The Moral Case for Stealing Data

Dr Victoria Baines, IT Livery Company Professor of IT

20th May 2025

History tells us that we can sometimes have unexpected, unauthorised access to data. In the last eight hundred years there has been much speculation about the nature of the relationship between Kings Richard I of England (the Lionheart) and Phillip II of France. Some have held that they were lovers, based on the following text in the *Gesta regis Henrici Secundi Benedicti Abbatis*, the chronicle of the reigns of Henry II and Richard I:

> *Ricardus dux Aquitanniæ, filius regis Angliæ, moram fecit cum Philippo rege Franciæ, quem ipse in tantum honoravit per longum tempus, quod singulis diebus in una mensa ad unum catinum manducabant, et in noctibus non separabat eos lectus. Et dilexit eum rex Franciæ quasi animam suam; et in tantum se mutuo diligebant, quod propter vehementem dilectionem quæ inter illos erat, dominus rex Angliæ nimio stupore arreptus admirabatur quid hoc esset.*
>
> *Richard, duke of Aquitaine, the son of the king of England, remained with Philip, the King of France, who so honoured him for so long that they ate every day at the same table and from the same dish, and at night their beds did not separate them. And the king of France loved him as his own soul; and they loved each other so much that the king of England was absolutely astonished at the passionate love between them and marvelled at it.*

This closeness did not, however, stop them going to war. In July 1194, their forces met at Fréteval in the Loire Valley. When Richard ambushed Philip, the French king fled, abandoning his baggage train which, according to Roger of Hovedon, also contained his archives:

> *Vast treasure of the King of France was also taken, with the furniture of the King's chapel, and the papers of all the subjects of the King of England who had deserted him and become adherents of the King of France and Earl John.*

While seizure of information does not appear to have been the primary aim, it gave Richard a strategic advantage. The papers on the deserters may have contained sensitive information, what we would now perhaps categorise as 'personal data'. One can see, for instance, how information on their geographical locations might be used to pursue them, or on their financial resources to extort them. Sensitive data, however it comes to be subject to unauthorised access, can endanger.

Some historians see the Battle of Fréteval as a defining moment in European data history. One belief is that it led to Philip's establishment of standing archives, the Trésor des Chartes. This has been challenged by the French National Archive, which clarifies that the first mention of a permanent depository for documents doesn't appear until 1231. In around 1205 Philip did begin compiling a cartulary, a register in which important documents were transcribed. So, one might at least be able to infer that data loss at Fréteval and perhaps elsewhere may have encouraged the king to alter his practices by keeping what in modern digital terms would be termed a 'backup copy.'

This episode highlights how, when data is kept in a physical artefact, it can literally be stolen. Down the centuries, various means have been used to protect repositories of information and knowledge, such as the chained libraries of the medieval period, and curses written into the books themselves. The laborious work of the scribe and even the early modern printer hindered attempts at swift, clandestine copying – although there is ample evidence that copyists 'interfered' with texts by adding their own insertions, comments, and

translations.[1] It has been suggested, most compellingly by Kathleen E. Kennedy (see Further Reading), that medieval copyists are the ideological ancestors of modern hackers, because in a pre-copyright era they treated text-based knowledge as an information commons to be openly distributed and freely recycled. The analogy has its constraints, not least the fact that reading and writing were elite activities until the 20th century in most societies. But it does perhaps help us to consider contemporary preoccupations of knowledge, information, and data protection from diverse historical perspectives.

When it comes to digital technology, it's very rarely the case that the only copy of data is stolen: most often it is copied, just as identity theft more often entails the cloning and reuse of identity credentials. The victim still has the data: the theft consists in the fact that someone else also has it. The physical artefact – if there is one at all – is of negligible value compared to the richly illuminated volumes of earlier eras. Value lies purely in the data stored or transmitted.

Of criminals, spies, and whistleblowers

One obvious motivation for taking data that doesn't belong to us is financial. This is the realm of the cybercriminal. At various points in my Gresham lectures, we have seen how our personal data can be monetised. Our login credentials can be used to gain unauthorised access to our online accounts or sold so that others can. The ransomware attacks so prevalent in the last ten years rely on extorting victims, demanding that they pay a ransom to regain access to locked files, and/or to prevent publication of copied data. Spoiler alert: criminals cannot be trusted to be true to their word on this; restored access is never guaranteed, and data often finds its way onto criminal marketplaces, even if the victim pays up. Unauthorised access to proprietary data on cutting edge research and development can give competitors – be they companies or governments – a commercial advantage.

In the case of the last of these, what we're really talking about is espionage. This may conjure up images of 20th century spy cameras such as the Minox subminiature range.[2] We might describe this as dual-purpose technology: as well as photographing human activity under covert surveillance, they were a means to capture data, copying a document where its physical removal would draw unwanted attention. Whether trade secrets or state secrets, the thief acts in another's interest. They may be freelancers selling to the highest bidder, or direct employees of the benefiting organisation or state.

Obtaining unauthorised access is arguably the most challenging part. In the cybercriminal world, this is the aim of phishing attacks that dupe victims into handing over their access credentials. But what if the access has been authorised? In the cybersecurity world we call this 'insider threat', and we tend to profile insiders variously as financially motivated or personally aggrieved. In the intelligence world, the category may also include operatives who are compromised, for instance by being taken prisoner or otherwise influenced. In all types of organisations, those who copy and/or leak data may be ideologically motivated.

People in this last category are often referred to as whistleblowers. The metaphorical use of this terminology is comparatively recent: the Oxford English Dictionary cites its earliest evidence for *whistle-blower* from 1936, in *Daily News* (New York) and for *whistle-blowing* from 1971, in New Scientist. One reference online to coinage of the term in the Elizabethan era appears to be erroneous.[3] The imagery of blowing the whistle appears to be associated both with stopping play in sport and either sounding an alarm or compelling action in a law enforcement context. Whistleblowing has come to denote the exposure of alleged wrongdoing, whether within an organisation or outside it. Insofar as it often involves the revelation of information that has previously been kept secret or not widely known, it bears some similarity with the practice of denunciation explored in my previous lecture, *How Surveillance Works*.[4] The French *revolutionaires* who used evidence from intercepted letters to denounce aristocrats and other traitors doubtless viewed themselves as exposers of wrongdoing.

For modern whistleblowers, evidence to corroborate claims is no less important. 1971, as it turns out, was a

---

[1] https://brewminate.com/medieval-hackers-scribes-copiers-and-the-free-flow-of-information-in-the-middle-ages/
[2] https://www.cia.gov/legacy/museum/artifact/minox-b-camera/
[3] https://dq.im/whistleblowing-more-than-just-hot-air/#:~:text=It%20is%20a%20term%20coined%20in%20the,attempt%20to%20prevent%20illegal%20or%20immoral%20activity.&text=In%20summary%20this%20case%20involved%20an%20employee,unfairly%20constructively%20dismissed%20because%20of%20protected%20disclosures
[4] https://www.gresham.ac.uk/watch-now/how-surveillance-works

big year for whistleblowing. It was the year that lawyer and activist Ralph Nader hosted the Conference on Professional Responsibility in Washington, DC, thereby starting the movement towards legal protection of corporate whistleblowers in the US.[5] It was also the year that former RAND Corporation analyst Daniel Ellsberg leaked to the New York Times a report he co-authored on the Vietnam War for the US military. What came to be known as the Pentagon Papers revealed a number of details about US involvement in the conflict that had not been made known to the public or the media – among them, that the geographical scope of US operations was wider than publicly reported, and that the Johnson administration knew from early on in the conflict that their resources were insufficient to win.

For me, two key points stand out in this case. The first was the necessity for Ellsberg to 'steal' – or at least photocopy – data in order to prove that what he was alleging was true. Without evidence, allegations could easily be denied. But removing data without due authorisation has consequences, particularly when the injured party is the government. In the case of classified data such as intelligence reporting, the thief is likely to face criminal charges including theft of government property and violations under espionage legislation. At worst, they can be judged a traitor. Given the risk and impact on government whistleblowers, it's fair to say that none of them decide to do it lightly.

Secondly, whistleblowers' revelations are very often mediated rather than being released to the public *en masse*. Motivations for this include making huge volumes of technical material more accessible to a non-specialist readership, legal risk to the publisher, protection of sources, and – dare I say it – retention of reader engagement over time through serialisation. Media outlets are, after all, focused at least in part on their circulation. In the case of the Pentagon Papers, the 47 volumes of relevant documents were declassified only in 2011, a full forty years after highlights were published by the media (see Further Reading). This is not to say that media outlets behave dishonestly in selecting material for our consumption: simply that we are often unable to make our own unguided assessment of the data that is exfiltrated as evidence of wrongdoing. As it happened, a legal memo, unpublished until 2023, reveals that New York Times reporter Neil Sheehan deceived Ellsberg, secretly making copies of the 7,000-page report after promising not to.[6]

Ellsberg's unauthorised removal and distribution of classified data set in motion a chain of events that in turn resulted in public debates about freedom of the press and the inviolability of the US Presidency. Nixon served an injunction on the New York Times to stop it publishing further excerpts, but this was subsequently lifted by a ruling of the Supreme Court. Ellsberg was charged with offences under the 1917 Espionage Act. Charges were dropped in light of evidence that two of the Watergate conspirators had broken into the offices of Ellsberg's psychiatrist to obtain files, and that The White House had ordered Ellsberg's communications to be illegally wiretapped. The ruling was not that Ellsberg was innocent, but that there was a mistrial due to procedural irregularities. Recordings of the President's telephone conversations on the day of publication reveal that legal action was under discussion very early on[7]:

> *NIXON: Well you know - uh, [stammering] it may not have the effect they inten - they - the thing though that Henry - that to me is just unconscionable - this is treasonable action on the part of the bastards that put it out.*
>
> *KISSINGER: Exactly. Mr. President.*
>
> *NIXON: Doesn't it involve secure information, a lot of other things? What kind of - what kind of people would do such things?*
>
> *KISSINGER: [Unclear] it has the most - it has the highest classification [unclear]*
>
> *NIXON: Yeah, yeah*
>
> *KISSINGER: It's - it's treasonable, there's no question - - it's actionable, I'm absolutely certain that this violates all sorts of security laws.*

Excerpt from transcription of President Nixon's phone call with Henry Kissinger, 13 June 1971, 3:09 p.m.

> *EHRLICHMAN: Hello, Mr. - Mr. President, the attorney general has called a couple times, about these New York Times stories; and he's advised by his people that unless he puts the Times on notice - uh, he's probably gonna waive any right of prosecution against the newspaper; and he is calling now to*

[5] https://whistleblowersblog.org/features/an-unheard-of-dream-ralph-naders-50-years-in-whistleblowing/
[6] https://theintercept.com/2023/10/07/pentagon-papers-daniel-ellsberg-neil-sheehan/
[7] https://nsarchive2.gwu.edu/NSAEBB/NSAEBB48/nixon.html

see if you would approve his - uh, putting them on notice before their first edition for tomorrow comes out.

NIXON: Hmmm.

EHRLICHMAN: I realize there are negatives to this in terms of the vote on the hill.

NIXON: You mean to prosecute the Times?

EHRLICHMAN: Right.

NIXON: Hell I wouldn't prosecute the Times. My view is to prosecute the Goddamn pricks that gave it to 'em.

Excerpt from transcription of President Nixon's phone call with John Ehrlichman, 13 June 1971, 7:13 p.m.

Where the basic offence is that of someone who "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information to be obtained is to be used to the injury of the United States…copies, takes, makes, or obtains, or attempts, or induces or aids another to copy, take, make, or obtain, any sketch, photograph, photographic negative, blue print, plan, map, model, instrument, appliance, document, writing or note of anything connected with the national defense", neither ethics nor perceived public interest are a mitigating circumstance. Despite a clearly stated belief that he 'did the right thing', Edward Snowden is potentially looking at a 30-year prison sentence if he returns to the US; Chelsea Manning, found guilty of sharing thousands of classified files about US military operations in Iraq and Afghanistan with Julian Assange's Wikileaks, was sentenced to 35 years. This sentence was commuted by Barack Obama after she had served 7 years. The material she disclosed included a video file that showed a US military helicopter killing civilians in Iraq.

While it may make legal sense for governments to designate those who leak classified data as traitors, the rhetoric used by some government spokespeople borders on the retaliatory. In a 2016 interview before his appointments by President Trump as Director of the CIA and Secretary of State, Congressman Mike Pompeo said in an interview, speaking directly to the camera, that "*the traitor Edward Snowden…should be brought back from Russia and given due process, and I think that the proper outcome would be that he would be given a death sentence for having put friends of mine, friends of yours, in the military today, at enormous risk because of the information he stole and then released to foreign powers*".[8]

Anticipation of the 'proper' judicial outcome here has the contrary effect of subverting due legal process. Snowden has maintained that he disclosed material only to journalists. The accusation that he released it to foreign powers highlights an uncomfortable truth – that classified data made public can be exploited by those who want to do a country harm, including other states. Reference to Snowden's exile in Russia is also of course pointed: although a statement published by WikiLeaks claimed that he had sought asylum in twenty other countries, the association with the US' Cold War enemy has always been problematic and has become even more so in light of subsequent reports that Snowden was working for a Russian IT company, and geopolitical developments in recent years.[9]

Legal protection for whistleblowers goes back at least as far as July 30th, 1178, when the US (then 'Continental') Congress intervened in the case of naval officers who had been subject to legal retaliation for speaking out about torture of British prisoners of war at the hands of the commander of the Continental Navy:[10]

The committee to whom was referred the petition of Richard Marven and Samuel Shaw, brought in a report, which was taken into consideration; Whereupon,

Resolved, That it is the duty of all persons in the service of the United States, as well as all other the inhabitants thereof, to give the earliest information to Congress or other proper authority of any misconduct, frauds or misdemeanors committed by any officers or persons in the service of these states, which may come to their knowledge.

---

[8] https://www.c-span.org/program/washington-journal/benghazi-investigation-and-hillary-clintons-emails/430143; relevant comments from 23:00.

[9] https://wikileaks.org/Statement-on-Snowden-s-Successful.html

[10] *Journals of the Continental Congress, 1774-1789, Volume 11*, p.732f. https://babel.hathitrust.org/cgi/pt?id=nyp.33433091241004&seq=324&q1=Marven+

Whereas, a suit has been commenced by Esek Hopkins, Esq. against Richard Marven and Samuel Shaw, for information and complaint by them and others made to Congress against the said Esek Hopkins, while in the service of the United States:

Resolved, That the reasonable expences of defending the said suit be defrayed by the United States.

Ordered, That the secretary of Congress furnish the petitioners with attested copies of the records of Congress, so far as they relate to the appointment of Esek Hopkins, Esq. to any command in the continental navy, and his dismission from the same, and also to the proceedings of Congress upon the complaint of the petitioners against the said Esek Hopkins, preferred to Congress through the Marine Committee, as mentioned in their petition.

There is an obvious tension, then, between competing conceptions of moral duty for a government employee. For one set of government actors, doing the right thing consists of speaking out; for another, it is protecting classified information at all costs. Edward Snowden is viewed as a hero by many, an insider who chose to speak truth to power regardless of the impact on his personal safety and circumstances. Over a decade on, questions remain. We still don't know how many files Snowden exfiltrated: estimates range from initial assessments in the tens of thousands to the Defense Intelligence Agency's later conclusion of around 1.7 million.[11] According to any of these, it's clear that the documents made public between 2013 and 2018 constitute a small proportion of the material copied. Why have so few been made public? Mike Pompeo's allegation that Snowden's revelations endangered people also raises a clear ethical quandary. President Obama alluded to this in public remarks a few months after publication, saying that "the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come."[12] I was still working in law enforcement when the story broke, and there was genuine concern – not to say fear – that serving military and intelligence professionals would be harmed as a result of the disclosures. The trouble is that we've not been able to test this hypothesis because any data about this impact is itself highly classified.[13]

In 2016, the US House of Representatives' review of Snowden's unauthorised disclosures reported that "To gather the files he took with him when he left the country for Hong Kong, Snowden infringed on the privacy of thousands of government employees and contractors. He obtained his colleagues' security credentials through misleading means, abused his access as a systems administrator to search his co-workers' personal drives, and removed the personally identifiable information of thousands of IC [Intelligence Community] employees and contractors."[14] This and reports in the media based on an NSA memo that agency employees were disciplined for giving their login credentials to Snowden would appear to indicate that he used social engineering to gain unauthorised access to data (Snowden has denied this).[15] The suggestion that he used underhand tactics shouldn't undermine the veracity of the disclosures per se. But it does perhaps give ammunition to those, including the US government, who challenge his identification as a whistleblower.

In the previous lecture, we explored the impacts of surveillance, how the feeling of being under observation can alter one's behaviour. This is sometimes known as 'chilling effects', and it has been suggested that Edward Snowden's revelations about mass electronic surveillance by the US and UK government led to mass chilling effects online. University of Toronto researcher Jonathon W. Penney analysed views of Wikipedia articles on sensitive topics such as terrorism.[16] What he found was a statistically significant immediate decline in web traffic to these articles after June 2013, when the Snowden's leaks were published. It raises the uncomfortable and paradoxical possibility that bringing this material out into the open actually constrained people's access to information to some degree.

The cases we have discussed above focus on public exposure of government wrongdoing. In the corporate world, it's now seen as a mark of an ethically responsible company to have a process for raising concerns and protecting those who do. But having a whistleblowing policy does not guarantee that there won't be

---

[11] https://www.vice.com/en/article/exclusive-inside-washingtons-quest-to-bring-down-edward-snowden/
[12] https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
[13] https://embed.documentcloud.org/documents/2101905-dia-david-leatherwood-declaration-in-leopold/
[14] https://irp.fas.org/congress/2016_rpt/hpsci-snowden.pdf
[15] https://www.reuters.com/article/net-us-usa-security-snowden/exclusive-snowden-persuaded-other-nsa-workers-to-give-up-passwords-sources-idUSBRE9A703020131108/; https://swampland.time.com/2014/02/13/nsa-leaks-edward-snowden-password/
[16] https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf

retaliation for speaking out. When in 2016 two anonymous letters to Barclays Bank raised concerns about the Chief Executive's decision to hire a former colleague, rather than following established whistleblowing procedures the Chief Executive "personally directed" the company's Chief Security Officer to investigate the whistleblower.[17] This executive reportedly then asked federal law enforcement in the US to try to identify the person who sent the letters, including attempting to obtain video footage of the person buying the postage stamps.[18] When this came to the notice of financial regulators, Barclays was fined $15 million in the US. The Chief Executive was personally fined £642,430 (10% of his pay) by UK regulators and $1.5 million in the US. Barclays also cut his bonus by £500,000. The UK Financial Conduct Authority put the company under special reporting requirements for its whistleblowing systems and controls.[19] This sounds like a good outcome, testament to the courage of that original anonymous letter writer and the process – and perhaps additional people – who brought the resulting misconduct to the attention of regulators. But here, too, chilling effects can be a legitimate concern. As observed by media commentators, 30% fewer whistleblowing investigations were opened by the company's whistleblowing team in 2019, the year following the fines.[20] From a baseline of 364 investigations opened in 2018, the company's annual reports show that it received 67 whistleblowing concerns in 2023 and 69 in 2024.[21] As in highly publicised government whistleblowing cases, in the corporate world also trust can be eroded even when wrongdoing is punished.

Of hackers, hacktivists, and bounty hunters

Unauthorised access to data is, of course, more commonly known as hacking. Over the last few decades, hacktivism has deployed some tactics similar to those of whistleblowers, often committing cybercrimes for ideological ends. As well as claiming responsibility for attacks that have disabled and defaced target websites, affiliates of the hacktivist group Anonymous have declared war on ISIS, targeted the Church of Scientology, and taken down thousands of sites on the Dark Web involved in the distribution of child sexual abuse material.[22] Their moral position is complex, encompassing more than the single issue of anti-government sentiment, perhaps reflecting its status as a decentralised collective. In 2012, it published the hacked personal data – including names, home addresses, email addresses and phone numbers – of members of the Westboro Baptist Church, after the group announced its intention to stage a picket at Sandy Hook Elementary School to promote its belief that a mass shooting at the school had been God's vengeance for same sex marriage equality.[23] In this last case, the motivation for Anonymous' activity appears commonsensical and compassionate to LGBT+ people. One might argue that it justifies the crimes committed; but again, there is no protection for this in law.

There is greater acceptance of 'ethical hacking', a practice which entails identifying vulnerabilities in software, systems or networks and reporting them to the organisation at risk so that they can take remedial action. This process is alternatively known as Coordinated (or Responsible) Vulnerability Disclosure, and it has spawned a new income stream and specialisation in cybersecurity. Big Tech companies offer 'bug bounties', rewards for reports of vulnerabilities. There are clear guidelines for these. For instance, to be eligible for a payout from Microsoft's bug bounty programme, submissions need to include proof, be the first report of an issue, avoid harm to customer data, privacy, and service availability, and give the company time to correct the issue before making it public; reports from automated scanning tools aren't enough, and social engineering and physical security attacks are off limits.[24] Precisely because such schemes can be lucrative – Microsoft offers payments of up to $250,000 for a single vulnerability – things do not always go to plan. It

---

[17] https://www.bbc.co.uk/news/business-46614109
[18] https://www.reuters.com/article/business/barclays-ceo-fined-15-million-for-trying-to-unmask-whistleblower-idUSKBN1IC11A/
[19] https://www.fca.org.uk/news/press-releases/fca-and-pra-jointly-fine-mr-james-staley-announce-special-requirements
[20] https://www.fnlondon.com/articles/barclays-whistleblowing-cases-dropped-by-30-in-year-after-staley-penalty-20200218
[21] https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2023/Barclays-PLC-Annual-Report-2023.pdf; https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2024/Barclays-PLC-Annual-Report-2024.pdf
[22] https://www.nbcnews.com/tech/security/hackers-take-down-thousands-dark-web-sites-post-private-data-n717556
[23] https://web.archive.org/web/20130602225316/http://www.anonpaste.me/anonpaste2/index.php?65e2832b96b888e3#Uxqr8wrq3ljskOY76+ubZQvSmcEtYCbIfZBqWpaGcMI=
[24] https://www.microsoft.com/en-us/msrc/bounty

can be challenging to invite hackers to hack and then demand that they play by your rules. Hackers who find a vulnerability but are not the first to report, or who are ignored by companies, can take revenge when they fail to win a bounty. Perhaps inevitably, the process has also been misused. In 2022, a platform for coordinating bug bounty reports and payouts found that one of its employees had stolen reports to sell on as their own.[25]

Equally, coordinated vulnerability disclosure is only effective if the receiving organisation does something with the information they receive. Failure to remediate puts systems and end users at unnecessarily prolonged risk. As a result, companies that specialise in identifying vulnerabilities often adopt policies and procedures that specify a time limit for receiving organisations to respond to reports and remediate issues, before disclosing them to the wider public.[26]

Deliberate, unauthorised release of personal data is popularly known as 'doxxing'. It's a common tactic of any group wishing to humiliate or harass a target, from abortion doctors to biomedical students to (somewhat bizarrely) celebrities who make a stand against cruelty to animals.[27] It's the digital manifestation of the threatening and silencing statement, "We know where you live", but with the added complication that publication of the details further endangers the physical safety of the target: once the data is out there, it is no longer in the publisher's control; anyone can choose to act upon it. Both the doxxers and those who use the leaked information to harass can claim a moral impetus. But, as the examples above show, moral justifications can be highly idiosyncratic, and certainly not universally shared.

Just as we might feel that Edward Snowden's alleged misuse of colleagues' login credentials crosses the line, so too do we see other instances of methods that could be viewed as harmful and unethical. In 2015, hackers calling themselves The Impact Team exfiltrated the entire customer database for Ashley Madison, a dating platform specialising in adultery. The group demanded the immediate closure of Ashley Madison and a sister service, Established Men. The Impact Team has been described as morally motivated: that's correct, but not quite in the way one might expect. Rather than simply judging the users for their infidelity, a statement by the group pointed the finger at the company for not honouring their promise to operate a private and secure service:

> *First, we expose that ALM management is bullshit and has made millions of dollars from complete 100% fraud. Example:*
>
> - *Ashley Madison advertises "Full Delete" to "remove all traces of your usage for only $19.00"*
> - *It specifically promises "Removal of site usage history and personally identifiable information from the site"*
> - *Full Delete netted ALM $1.7mm in revenue in 2014. It's also a complete lie.*
> - *Users most always pay with a credit card; their purchase details are not removed as promised, and include real name and address, which is of course the most important information the users want removed.*
> - *Other very embarrassing personal information also remains, including sexual fantasies and more*
> - *We have all such records and are releasing them as Ashley Madison remains online.*

When the parent company did not comply, the personal data of 37.6 million users was exposed to public scrutiny. As reported in the media, this led to real world harm for many, even – as Impact Team's assessment above highlights – people who were no longer actively using the platform. Careers, marriages, lives ended.[28] The users were the ones who paid the price, which appears inconsistent with the hackers' professed dismay at their being defrauded. And as with all doxxing, there were parties ready to exploit the data further – in this case, moral crusaders, including (reportedly) an Alabama newspaper in which the names of all local subscribers were printed. Ultimately, we can never know for certain whether the hackers operating under the name Impact Team really did conduct the attack out of moral outrage or to expose perceived wrongdoing. But what this and other unauthorised exposures highlight is that there is often a tension between morality and compassion, public interest and the best interests of individuals.

---

[25] https://www.bleepingcomputer.com/news/security/rogue-hackerone-employee-steals-bug-reports-to-sell-on-the-side/

[26] See, for instance, the vulnerability disclosure policy of Pen Test Partners, whose work in highlighting security issues has featured in my Gresham lectures, especially "Sex and the Internet". https://www.pentestpartners.com/about-us/vulnerability-disclosure-policy/

[27] https://www.straitstimes.com/asia/east-asia/chinese-celebrities-doxxed-by-netizens-after-condemning-animal-abuse

[28] https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked

When is a secret not a secret?

Recent events have demonstrated very clearly that in the digital age, governments find it increasingly hard to keep control of information, even when it is shared on channels perceived to be secure. Journalist Jeffrey Goldberg did not hack his way into a discussion on the messaging app Signal between leading US government figures about plans to attack the Iran-backed Houthi group in Yemen.[29] He was mistakenly added to the conversation by National Security Adviser Mike Waltz. In previous lectures, particularly "Cybersecurity for Humans" from 2023, we discovered how protecting information, networks, and systems relies not only on technology but also following due process and ensuring that we address human vulnerabilities.[30] Using an end-to-end-encrypted app means that messages can be read only by those who are members of the group. But, as the Signal 'leak' illustrates, all the technical security measures in the world cannot eliminate the risk of failures in process and human error.

While the Trump Administration maintains that no classified information was shared in the group, the transcript is nevertheless revelatory and arguably embarrassing. Vice President JD Vance's and Secretary of Defense Pete Hegseth's highly informal references to "bailing out Europe again" and "PATHETIC" [original emphasis] "European free-loading", Hegseth's distribution to the group of the precise timetable for airstrikes ("THIS IS WHEN THE FIRST BOMBS WILL DEFINITELY DROP"), and use of macho emojis when targets were hit were clearly not intended for a wider audience, let alone a public one. In this context, Hegseth's reassurance on the chat that "We are currently clean on OPSEC" [operational security] unfortunately and somewhat ironically did not apply to the channel on which it was uttered.

Messages in the group were set to disappear after a specified period of time: in the material published by Goldberg, this was changed from one week to four weeks. As emerged also in the inquiry into the UK government's response to Covid-19, use of unofficial messaging channels can frustrate oversight and accountability efforts, especially where messages are liable to deletion.[31]

Insofar as they appear to evidence poor operational security and less than statesman-like behaviour, there's a strong case for arguing that Goldberg's revelations were clearly in the public interest. For its part, the Trump Administration initially accused the journalist of lying, then branded him a "total sleazebag" when he published the group chats to which he was party. The connotation of this insult suggests that he behaved unethically, that the 'right' thing to do was to keep the incident and the content of the discussion to himself. But as a journalist, Goldberg clearly has a different moral imperative to that of the US government. And precisely because the Administration has denied that the material included classified information, he cannot be prosecuted under the Espionage Act.

Back to the start: whose morals?

In the last three years I have given eighteen Gresham lectures, including this one. From the outset, we have considered how ownership and regulation of technology is complicated by different and often diverging perceptions of what is acceptable behaviour; how our emotional investment in online interactions and experiences blurs the line between digital and physical and allows others to exploit our hopes, fears, and principles. We have seen how our use of IT confronts us with tough ethical choices, we've explored what happens when we mystify and catastrophise about technology, and we've identified ways to make cybersecurity more inclusive and accessible – we even had a go at that ourselves with our Cyber Shorts series of videos.[32]

We've challenged preconceptions about who gets to use and misuse IT, examined our increasing reliance on it for our critical infrastructure, our physiology, and our intimate relationships; we've taken stock of its impact on our privacy, and wondered where all of this is headed. This year, we have sought out lessons from history, and we have discovered ancestors who like us fetishised technology and exploited others in the name of progress; we have seen how people find a way to engage in IT even in the face of significant

---

[29] https://www.bbc.co.uk/news/articles/cn04d4xdz93o
[30] https://www.youtube.com/watch?v=47mCkAIXBzY
[31] https://www.bbc.co.uk/news/technology-67780595
[32] https://www.youtube.com/watch?v=NzHhKBARvo0; https://www.youtube.com/watch?v=CbhE2h0QHRA; https://www.youtube.com/watch?v=eMmDcfUF6g8

obstacles; we have found that our love/hate relationship with Artificial Intelligence is nothing new; we have questioned the use of data to describe, prescribe, and proscribe us; and, we have acknowledged our deep seated urges to watch and control each other with technology.

The morals and ethics of all of us – whether we are private citizens, corporations, or governments – have been close to the surface throughout. Technology does not develop in a vacuum: it is shaped by society and shapes society in return. As soon as it is put in the hands of any person or group of people, it reflects their moral and ethical viewpoints as much as it may challenge them. What I have learned from these Gresham lectures is that IT is never just 0s and 1s. It is never, ever, neutral.

© Professor Victoria Baines 2025

Resources and Further Reading

Kathleen E. Kennedy. 2015. *Medieval Hackers*. Punctum Books. Brooklyn.

David Lyon. 2014. “Surveillance, Snowden, and Big Data:

Capacities, consequences, critique”. *Big Data & Society*, July-December 2014: 1-13. https://journals.sagepub.com/doi/epub/10.1177/2053951714541861

National Archives [US]. Undated. “Pentagon Papers”. https://www.archives.gov/research/pentagon-papers

The National Security Archive. 1995-2017. “THE PENTAGON PAPERS: SECRETS, LIES AND AUDIOTAPES: Audio Tapes from the Nixon White House.” The George Washington University. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB48/nixon.html

Jonathon W. Penney. 2022. “Understanding Chilling Effects”. *Minnesota Law Review* 106: 1451-1530. https://minnesotalawreview.org/wp-content/uploads/2022/04/6-Penney_Web.pdf

The Snowden Archive, a collection with timeline of documents copied by Edward Snowden and subsequently published. https://github.com/iamcryptoki/snowden-archive