privacy has been breached, harder still to determine who is responsible, and there is no central authority from which to obtain redress.

Meanwhile, with its distributed structure and cleverly-designed architecture, the World Wide Web is rapidly becoming the information repository of choice. This increases risk as it brings together under one virtual roof more information about you than other more traditional repositories. It is possible to build up a very comprehensive picture of you from your web presence. And for some reason that sociologists would be more qualified to address, the Web attracts many types of subterranean behaviour. The tendency of people to publish compromising material, or to engage in risky behaviour, seems, anecdotally at least, highly prevalent online.

Compare the digital with other more usual methods of transferring private information. *Paper* is bulky, hard to copy and copying is not always accurate. Comprehensive information about oneself is not usually stored in one physical document. *Human memory* is notoriously fallible, and hard to transfer – it usually involves the time-consuming representation of the memory before the transfer can begin, so even if the memory is accurate

the representation of it may not be. *Gossip* is hard to suppress – it has been compared to the many-headed hydra of Greek myth, in that whenever one head it chopped off, two more grow in its place. However it is typically inaccurate, at least after a relatively small number of transfers between people (not that the inaccuracy seems to bother them), and it can be hard to find the gossip you need to order – it is supply- rather than demand-driven. The transfer of digital information is far more powerful.

PRIVACIES

The assiduous reader will have noted that privacy has not been defined – we have talked about threats to it and invasions of it, not about what would be or is being invaded. But privacy is a many-splendoured thing, as we will see in this book. A dictionary definition won't quite nail the topic down as we would like.

The usual understanding of privacy is to do with a subject's control of information about him or herself. Knowledge about a person is often made into a document such as a medical record or a photograph. If the person has a measure of privacy, then it is possible to restrict the distribution of the representation of that knowledge.

Information about a person could, of course, be false, out of date or badly maintained, or because of a simple error such as a confusion of names it might be thought to apply to the wrong person. Information can be used to restrict someone's freedom of action, again either intentionally or otherwise. Someone could be coerced into behaving in a particular way with a threat to release certain information, or someone's choices could be diminished.

THE CASE OF THE DISAPPEARING BODY

19

Animal rights activists have been known to release personal information to intimidate opponents.¹⁵ In a number of cultures publicity about HIV status, homosexuality, or illegitimacy can result in social stigma. In the Soviet Union, someone's family background or party membership could determine their official status.¹⁶ Politicians live under the constant threat of the effect of the information about them.

But privacy is not straightforwardly definable in simple terms of access and control of information. One has private spaces, takes private decisions, has freedom of thought, has private property – and all of these have online analogues. When cameras became quick enough to allow photographs to be taken without an elaborate pose, a new issue arose as to whether people – public figures, perhaps – had any kind of right to prevent others taking a likeness without consent, even in a public place. One can't step into a public place without expecting to be *seen*, but the recording of that moment is an entirely different matter. There are many cultures which lack the assumption that one cannot be private in a public place; it is a Western dogma that one's privacy cannot be invaded if one is voluntarily in public.

Privacy takes a number of shapes, and can manifest itself in several different ways. One's house is a literal private space, where one would hope to control access. One's body is private; naturally one would want to restrict others' physical access to it, but also one often wishes to avoid even being seen. Many people wish to keep knowledge about themselves private, sometimes for pragmatic reasons (bank details), but sometimes for reasons that are less tangible (salary). For some, privacy is an absence of people. For others, it is about carving a small, controllable space out of a wider untamed one. Others wish to avoid interference with their

decisions, or do not want to be held accountable for some of their acts. Still others want to be free to exchange their property. Some wish to subvert society without risking punishment.

Our second reason for being wary of definitions is that privacy is not value-neutral. It is not an unalloyed good, although much privacy discourse assumes it is. Some people and some cultures regard privacy with suspicion. Most of us at one time or another seek privacy, but at other times shun it without inconsistency. In general, in the West at least, the popular opinion of privacy has become more positive over the centuries. Privacy is (beginning to be) protected by the law, and many social trends take us in the direction of greater privacy, such as the reduction in the size of families living in a single household. But on the other hand, many use new technologies to expose themselves to view to a previously unimaginable degree. Webcams and *Big Brother* provide almost unlimited access to some exhibitionists, while very few people will pass up the opportunity to appear on television. Television hosts such as Jerry Springer base careers on the willingness of bizarre and damaged people to wash their dirty linen in public. Even very recently bereaved people will talk about their loss on TV news programmes. Most academics would kill to be interviewed about their work, even as they cling tenaciously to the copyrights on their unread articles. Many diaries are written to be read (ultimately). As Wilde put it, 'there is only one thing in the world worse than being talked about, and that is *not* being talked about.'

This ambivalence about publicity and privacy dates back to the key founding moments of Western civilisation. For instance, Plato, in his *Republic*, imagined a society where the children of the ruling class would be educated in common and quarantined from

the usual family life. Meanwhile, Aristotle's *Politics* makes a modern-sounding distinction between the private domain of the household and the public space of the *polis*, the democratic decision-making forum where all citizens' voices were heard. But Aristotle's view was that the private domain was uninteresting and dull – boring household governance – whereas the *polis* was where it was at. This preference for the public was preserved by etymology – the word 'private' is related to Latin 'privare', to deprive, and the connotation of privacy for classical thinkers was very much to do with deprivation rather than voluntary withdrawal.

A third privacy-related dilemma is that it benefits different agents. If you wish something you do to be unknown to the rest of society, then you are the beneficiary of your privacy. On the other hand, if you wish to do something that many consider disgusting, such as urination, in public, then you will be admonished that that is an action that should only occur in private, and in that case your (enforced) privacy benefits everybody else, and may in fact frustrate your reasonable or unreasonable exhibitionism (it is only a couple of centuries since seeing a monarch 'at his stool' was considered a great privilege). Sometimes privacy is a space into which one can gratefully withdraw, sometimes it is the space where one is corralled to prevent offence. One can be either comforted or frustrated by decorum. Feminist thinkers have complained that the privacy of 'one's own home' facilitates a great deal of abuse of wives and children by husbands, and entrenches patriarchy.¹⁷

Privacy can also be aggregated. Groups can benefit from privacy (families, say) without necessarily everyone within the group benefiting (downtrodden wives). Within a group one can be both private and not private; one can be private from the outside world,

yet visible and accessible to others in the group. Even within a private group, one can require privacy – many people seek privacy away from their family, even when they are already within the paradigm private space, their own home.

Fourthly, privacy is very similar to a number of other concepts, and is hard to disentangle. For instance, there are strong connections between privacy and secrecy, but we should not confuse them. A state secret is secret but not private; one's clothes are private but not secret. Those who conceive of privacy as a lack of accountability merely want to make their own decisions about, for instance, marriage or money or the way they manage their children without interference – they are not necessarily bothered about who knows about them. Structurally, there is very little distinction between privacy and loneliness, or ostracism, or deprivation, or isolation. The difference may well be the attitude we hold towards the private state, rather than any structures or external relations for the subject. Privacy often carries with it a notion of choice. One chooses to be private, whereas one does not (usually) choose to be lonely.

For all these reasons, we are wary of defining privacy, because it would be hard – we suspect impossible – to give necessary and sufficient conditions, especially as technology changes the context so rapidly. This book, focusing on technology in twenty-first century Western democracies is certainly not going to attempt to nail down such a slippery concept. Nevertheless, it is well to note that any concept whose definition and properties are tightly interwoven with social practice has a cultural location and a history, and we must expect that the concept will change with the context.

One final caveat: it is quite clear that many people wish to obtain or preserve privacy because they are performing actions

THE CASE OF THE DISAPPEARING BODY

23

that are illegal or otherwise damaging to others. Similarly, many people, organisations or authorities wish to invade privacy for profit or political gain, whatever rights they trample upon. Such cases of transgression of the law or accepted moral codes are pretty straightforward to judge (if hard to prevent in practice), and we do not wish to focus upon them. The point about privacy is that it raises *hard* cases; people want privacy for perfectly good reasons, and others want information for equally good reasons. Technology will alter the delicate balance between such people as it evolves. In this book we are interested, primarily, in how to prioritise dealings made in perfectly good faith. When most people are law-abiding and public-spirited, how do we avoid risk, and how should we prevent illegal actions in the future without demonising those in the present?