Submarine state

On secrets and leaks

Daniel Nemenyi

> It's not answerable to anyone, given it doesn't exist in law; no minutes are kept; and it's confidential. No citizen ever knows what is said within… These are decisions of almost life and death, and no member has to answer to anybody.
>
> Yanis Varoufakis, description of the Eurozone[1]

Recently in this journal Maïa Pal succinctly formulated a major quandary of contemporary politics. Pal notes that the secrecy under which the negotiation of the 'largest free-trade zone in the world' is taking place – TTIP, TPP, CETA (and, we should add, TiSA, the Trade in Services Agreement) – ensures that 'what communities are being excluded from is, in a sense, the regulation of regulation' (*RP* 190, p. 8). Even members of Congress, the USA's official regulatory organ, have complained of the silence met by their own staff when applying for permission to access these negotiations' processual documentation,[2] which, if it were not for WikiLeaks and the occasional leaking delegate, would remain securely under seal until several years after any possible signing. Though the primary object of Pal's commentary is the content of the regulations themselves, her distinction between two kinds of regulation – the neoliberal regulations themselves and the 'regulation of regulation' from which, she writes, 'communities are being excluded' – reflects precisely the distinction made in 1997 by the landmark contemporary report on secrecy within a Western nation state, the *Report of the Commission on Protecting and Reducing Government Secrecy* chaired by Senator Daniel Patrick Moynihan.[3] There is a history and a logic to the politics of secrecy today.

History of the state secret

The Moynihan Secrecy Commission considered secrecy to be not only a form of government regulation, but 'the *ultimate* mode of regulation', since, as Moyniham exclaimed in his Senate testimony, 'the citizen does not even know that he or she is being regulated!' Like Pal, the Moynihan Secrecy Commission distinguishes two forms of regulation, treating secrecy as kind of 'meta-regulation' governing the possibility of regulation itself. Whereas 'regular' or 'domestic' regulation, that derived from statute, concerns the behaviour and action of citizens, the 'parallel regulatory regime' of 'foreign' or 'secret' regulation, derived often from undisclosed or vaguely defined legal sources, concerns what they may know, their access to information, secrecy. The Commission details how under the guise of a spectre of a Communist 'enemy within' during the Cold War a 'culture of secrecy' developed within government, independently of the threat of an actual organized Communist movement. The Communist Party had by 1950 already been 'neutralized', the Commission writes, and more ominously, 'existed … merely as a device maintained by the US Government to trap the unwary'.

Eisenhower in particular heightened this trend, rolling out a full national programme 'for keeping out the disloyal and the dangerous' that would win the approval of Senator McCarthy. Disloyalty was twinned with danger of any kind, which lumped anyone 'who talks too freely when in his cups, or a pervert who is vulnerable to blackmail' into the category of the 'enemy within'. The precedent for this was an Executive Order made by President Wilson the day following the USA's declaration of war against Imperial Germany and its direct involvement in World War I. Wilson's purportedly temporary emergency measure allowed for the swift removal of anyone within federal government 'inimical to the public welfare by reason of his conduct, sympathies or utterances'.[4] Two months later the long-contested 1917 Espionage Act was passed, which makes it illegal, by punishment of death or thirty years imprisonment, to transmit for any reason whatsoever secret state information to an enemy and, by extension, the public and media. As Chelsea Manning would discover, the Espionage Act admits no moral defence.

Despite this, when leaks to the press of secret information did happen, they generally derived from state's echelons as a way of flexing political muscle. 'The ship of state is the only known vessel that leaks from the top', a Plato-inspired saying goes. The Moynihan Secrecy Commission notes that 'Presidents soon came to realize that "even harmless secrets were coins of power to be hoarded"', and that '[s]ecrets had become assets; organizations hoarded them, revealed them sparingly and in return for some consideration'. This was most famously the mode by which J. Edgar Hoover, an 'artist with leaks' as contemporary historian Matthew Connelly calls him, held dissidents and even presidents in check, becoming arguably the most powerful figure in US politics due to his FBI's extensive accruement and targeted revelation of secrets.[5] The leak was an institutionalized mode of political exchange, of governing and trading blows, inasmuch as its parent, the secret, became a valuable commodity of regulation.

Hoover's amassing of secrets was by no means anomalous to the general culture of government during the Cold War. Systematically ever greater amounts of data classified as Secret or Top Secret was being generated, whilst the rate of declassification failed to keep pace. This in itself ensured the expansion of state arcana. Hence a culture of secrecy within government inflated during the Cold War and not only, probably not even primarily, because of Soviet espionage or actual 'Huns within our own gates'. Rather through a power dynamic internal to governance itself.[6] 'Secrecy begets suspicion', Moynihan's Commission writes, to which could be added 'and suspicion begets secrets'.

The Cold War culture of secrecy would expand massively in our own time. Far from the 'culture of openness' called for by the Moynihan Secrecy Commission, under Obama's much vaunted promise of 'open governance'[7] less than 1 per cent of the annual US classification bill is spent on declassification, with the bill itself having soared to $14.98 billion.[8] The quantity of secret information is such that almost 5 million Americans are employed to interact with it – a 50 per cent rise since 1999 – of which 1.4 million may access the highest, Top Secret, level.[9] Over 77 million US documents were stamped as risks to national security should they be known to the world in 2014, compared to under 6 million in 1996.[10] Hillary Clinton's reliance on a personal, non-archived inbox whilst Obama's secretary of state has highlighted a further fact: vast swathes of national archive material simply no longer exist. Of the billion-odd emails sent by the State Department in 2013, only 41,749 were not deleted.[11] The rise of big data alongside a culture of governmental secrecy has engendered national archival arcana, albeit with voids of astounding magnitude. As a result, leaks have swollen in size too, and so has, apparently, the scale of their punishment. Eight Espionage Act prosecutions against leakers have taken place under Obama, compared to three by all presidents before him; Manning's and Edward Snowden's are the most famous.

Leaks

The ship of state is increasingly a submarine: hidden but leaking from all sides. The repression recently meted out to leakers has been attributed to the honed capacity to surveil and prove the culpability of their assailants. Yet in reality many of these leaks demonstrate the opposite. As a rule, systems of secrecy become harder to secure the larger and more complex they become. Manning was caught because access to data and programmes on the computers she used was inadequately controlled.[12]

Given cryptographer Bruce Schneier's rule that security is not a final product but a process as strong as its weakest link, the same rule which applies to computer security and secrecy systems in general applies to the state: the number of possible vulnerabilities grows proportionally to its size and complexity.[13] Take the enormity of the recent 'thefts' of data from the US Office of Personnel Management (OPM), the body responsible for government hirings and, ironically, managing Secret and Top Secret security clearances. OPM recently discovered that since May 2014 records containing sensitive information on 4.2 million federal personnel had been gradually stolen; and that, more recently, their highly detailed background-check data on 21.5 million current, former and prospective federal employees, contractors and families thereof had been too.[14] These records are so detailed as to essentially constitute biographies. A hack of similarly rich data also befell US health insurance giant Anthem Blue Cross earlier this year, when their records on approximately 80 million Americans were breached. China denies the obligatory accusations of its culpability for such leaks, but what is clear is that intimate information on the lives of Americans (and surely many others) is being gathered in ways beyond that conventionally considered as surveillance even after Snowden.

Regardless of the actor directly responsible for these leaks, the fact remains that they could not have occurred had the data not been recorded and stored in the first place. An argument premissed on such lines must be made against the UK's care data programme, in which the NHS's entire health-care database is to be leased to private researchers despite the ease by which its name-redacted records could be de-anonymized (a mode of leaking). A similar argument was pursued in the *NASA* v. *Nelson* case (2007). Employees of the space agency objected to the imposition of questionnaires which demanded such intimate detail of their lives as to determine their 'suitability' of access against a screening matrix which actually bunches together such 'perversions' as

> homosexuality, sodomy, carnal knowledge, incest, bestiality, indecent exposure or proposals, illegitimate children, cohabitation, adultery, mental or emotional issues, minor traffic violations, displaying obscene material, acting drunk, and making obscene phone calls.[15]

Since even the Supreme Court rejected the employees' concerns, such data remained collectable and therefore liable to be breached; as it was in October 2012 when a non-encrypted NASA laptop containing a copy of the employee database was stolen.[16]

Access control

A dyadic movement should be noted. Whilst the state becomes increasingly imperceptible from the outside, it simultaneously demands full transparency and information on the part of all others. To be in full view of the state is necessary for the determination of access to, or exclusion from, its archives and control. Deleuze was in a sense right to claim in the early 1990s that 'the digital language of control is made up of codes indicating whether access to some information should be allowed or denied',[17] but, by relegating 'Foucault's' disciplinary power to the past he ignored the fact that such control necessitates a Benthamite apparatus of 'systematic observation' (as the NSA calls surveillance) in order to both ascertain levels of access and discipline its

monsters. Deleuze expressed concern over the possibility of a future amalgamation of disciplinary and control power without acknowledging that the 'era of control' itself was instantiated with the qualities of both modes of power.

Topologically, it has been defined by two forms of border. On the one hand there is that governed by access control. Historian Matthew Connelly has charted how the compartmentalization of state knowledge into access-defined spheres was the invention of the Manhattan Project, whereby only a handful of the 100,000 people involved in the secret development of the American atomic bomb were deemed to be in the 'need to know' category, the overall end towards which they were each working. Compartmentalization pitted its chief proponent, director of the Manhattan Project Leslie Groves, against Robert Oppenheimer himself, who held to a belief in free scientific discourse and was known to publicly mock the Manhatten Project's mode of secrecy (which is ours today). Eventually the 'father of the atomic bomb' would begin to have his access permissions revoked altogether in the months following Eisenhower's aforementioned McCarthyite screening regime, with the presidential order that 'a blank wall be placed between Dr Oppenheimer and any secret data'. It is just such a 'blank wall', constituting the border of control and governing access within a secrecy system, which is encountered in so much of the national archive today.

From its onset the Cold War was also defined according to the external border, that which separated two discreet masses, defined as the 'iron curtain'. Deleuze's positing of the era of the mass and individual as being over is strikingly of its time: announced whilst the Soviet Union was collapsing to the applause of those who considered its end that of history itself and whose capital and machinery were finally able to swash the entire globe. Today, as Pal observes, in the TTIP regulations, power is once again separating into 'mega-regional' blocks, with those bound by the northern American trade agreements on one side, and those bound to the BRICS (Brazil, Russia, India, China and South Africa) on the other. A recently leaked EU diplomatic cable concerning TPP claims, 'Washington … is negotiating with every nation that borders China, asking for commitments that exceed those countries' administrative capacities, so as to "confront" Beijing.'[18] Foucault's schema of discreet masses remains alive and well today. The premiss of the 'enemy within' as criminal and monster, through which

Discipline and Punish understands the modern age, has perhaps always provided the justification for such systems of *mass* surveillance. Privacy activists have since the 1980s highlighted the tendency for 'The Four Horsemen of the Information Apocalypse' – terrorists, kidnappers, drug dealers and paedophiles – to be used to justify the 'systematic observation' of all by the secret services. Foucauldian categories of the social enemy and the masses have lost none of their sway in the cybernetic age.

Crypto war

That the NSA-led 'Five Eyes' conduct digital surveillance together on a mass scale, even internally, was well known already by the 1990s in regards to their ECHELON system, as was China's 'Great Firewall' and Russia's SORM. What was not known until Snowden's revelations, aside from the sheer detail they provide, was that surveillance had become so ubiquitous that '[t]he level of operational security required to maintain privacy and anonymity in the face of a focused and determined investigation is beyond the resources of even trained government agents.'[19] This is to say that the Crypto Wars of the 1990s were lost.

The public right to strong forms of cryptography resistant to even state code-breaking was a site of major conflict in the USA and the UK as the Internet became a commercial and private (rather than US-owned) entity at the start of the 1990s, and as telecommunications networks became simultaneously digitized. In 1991 the US Senate attempted to pass a counterterrorism bill which included this clause:

> that providers of electronic communications services and manufacturers of electronic communications service equipment should ensure that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.[20]

Though itself defeated by libertarian and commercial outcry, the spirit of this bill – that the state should have access to all electronically mediated secrets – was to cause a number of legal struggles over the decade whose final outcome came to define the basis of digital politics of today. Whilst the 1991 bill was still under discussion, American cryptographer and anti-nuclear activist Phil Zimmermann published his email encryption algorithm Pretty Good Privacy (PGP), the first freely distributed algorithm capable of strong, military-grade encipherment. Its minimum strength was leagues beyond that defined by American export licences, which still considered cryptography a form of munitions, but the failure of Zimmermann's ensuing criminal investigation (along with Netscape's provision for strong encryption in their non-American web browsers) ensured something of a global democratization of strong cryptography. Bruce Schneier summarized the spirit of this early 1990s' movement when he described cryptography as 'the great technological equalizer; anyone with a cheap … computer could have the same security as the largest government.'[21]

As telecommunication networks simultaneously became digitized (and thus more effectively encrypted), secret services promulgated the threat that internal communications might en masse 'go dark' – from them – with the proliferation of new and strong phone-to-phone encryption boxes. A similar scenario had unfolded in South Africa in the 1980s, contributing significantly to the overthrow of the apartheid government.[22] The US solution was the 'Clipper chip', a telephone with a built-in strong cryptographic chip that provided the secret services with back-door access (and, by extension, any hacker capable of mimicking their back-door algorithm). Given that equivalent boxes without such back doors could be imported from Europe, Clipper-chipped phones were a commercial failure. The conflict continued. Following in Bill Clinton's steps, Britain's John Major decreed that makers of cryptographic algorithms enforce the registration of their users' names, addresses, intentions and cryptographic

keys with a 'trusted third party' accessible to the intelligence agencies. Blair betrayed his popular pre-cabinet opposition to regulating public cryptography by reinstating such 'key escrow' *de jure* in 2000, but the *de facto* rise of cryptography-powered online services (shopping, banking, gambling) ensured that in 2005 it would not be reinstated. Privacy activists declared 'The "crypto wars" are finally over – and we've won!'[23]

Or not. Schneier, who was privy to Snowden's troves before publication, lists four modes by which the peoples' victory was secretly undermined by the NSA and GCHQ. First, their weakening of cryptographic algorithms.[24] Second, their piggybacking of domestic surveillance applications through enforced secret back doors – for example, the threatening of Yahoo with a minimum $250,000-per-day fine for not succumbing quietly to PRISM. Third, the stockpiling of unknown 'zero-day' software and hardware vulnerabilities for future exploitation – analogous to the stockpiling of secrets by which J. Edgar Hoover was infamous. Fourth, hacking the fabric of the packet-based Internet architecture itself, a method long decried by the West of China's 'Great Firewall'. In total, a 'ubiquitous' surveillance machine 'efficient beyond', Schneier writes, 'Bentham's wildest dreams'.[25]

Some consider a second round of crypto-wars to be today under way, including Schneier. The business lesson of the Clipper chip has induced certain US technology corporations to be seen to resist the intelligence agencies' apprehension of their data, by means such as encrypting their phones and network channels. As in the 1990s, the various Horsemen have been rolled out ('Apple will become the phone of choice for the paedophile') and a terrorist-jousting prime minister intends to 'command all the software creators we can reach to introduce back doors into their tools for us' – again to the dismay of those who actually understand the process of software creation.[26] But such legislation would be little more than a spectacle, giving an air of regulation to the essentially unregulatable. 'Necessarily secret', the odd kind of 'transparent oversight' of the British intelligence agencies when they sat before Parliament's Intelligence and Security Committee after Snowden's revelations, has precedent since at least an eighteenth-century House of Lords ruling on the regulation of GCHQ's ancestor, the Decyphering Branch, when it was decided 'it is not consistent with the public Safety, to ask the Decypherers any Questions, which may tend to discover the Art or Mystery of Decyphering.'[27]

For practical reasons, there can be no serious regulation of surveillance. Schneier writes, 'the more intrusive a surveillance system is, the more likely it is to be hidden.'[28] Foucault writes, 'in the central tower, one sees everything without ever being seen.'[29] Surveillance takes place *in camera*. It is a camera obscura whose window silently inverts secrets into information, whose prism refracts them into organizable metadata.

The simultaneous explosion of secret archives and surveillance apparatuses needs to be thought as a unity, as the two reinforcing modes by which power consolidates its monopoly over the commodity of informational power, the secret. 'Crypto war' names not only a discreet event but a fundamental political struggle over the control of secrecy: both defensive, preventing access to knowledge, and offensive, breaking into another's knowledge. There are many forms of the latter *crypt-analysis*, including surveillance, leaking, data theft, user tracking and software cracking; as there are of the former *crypto-graphy*, the secret national archive, the encrypted hard disk, 'darknet', the proprietary software executable. It is not a matter of ethically rejecting one side and affirming the other, but of positioning ourselves on the threshold of an information source so as to control and command access to strategic secrets – ours or others –and thereby to amass power.

Deleuze was wrong to say that the thermodynamic machine was redundant in the cybernetic age. At stake here is a kind of Maxwell's demon, a threshold subject, who decides whether the gates of information are open or closed.

Notes

1. Harry Lambert, 'Yanis Varoufakis Opens up about His Five Month Battle to Save Greece', *New Statesman*, 13 July 2015, www.newstatesman.com/world-affairs/2015/07/exclusive-yanis-varoufakis-opens-about-his-five-month-battle-save-greece.
2. Senator Wyden, 'IYCMI: Wyden Statement Introducing "Congressional Oversight Over Trade Negotiations Act"', 2012, www.wyden.senate.gov/news/blog/post/iycmi-wyden-statement-introducing-congressional-oversight-over-trade-negotiations-act.
3. *Report of the Commission on Protecting and Reducing Government Secrecy*, United States Government Printing Office, Washington DC, 1997, www.fas.org:8080/sgp/library/moynihan.
4. 'Executive Order 2585 – Taking Over Necessary and Closing Unnecessary Radio Stations', 6 April 1917; 'Executive Order 2587A – Federal Employees Removal on Security Grounds', 7 April 1917.
5. Matthew Connelly, 'The Cold War and the Culture of Secrecy', 2015, www.lse.ac.uk/IDEAS/events/events/2015/15-01-13-M.-Connelly3.aspx.
6. The Commission notes that despite the vast apparatus for ascertaining 'the enemy within', between 1975 and 1996 only fifteen successful cases of Americans engaging the enemy were discovered.
7. Barack Obama, 'Transparency and Open Government', www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
8. This is a rise from $9.9 billion in the year Obama took office, and $2.6 billion in the year preceding Moynihan's 1997 report. *2014 Report to the President*, National Archives and Records Administration, Information Security Oversight Office (ISOO), p. 24, www.archives.gov/isoo/reports/2014-annual-report.pdf.
9. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, John Wiley, Chichester, 2000, p. 99.
10. ISOO, *2014 Report to the President*, p. 6.
11. Office of Inspector General (OIG), *Review of State Messaging and Archive Retrieval Toolset and Record Email*, March 2015, https://oig.state.gov/system/files/isp-i-15-15.pdf.
12. Ed Pilkington and Matt Williams, 'Bradley Manning Hearing Told of Lax Security at Military Intelligence Unit', *Guardian*, 18 December 2011, www.theguardian.com/world/2011/dec/18/bradley-manning-wikileaks-hearing.
13. Schneier, *Secrets and Lies*, p. xii.
14. 'OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats', 9 July 2015, https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats.
15. Rainey Reitman, 'NASA's Data Valdez: Thousands of Employees' Personal Information Compromised in Embarrassing Data Breach', *EFF*, 29 November 2012, www.eff.org/deeplinks/2012/11/nasas-data-valdez-thousands-employees-personal-information-compromised.
16. 'Agencywide Message to All NASA Employees: Breach of Personally Identifiable Information (PII)', 13 November 2012, www.spaceref.com/news/viewsr.html?pid=42609.
17. Gilles Deleuze, 'Postscript on Control Societies, *Negotiations*, Columbia University Press, New York, 1997, p. 180.
18. 'EU and French diplomats who strongly criticize US trade policies and call TPP treaty a confrontation against China', WikiLeaks, 29 June 2015, https://wikileaks.org/nsa-france/intercepts/WikiLeaks_US_Spying_On_French_Diplomats_Criticizing_US_Trade_Policies.pdf.
19. Bruce Schneier, *Data and Goliath,* W.W. Norton, New York, 2015, p. 43.
20. S.266 – Comprehensive Counter-Terrorism Act of 1991, www.congress.gov/bill/102nd-congress/senate-bill/266.
21. Schneier, *Secrets and Lies,* p. xi.
22. See Tim Jenkin, 'Talking to Vula: The Story of the Secret Underground Communications Network of Operation Vula', *Mayibuye*, 1995, www.anc.org.za/show.php?id=4693.
23. Foundation for Information Policy Research, 'The Crypto Wars Are Over!', 25 May 2005, www.fipr.org/press/050525crypto.html.
24. See Finn Brunton, 'Kleptography', *RP* 183, January/February 2014.
25. Schneier, *Data and Goliath,* pp. 146–151; 32.
26. Cory Doctorow, 'What David Cameron just proposed would endanger every Briton and destroy the IT industry', *boingboing*, 13 January 2015, http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html.
27. David Kahn, *The Codebreakers,* Weidenfeld & Nicolson, London, 1966, p. 171.
28. Schneier, *Data and Goliath,* p. 30.
29. Michel Foucault, *Discipline and Punish*, trans. Alan Sheridan, Penguin, London, 1991, p. 202.