‘Secure, anonymous, unregulated’: *Cryptonomicon* and the transnational data haven

Philip Leonard
Nottingham Trent University, UK

Abstract

This essay considers how Neal Stephenson's 1999 epic novel *Cryptonomicon* engages with the long-standing and complex relationship between cryptology and national/transnational identity. *Cryptonomicon's* layered and disjointed structure allows it to explore the impact of cryptography and cryptanalysis in the Second World War (as well as their impact on the consequent rewriting of the international political stage), to reflect on the place of technology in the recent history of cryptology, and to consider how emergent (and supposedly secure) data storage technologies not only open up planetary-wide communication traffic but also unsettle the agreed protocols of national and international law.

Stephenson provides a sense of technology's global effects by offering not a straightforward narrative of the demise of the nation-state but by showing how technologies are in a process of constant negotiation with the institutions of the nation-state, drawing upon the economic, material, and intellectual resources of the nation state, while at the same time challenging notions of a bordered and coherent national identity and working to disestablish nations of their regulatory authority. The essay is informed by recent work on cryptology, data havens, globalization, transnationalism, and postcoloniality, as well as Derrida's work on archives and technology.

Keywords

Cryptology
Cryptonomicon
Data havens
Derrida
Nationality
Stephenson
Technology

Credited by some as a more compelling and engaged response to the information age than the other heavyweights that tend to dominate postmodernity's novelistic horizons (Garner, 1999), Neal Stephenson's 1999 novel *Cryptonomicon* works on an epic scale that resists easy synopsis. Its geographical landscape is a global one, with characters ranging across China, Japan, the Philippines, Sweden, the UK, and the USA. Its sense of history is elaborately bifurcated, shuttling between the Second World War and the 1990s it traces the roots of the dotcom era to the information war of the 1940s. Its cast of dramatis personae is a lengthy one, although much of the narrative moves (with a logic that sometimes stretches credulity) between three central figures: Lawrence Waterhouse, a PhD student in maths at Princeton who enters the Second World War and soon becomes one of the Allies' key figures in the intelligence war; Randy Waterhouse (grandson of Lawrence), erstwhile librarian and UNIX autodidact, who becomes the chief software engineer in a telecoms venture for migrant Filipino workers, and who finally – incredibly - discovers Japan's lost war gold; and Bobby Shaftoe, a gung-ho marine and grandfather to rogue marine services contractor America (Amy) Shaftoe, who later becomes Randy's girlfriend. Gathered around this central cast is a large company of extras; the presence of many of these supplementary characters – such as Alan Turing, General MacArthur, Admiral Yamamoto, Albert Einstein, Winston Churchill, and Ronald Reagan – could easily seduce Stephenson's readers into treating this text as historical fiction.

Stephenson's text is fascinated by technology and much of it is devoted to situating technoculture not in the closing years of the twentieth century, but in a longer history that has been largely unwritten. However, as much as *Cryptonomicon* seeks to establish the shaping of the present by technologies of the recent past, and as much as it finds

programmers, computer scientists, and hackers (such as Turing and Lawrence Waterhouse) to be the unacknowledged heroes of the twentieth century, this text cannot be placed firmly in the category of documentary revisionism. Often – almost invisibly – *Cryptonomicon* refuses the accepted protocols of historical fiction, to the extent that recognition of technology's cultural centrality here takes place in a narrative that works against the secure transmission of information and becomes conceptually vertiginous. Indeed, *Cryptonomicon* encourages readers to treat its claims to accuracy with suspicion by including, in its seemingly reliable history of the information wars, a fictional work that is itself entitled *Cryptonomicon*.

This essay will consider *Cryptonomicon's* documenting of technology's unwritten history, focusing in particular on the ways in which this novel charts the emergence of the data haven at the end of the twentieth century and traces the roots of this apparently new technology both to earlier archival technologies and to cryptographic attempts to secure information. What *Cryptonomicon* reveals, in its *almost* encyclopedic treatment of data havens' dependence on cryptology, is a strange reshaping of both communication and the nation-state. Language here functions simultaneously as a reliable and insecure medium of information exchange, and the nation-state is seen to be a mode of territorial distinctiveness that is at once essential to and threatened by new technological systems.

Unbreakable encryption?

Cryptonomicon's narrative constantly gravitates towards the manipulation of information, especially the interfacing of the human intellect with the computer in both the encryption and decryption of individual, corporate, and state secrets. Long sequences of the novel are

often given over to disquisitions on the encoding and decoding of personal, commercial, political, and military information. Early in the novel, for example, readers are introduced to Novus Ordo Seclorum (abbreviated to Ordo), Randy's preferred software for encrypting emails to Avi, his business partner in Epiphyte Corp.[1] One of Ordo's strengths, we are told, lies in its ability to generate encryption keys that are of unlimited length:

> Randy pulls down a menu and picks an item labeled: 'New key…'
> A box pops up giving him several KEY LENGTH options: 768 bits, 1024, 1536, 2048, 3072, or Custom. Randy picks the latter option and then, wearily, types in 4096.
>
> Even a 768-bit key requires vast resources to break. Add one bit, to make it 769 bits long, and the number of possible keys doubles, the problem becomes much more difficult. A 770-bit key is that much more difficult yet, and so on. By using 768-bit keys, Randy and Avi could keep their communications secret from nearly every entity in the world for at least the next several years. A 1024-bit key would be vastly, astronomically more difficult to break.
>
> Some people go so far as to use keys 2048 or even 3072 bits in length. These will stop the very best codebreakers on the face of the earth for astronomical periods of time, barring the invention of otherworldly technologies such as quantum computers. Most encryption software – even stuff written by extremely security-conscious cryptography experts – can't even handle keys larger than that. But Avi insists on using Ordo, generally

> considered the best encryption software in the world, because it can handle keys of unlimited length—as long as you don't mind waiting for it to crunch all the numbers.
>
> …
>
> Randy is trying to generate one that is ridiculously long. He has pointed out to Avi, in an encrypted e-mail message, that if every particle of matter in the universe could be used to construct one single cosmic supercomputer, and this computer was put to work trying to break a 4096-bit encryption key, it would take longer than the lifespan of the universe (Stephenson, 2000, pp. 53-4).

What Ordo brings to the history of code-making, then, is a mode of encryption that is more virtual and machinic than it is human: all that Ordo requires from Randy is an arbitrary sequence of key strikes, from which it generates the random numbers that then constitute the encryption algorithm. Randy is, in other words, effectively removed from the process of translation that makes his emails incomprehensible to anyone other than their intended recipients; instead he becomes simply an instrument which allows Ordo to carry out the more rigorous work of thinking.

Perhaps more important than the question of Randy's relegation to technology's appurtenance is the question of perfectible communication that Ordo raises. Offering Randy and Avi a mode of encryption that would take nearly an infinity to break, Ordo seems finally to realize the long-held belief that an unbreakable code is effectively possible. Robert Churchhouse (2002) opens his *Codes and Ciphers* with the observation that 'For at

least two thousand years there have been people who wanted to send messages that could only be read by the people for whom they were intended' (1), and the various modes of concealment and encipherment that developed during this period have been based upon the assumption that they could resist decipherment and disclosure. From Caesar's simple substitution cipher (which replaces each letter in a message with one that is three places after it in the alphabet) to PGP (Pretty Good Privacy – highly secure freeware for data encryption and verification), cryptography has acquired greater sophistication and taken on greater prominence in everyday communication.[2] This history of cryptography has, however, been a history of secrets deciphered, since the most complex codes of the past now appear elementary and even the most secure codes of today (such as PGP) are thought by some to have been broken by the US Government. One reading of *Cryptonomicon* might find in Ordo a method of encoding that finally overcomes cryptography's difficult history: Ordo remains apparently secure throughout the novel, and it is this secure exchange of information that allows Randy's hacker nonconformism (as well as Avi's entrepreneurial flair) to flourish in a business environment left arid by governmental surveillance and corporate espionage. *Cryptonomicon* suggests, in other words, that communication between two parties has, in the past, been corruptible by an intrusive third party; what new technologies now allow is an unprecedented level of confidence in language as a private medium which can guarantee the legitimacy of expression.

A new history of technology

Importantly, *Cryptonomicon's* sense of history is neither a straightforwardly linear nor an epochal one, since it refuses either to reaffirm the idea that the technological present

smoothly builds on technologies of the recent past or to endorse the notion that we now inhabit a technologized 'end of history' which overcomes the failures of the pre-technological past. As much as this novel often constructs Randy and his associates as the beneficiaries of a newly technologized and global order, it sees this order as one which has neither shaken off the limitations of antecedent technologies nor entered an unprecedented age of technologized - posthuman – enlightenment. In this respect, the novel echoes Siegfried Zielinski's claim that 'media worlds' are not distributed sequentially, but 'combine at particular moments in time, collide with each other, provoke one another, and, in this way, maintain tension and movement within developing processes' (Zielinski, 2006, p. 258).

Three examples from the novel demonstrate this departure from both evolutionary and epochal historiography. First, software. Ordo certainly functions mostly by removing human involvement and by operating with almost complete autonomy in its encryption of data. But this novel does not, unlike some recent accounts of the machinic reconstruction of consciousness and the body, suggest that the human is, in its greater association with technology, entering its terminal phase. Although advanced encipherment might well depend upon tools such as Ordo, these tools are also seen to require human collaboration, with cryptology being possible only as the result of a complex interfacing of machines, software, and human intelligence. For instance, when Randy is working on the Arethusa cipher – the code which, when broken, leads him to the mine housing Japan's war gold – we read:

> Unlike human codebreakers, computers can't read English. They can't even recognize it. They can crank out possible decrypts of a message at tremendous speed but given two character strings like
>
> SEND HELP IMMEDIATELY
>
> and
>
> XUEBP TOAFF NMQPT
>
> they have no inherent ability to recognize the first as a successful decryption of a message and the second as a failure (Stephenson, 2000, p. 824).

Cryptonomicon, in other words, finds both the past (Lawrence Waterhouse's information war) and the present (Randy Waterhouse's information economy) to be simultaneously machinic and human, since even the most advanced software does not fully supplant the human.

Second: hardware. As much as *Cryptonomicon* seems to find an unparalleled authenticity in new modes of cryptographic deception, it does not seek wholly to detach new encryption technologies from earlier efforts to secure the exchange of messages. Indeed, *Cryptonomicon's* sense of emergent communications must be seen as one that interlaces the technologies of the present with those of the recent past. Perhaps the most telling examples of this genealogy occur when it seeks to establish code-breaking machines of the Second World War as computing technology, rather than simply as electromechanical precursors to the devices that we now conceive as computers. The Turing Bombe at Bletchley Park (which performed the calculations that allowed the Enigma cipher finally to be broken) is seen as an early attempt at mechanized thought, but

it is Waterhouse's use of a room-sized device in Manila to crack Japanese codes that provides *Cryptonomicon* with the clearest image of an embryonic computing intelligence:

> The Basement is filled with ETC card machines and with several racks of equipment devoid of corporate logos, inasmuch as they were designed and largely built by Lawrence Pritchard Waterhouse in Brisbane. When all of these things are hooked together in just the right way, they constitute a Digital Computer. Like a pipe organ, a Digital Computer is not so much a machine as a meta-machine that can be made into any of a number of different machines by changing its internal configuration. At the moment, Lawrence Pritchard Waterhouse is the only guy in the world who understands the Digital Computer well enough to actually do this, though he's training a couple of Comstock's ETC men to do it themselves. On the day in question, he is turning the Digital Computer into a machine for calculating the zeta function that he thinks is at the core of the cryptosystem called Azure or Pufferfish (Stephenson, 2000, p. 830).

Third: knowledge. What underlies the emergence of the computer during this period – and its eventual status as the apparent guarantor of private and authentic communication – is a scientific (mathematical, physical, and cryptological) reasoning that endures across history. Lawrence Waterhouse's successes as a cryptanalyst (and, as a consequence, the Allied successes against Germany and Japan) are attributed in *Cryptonomicon* to a

theoretical grasp of universal principles that allow a purer, more precise, and better functioning knowledge than thought that is limited by the praxis of the moment:

> The basic problem for Lawrence was that he was lazy. He had figured out that everything was much simpler if, like Superman with his X-ray vision, you just stared through the cosmetic distractions and saw the underlying mathematical skeleton. Once you found the math in a thing, you knew everything about it, and you could manipulate it to your heart's content with nothing more than a pencil and a napkin. He saw it in the bell curve of the silver bars on his glockenspiel, saw it in the catenary arch of a bridge and in the capacitor-studded drum of Atanasoff and Berry's computing machine. Actually pounding on the glockenspiel, riveting the bridge together, or trying to figure out why the computing machine wasn't working were not as interesting to him (Stephenson, 2000, p. 8).

Cryptonomicon constantly attributes the Allied victory more to a nerdish facility for pattern recognition than to combat heroism or battlefield strategy, and it reveals the debt that today's technologists owe to figures like Turing and Lawrence Waterhouse. However, when read primarily as text which locates the informational age in the past as much as the present, *Cryptonomicon* could be seen to offer little more than a revisionist account of technology, one which is concerned only to establish a new history of technology and a new history of the twentieth century. Stephenson's novel goes further than such a revisionist rewriting, troubling straightforward assumptions about narrative, time, and

historicity by drawing attention to a bond between software, hardware, and knowledge that cannot simply be attached to modernity. *Cryptonomicon* might well point to a new order of the ages, but this order is one marked neither by an epochal shift towards an informational age nor a progressive maturation of incipient technologies. Rather, the novelty of this moment is to be found in the emerging sense that information technologies occupy a profound, intimate, and *enduring* place in culture and consciousness.

'The wreckage of cryptosystems'

If Stephenson's novel provides a more complex sense of history than the one that it seemingly promotes, then it also challenges the technotopian positivism that is attached to the notion of secure encryption. The hubris that is attached to the notion of an unbreakable cipher is revealed in much of the literature on cryptology. Fred Piper and Sean Murphy observe that 'Being unbreakable is a claim that many designers have made for their algorithms, usually with disastrous consequences' (Piper & Murphy, 2002, p. 52), and *Cryptonomicon* echoes this sentiment in an email exchange between Randy and Enoch Root (a former military priest and colleague of Bobby Shaftoe, who eventually helps to disinter Japanese war gold):

> You and I both know, Randy, that the history of crypto is strewn with the wreckage of cryptosystems invented by arrogant dilettantes and soon demolished by clever codebreakers. You probably suspect that I don't know this – that I'm just another arrogant dilettante (Stephenson, 2000, p. 432).

Cryptonomicon repeatedly bears witness to the disasters that have befallen those 'arrogant dilettantes' who remain confident in the security of their ciphers. The interception and deciphering of messages that allowed the US air force to locate and assassinate Admiral Yamamoto in 1943, as well as Germany's catastrophic reliance on the Enigma cipher, appear in Stephenson's text as evidence of cryptographers' ill-conceived certainty about their media.

Cryptography's history is shown to be a difficult (and often disastrous) one here, but this novel also suggests that current encryption technology offers a level of security that can finally resist unsolicited decryption. And yet, Ordo, introduced as an encryption software which allows information 'to remain secret for as long as men are capable of evil' (Stephenson, 2000, p. 55), too fails fully to secure Randy's messages. While Ordo is seen to produce encryption algorithms that defend against current code-breaking technologies, it is nevertheless susceptible to other forms of attack. For example, some of Randy's emails are archived on his company's server in California; when the information stored here begins to interest the US government Avi fears that a subpoena could force Epiphyte to disclose its decryption keys. A different, and more dramatic, interception of Randy's data occurs when he is imprisoned in the Philippines; falsely charged with drug-smuggling, Randy is given his laptop and encouraged to continue working while incarcerated. At this point he becomes convinced that he is the victim of 'Van Eck phreaking', a (fictional) form of electronic surveillance which allows others to 'pick up the radiation emanating from the wire that connects screen buffer to video hardware, and translate it back into a sequence of ones and zeroes that can be dumped out onto their own screen' (Stephenson, 2000, p. 354); in other words, what Randy sees on his monitor can also be seen by those surveilling it.

Ordo might, then, guarantee email and storage security, but it cannot protect against other forms of interception.

Passages such as these suggest that *Cryptonomicon* is not convinced, as it appears to be, that communication can be confidential, or that that new technologies have allowed cryptology to emerge from its uneasy history of secrets disclosed. While hackers like Turing, Lawrence Waterhouse, and Randy Waterhouse need secure cryptosystems, the underlying hermeneutic of the novel is that there can be no secure cryptosystem. Since it is the breaking of codes and the confounding of cryptographers' intentions that allows each of them to acquire concealed information and to reform the global economic order, *Cryptonomicon's* less visible concern is to establish language as an uncertain and ultimately ungovernable medium. Here, as in all writing, language is seen to be both functional and dysfunctional since the coded message allows the act of transmission to occur, but only by opening this transmission to interception, hacking, and misappropriation in ways that can be neither controlled nor perceived.

Information and the nation-state

Reading *Cryptonomicon* against the grain of its apparent investment in the reliability of communication and communications technology elicits further questions about this text's ambiguous engagements with the technocultural politics of the twentieth century. In Stephenson's text, not only is language at least double and history an equivocating medium of disclosure and concealment, but also, more generally, shifting patterns of information exchange are seen to produce cultural uncertainty. Avi's account of the changing terrain of informational control draws attention to this unsettling transformation:

> '… as we've talked about many times, there are many reasons why different governments might want to control the flow of information. China might want to institute political censorship, whereas the U.S. might want to regulate electronic cash transfers so that they can keep collecting taxes. In the old days they could ultimately do this insofar as they owned the cables'.
>
> 'But now they can't', Randy says.
>
> 'Now they can't, and this change happened very fast, or at least it looked fast to government with its retarded intellectual metabolism, and now they are way behind the curve, and scared and pissed off, and starting to lash out' (Stephenson, 2000, pp. 838-9).

No longer is it the case that national governments regulate and restrict the global distribution of information. Rather, *Cryptonomicon* shows, these governments' unprecedented level of national anxiety results from a hitherto-invisible class of technologically creative iconoclasts – hackers, maverick programmers, and visionary engineers – who bend and manipulate information, stretch the limits of technology and redefine the systems with which they work, in the process profoundly reshaping the social, political, commercial, and military landscape. The hackerist libertarian ethic that drives *Cryptonomicon's* narrative forward does not, then, simply seek to establish geeks as the emergent priests of a new informationalist age. This text also shows how these characters engage in an often subtle, but sometimes brutal, renegotiation of the rules that particular nation-states (and the international organizations to which they belong) seek to impose

upon those who move information, capital, and themselves across the territories of the world.

In this regard, Stephenson's text's fictional and historical interests correspond closely with recent theoretical responses to technoculture's increasingly transnational, and often contra-national, trajectories. Gilles Deleuze and Félix Guattari (1988) perhaps stand at the vanguard of those who find social systems, such as the nation-state, constantly encoded, decoded, and recoded by machinic assemblages (pp. 424-73). More recently, the work of such prominent – and divergent – commentators as Manuel Castells (1996-7), Paul Virilio (2002), and Michael Hardt & Antonio Negri (2006) combines to underline the erosion of national frontiers by media, communications, and commercial technologies. Closer to *Cryptonomicon's* thematics, Jacques Derrida's *Politics of Friendship* (1997) places the question of encryption at the heart of the nation-state's current anxieties:

> A debate… is under way today… between the State and citizen associations (all assuredly 'democrats' and 'liberals') concerned over the right to initiative, invention, communication, commerce, and safeguarding privacy…. Today we have a State just as 'liberal' and 'democratic', just as concerned over its responsibilities, as its citizens, but *providing* it can maintain its hold on the means of protecting internal security and national defence (144).

Here, Derrida points to a conflict that has, in recent years, started to unsettle the democratic state's claims to democratic representation: with the availability of increasingly sophisticated encryption technologies (such as PGP) ordinary inhabitants of the digital

sphere are now able to shield their data from the gaze of law enforcement agencies. This discord is often read as a dispute between the civil liberty of the individual and the sovereignty of the state (see, for example, Lessig, 2004), but for Derrida it exposes the limits of the representative and liberal nation-state, since such a state will tolerate neither the internal nor external negotiation of its national borders.

Both the threat that data confidentiality poses to national governments and governments' political, military, and informational attempts to restrict high-level encryption, are, in *Cryptonomicon,* seen to shape the twentieth century's formative moments. Encryption technologies of the recent past are shown to play a critical role in the defence of the nation: the breaking of German and Japanese codes is given a decisive place in the Second World War, since decryption allowed Allied nations to prevail and, as a consequence, to retain their national character. Encryption technologies are also revealed as one of the most significant threats to both national security and national identity in recent years. No longer the sole preserve of governmental research or the outcome of national defence strategy, encryption is now serving individuals, non-governmental organizations, and corporations; as a consequence, nation-states have recently started both to enhance their decryption capabilities and to restrict the distribution of encryption software. When Epiphyte's server is seized we encounter *Cryptonomicon's* most forthright response to this conflict between data privacy and national governments: 'The FBI hates and fears strong crypto' (Stephenson, 2000, p. 689). This seizure, Epiphyte's employees conclude, is one outcome of multilateral efforts to restrict the movement of data:

> ‘I guess I’m just being paranoid and sort of assuming that the Dentist is somehow collaborating with forces in the U.S. government that are anti-privacy and anti-crypto’, Randy says.
>
> …
>
> ‘Not just the U.S. government,’ Cantrell says. ‘The Black Chamber’.
>
> ‘What the hell do you mean by that?’ Doug asks.
>
> ‘There was a high-level conference a couple of weeks ago in Brussels. Hastily organized we think. Chaired by Attorney General Comstock. Representatives of all the G7 countries and a few others. We know people from the NSA were there. People from Internal Revenue. Treasury people – Secret Service. Their counterparts in the other countries. And a lot of mathematicians known to have been co-opted by the government. The U.S. vice president was there. Basically we think that they are planning to form some kind of international body to clamp down on crypto and particularly on digital money.’
>
> ‘The International Data Transfer Regulatory Organization’, Tom Howard says (Stephenson, 2000, p. 725).

Archive and enigma

Derrida’s interest in encryption mainly gravitates towards the issue of democratic nations’ undemocratic efforts to protect national territoriality, and this issue is certainly dramatized in *Cryptonomicon’s* open account of the extreme measures that governments will take in order to police information. Stephenson’s novel also, however, reflects on certain states’

willingness to engage in the technological renegotiation of their status as nations. Epiphyte's participation in the founding of a data haven ('the Crypt… Secure, anonymous, unregulated data storage' (Stephenson, 2000, p. 564)) in the (fictional) sultanate of Kinakuta provides the clearest example in *Cryptonomicon* of new technologies' impact on a global order which remains organized around the concept of national identity. Epiphyte's involvement in the Crypt begins as a technological opportunity: its initial role is to install the storage systems and establish the network that will allow the Crypt to provide secure data hosting. When outlining his plans for the development of the Kinakutan data haven, the sultan observes that:

> Many Net partisans are convinced that the Net is robust because its lines of communication are spread evenly across the planet. In fact… nearly all intercontinental Web traffic passes through a small number of choke-points. Typically these choke-points are controlled and monitored by local governments. Clearly, then, any Internet application that wants to stand free of governmental interference is undermined, from the very beginning, by a fundamental structure problem…. Bottlenecks are only one of the structural barriers to the creation of a free, sovereign, location-independent cyberspace…. Another is the heterogeneous patchwork of laws, and indeed of legal systems, that address privacy, free speech, and telecoms policy (Stephenson, 2000, pp. 317-18).

Kinakuta's particular geographical, economic, and political status, the sultan goes on to argue, means that it is uniquely placed to decomplexify the relationship between national governments and information by allowing the unrestricted flow of data across its borders and, as a result, finally create a global network that is truly unrestricted:

> 'Time to start over,' he says. 'A very difficult thing to do in a large country, where laws are written by legislative bodies, interpreted by judges, bound by ancient precedents. But this is the Sultanate of Kinakuta and I am the sultan and I say that the law here is to be very simple: total freedom of information. I hereby abdicate all government power over the flow of data across and within my borders. Under no circumstances will any part of this government snoop on information flows, or use its power to in any way restrict such flows. That is the new law of Kinakuta. I invite you gentlemen to make the most of it' (Stephenson, 2000, pp. 318-19).

Clearly, the sultan here refers to what *Cryptonomicon* has already established: the movement of secure information can acutely conflict with the interests of the nation-state. The sultan's response to this conflict is not that of the G7/G8 nations, which seek increasingly to restrict the passage of encrypted data (Cybercrime, 2007), and neither does he propose abandoning Kinakuta's entire legislative apparatus; for him, Kinakuta would benefit economically from a data archive that would simply require the dismantling of its informational borders.

The effects of establishing such an archive extend further than the sultan's observations suggest, however, since the deregulation of Kinakuta's virtual limits must result in further, unpredictable, changes in the shape of this nation. On this matter Derrida's work is again instructive.

Archives, Derrida tells us, have not always functioned simply as repositories that hold the records of the past – that is, as a form of prosthetic memory. Their origins lie in the location of the documentary present and in the safeguarding of political power: the etymology of 'archive', he observes, points to

> a house, a domicile, an address, the residence of the superior magistrates, the *archons*, those who commanded. The citizens who thus held and signified political power were considered to possess the right to make or to represent the law. On account of their publicly recognized authority, it is at their home… that official documents are filed. The archons are first of all the documents' guardians. They do not only ensure the physical security of what is deposited…. They are also accorded the hermeneutic right and competence. They have the power to interpret the archives (Derrida, 1996, p. 2).

Clearly, this relationship between document storage and legal-political governance no longer operates in the same way. The places that house documents have ceased to be the residences of those in power, and archivists cannot claim exclusive or authoritative interpretation of the material for which they are responsible. As Derrida has more recently

argued, 'The archive's trustees may find themselves, because of the archive's devious structure, dispossessed of all power and all authority over it' (Derrida, 2006, p. 11).

Repositories of different sorts figure prominently throughout *Cryptonomicon*, and this text reveals that the relationship between information storage and political governance has changed substantially, with new technologies transforming this relationship still further by exposing the departure from the nation-state's regulatory authority in the second half of the twentieth century. Bletchley Park (the location of the UK's cryptanalysis and intelligence activities in the Second World War) and Golgotha (the mine that is constructed to house Japan's gold towards the end of the Second World War) provide two examples of repositories which, in the middle part of the twentieth century, were established to protect the authority of these nations' *archons*. When Lawrence Waterhouse is posted to Bletchley Park, we encounter his first impressions of this estate as one which lost its attachment to the English aristocratic landscape and has instead become an informational hub in the Allied efforts to win the war:

> The place has been well looked after, but as Waterhouse draws closer, he can see black lianas climbing up the brickwork. The root system that he glimpsed in the Underground has spread beneath forest and pasture even to this place and has begun to throw its neoprene creepers upwards. But this organism is not phototropic—it does not grow towards the light, always questing towards the sun. It is infotropic. And it has spread to this place for the same reason that infotropic humans like Lawrence Pritchard Waterhouse and Dr. Alan Mathison Turing have come here, because Bletchley Park has roughly the

> same situation in the info world as the sun does in the solar system. Armies, nations, prime ministers, presidents and geniuses fall around it… (Stephenson, 2000, p. 143).

Importantly, *Cryptonomicon* shows that although information – in the form of German and Japanese coded messages – is gathered together and held at Bletchley Park, this process of data collection is, for the British and Allied military, a protected and secure one. Indeed, the very existence of this establishment is described (after the Allies' Ultra Mega code) as 'the second best kept secret in the world' (Stephenson, 2000, p. 143). Bletchley Park functions, then, as a shielded and safe repository which will, apparently, ensure the survival of particular nation-states.

Golgotha is elaborately constructed as a subterranean crypt not only to be invisible to those in search of it, but also to be impenetrable to those who seek to disinter Japan's purloined gold. Goto Dengo, Golgotha's chief engineer of this mine, describes the consequences for unauthorized intruders who attempt to enter this vault:

> 'Anyone who attacks Golgotha will attack from above—to gain horizontal access, the distance is too great. This means they will have to tunnel downwards, either through fresh rock or through the column of rubble with which this ventilation shaft will be filled. In either case, they will discover, when they are about halfway down, a stratum of sand, three to five meters in depth, spread across the whole area… There are a dozen of these', he says. 'Each one leads to the Lake Yamamoto shaft – so pressurized water will be

> behind it. The only thing holding them in place right now is tar – obviously not enough to hold back the pressure of the lake water. But when we have filled these rooms with sand, the sand will hold the manholes in place. But if a thief breaks in and removes the sand, the manhole explodes out of its seat and millions of gallons of water force their way into his excavation' (Stephenson, 2000, p. 661)

Just as Bletchley Park is built as an informational archive which serves those who command Allied nations, so the physical invulnerability of Golgotha is, then, seen to ensure the economic security of post-war Japan.

Even these most complex attempts build the fortunes of the nation-state around various modes of secure storage are, however, compromized in *Cryptonomicon*. Such repositories, supposedly ordered instruments in the service of the *archons* of the nation-state, are at times seen by this novel to require interpretation by those who do not govern. Bletchley Park, for example, works not as an intelligence archive which is accessed and controlled by Churchill or Roosevelt but as a facility in which interpretation has become the responsibility of the state's functionaries:

> It is early in November of 1942 and a simply unbelievable amount of shit is going on, all at once, everywhere. Zeus himself would not be able to sort it all out, not even if he mobilized the caryatids—tell them never mind what we told you, just drop those loads. Temples collapsing everywhere, like spyglasses, he'd send those caryatids—and any naiads and dryads he could

> scare up—to library school, issue them green visors, dress them in the prim asexual uniforms of the OPAMS, the Olympian Perspective Archive Management Service, put them to work filling out three-by-five cards round the clock. Get them to use some of that vaunted caryatid steadfastness to tend Hollerith machines and ETC card readers. Even then, Zeus would probably still lack a handle on the situation. He'd be so pissed off he would hardly know which hubristical mortals to fling his thunderbolts at, nor which pinup girls and buck privates to molest. Lawrence Pritchard Waterhouse is as Olympian as anyone right now. Roosevelt and Churchill and the few others on the Ultra Mega list have the same access, but they have other cares and distractions. They can't wander around the data flow capital of the planet, snooping over translators' shoulders and reading the decrypts as they come, *chunkity-chunkity whirr*, out of the Typex machines. They cannot trace individual threads of the global narrative at their whim… (Stephenson, 2000, p. 162)

Stephenson's text attaches a similar loss of political – narrative – authority to Golgotha. In order to protect the integrity of this crypt, Dengo and his fellow engineers (those who know its secrets) are, upon its completion, condemned to death when they are sealed within it. Dengo's escape, and his subsequent disclosure of its location both to an international group of conspirators (including Enoch Root and Lawrence Waterhouse) at the end of the Second World War and, later in the novel, to Avi and Randy, mean that it ceases both to exist covertly and to function securely. Because of this compromized existence, the gold that is

housed there fails to protect either Japan's economic interests or its narrative of national identity.

Cryptonomicon also explores the ways in which today's archives, which increasingly take the form of networked storage, are moving regulatory power further from those who manage the social sphere. The sultan of Kinakuta is acutely aware of this transfer of power when he describes his country's data haven as one which requires the abnegation of governmental authority: 'Our policies concerning free speech, telecommunications and cryptography have evolved from a series of simple, rational decisions. But they are today so complex that no one can understand them, even in one single country, to say nothing of all countries taken together' (Stephenson, 2000, p. 318). However, the consequences of such policies for Kinakuta's national autonomy are equally complex: although the Crypt brings economic benefits to Kinakuta, it must also result in a corresponding loss of the sultan's political power; or, in a more Derridean idiom, the Crypt might well emerge as an expression of monarchical authority, but this archive at the same time requires the archon to renounce hermeneutic authority.

Derrida does not read this functional transformation of the archive – this transfer of power from one interpretative body to another – as the outcome of a deliberative drive for political justice. For Derrida, archives produce conceptual uncertainty as much as they allow the secure location of information: archives are 'at once *institutive* and *conservative*' (Derrida, 2000, p. 7), since the consigning of documents necessarily changes the significance of that material. Archives preserve the status of documents, but they also subject these documents to the modifying effects of storage technologies and open information to further interpretation. It is because of this ambiguous function, Derrida

argues, that the precise and enduring meaning of archived information cannot be guaranteed: 'The archive', he writes, 'always works… against itself' (Derrida, 1996, p. 12),

The Crypt's relationship to both Kinakuta and Epiphyte exemplifies the ways in which archives both allow preservation and provoke transformation. The data haven is located on Kinakuta because of this nation's particular qualities, and yet this new technology for the storage and distribution of information leaves Kinakuta's future uncertain. Kinakuta embraces the technological opportunities that are offered by a data haven, but it can do so only by modifying itself as a sovereign nation. Since the Crypt will allow transnational groups further to disregard national and international law (and thus further diminish the influence of nations), Kinakuta's national status must eventually suffer from its technological enterprise. Writing for itself an impossible future, Kinakuta demonstrates how even those nations that renounce their powers to regulate data are threatened by advanced encryption.

Compounding this drift from established modes of collective belonging is Epiphyte's discovery of Japan's buried war gold. This gold is discovered not as a result of Epiphyte's normal business interests, but because of Randy's extracurricular research into his grandfather's archive of wartime codes (which, when decrypted, reveal the location of the mine that houses Japan's gold). In other words, it is an unknown and unforeseeable episode in Randy's family history that leads Epiphyte to rethink the Crypt's purpose. Rather than simply taking the gold and retreating into personal wealth, Randy and Avi see in it the opportunity for founding a digital currency that would be securely located in the Crypt, beyond the reach of governmental legislation and not tied to the bullion depository of a particular nation-state. As one reviewer of Stephenson's novel remarks:

> Randy Waterhouse and his cypherpunk business partners are about to do what everyone else has only talked about: open the first true offshore data haven on a remote Pacific atoll. If they can launch a new electronic currency backed by a few hundred metric tons of Nazi gold, well, that's an even more efficient way to wreck those antediluvian nation states (McCullagh, 1999).

This review's phrasing hyperbolizes *Cryptonomicon's* response to the recoding of the nation-state by both existing and fictional technologies, but it does underline emerging technologies' deleterious impact upon national identity. Crucially, what *Cryptonomicon* further reveals is that these consequences cannot be envisaged, even by those who introduce, promote, and manage them. The Crypt and all that it involves (a transnational digital currency, unrestricted data storage and distribution, secure encryption) is, at the end of *Cryptonomicon*, set to reshape the distribution of political and economic power across the globe. But this archive (like others, Derrida might observe) is one that is already operating in ways that were not anticipated.

The Global?

How are we to account for the recent interest in cryptography? Evidence of recent cinematic and literary interest in the technological protection of information is to be found not only in Stephenson's novel, but also in Robert Harris's 1995 novel *Enigma* (and its filming by Michael Apted in 2001), in Dan Brown's 1996 *Digital Fortress*, and in Fox's five seasons of *24*. It is perhaps no accident that this interest developed at the moment when

several forms of cultural anxiety merge: fallout from the millennial fear that technology is making humanity's future uncertain, greater demand for secure systems for email and online commerce, and the fear that other regions of the world are becoming unreadable. In order to overcome these anxieties, we persuade ourselves that our secrets are inaccessible to others, and we remain confident that greater intellectual and technological sophistication allows our official representatives to decipher others' secrets. But who is this 'we'?

Stephenson's text suggests that these cultural anxieties result from a questionable understanding of technology's history and function. *Cryptonomicon* suggests that both the anxious disavowal and the clamorous embracing of today's technologies fail to perceive the shaping of the past by information (and especially cryptological) technologies. More importantly, it suggests that the concept of 'we' is being profoundly reinvented in ways that are now troubling the nation as a system of collective belonging. It does so not by endorsing globalist pronouncements on the nation-state's terminal decline, nor by suggesting that governments will prevail in the face of the technocultural threat. Instead, this novel shows how technologies are in a process of constant negotiation with the institutions of the nation-state. Data storage and distribution technologies here open up planetary-wide communication traffic but, in a world that is not yet global, they draw upon the economic, material, and intellectual resources of the nation-state at the very moment that they challenge national borders and work to divest nations of their regulatory authority.

References

Castells, M. (1996-7), *The Information Age*, vols 1-3, Oxford: Blackwell.

Churchhouse, R. (2002), *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet* Cambridge: Cambridge University Press.

Cybercrime (2007), 'Meeting of G8 Justice and Home Affairs Ministers' . Retrieved March 15, 2007, from http://www.cybercrime.gov/g82004/g8_background.html.

Deleuze, G. & Guattari, F. (1988), *A Thousand Plateaus: Capitalism and Schizophrenia*, trans. Brian Massumi, London: Athlone.

Derrida, J. (1996), *Archive Fever: A Freudian Impression*, trans. Eric Prenowitz, Chicago: University of Chicago Press.

Derrida, J. (1997), *Politics of Friendship*, trans. George Collins, London: Verso.

Derrida, J. (2006), *Geneses, Genealogies, Genres and Genius: The Secrets of the Archive*, trans. Beverley Bie Brahic, Edinburgh: Edinburgh University Press.

Garner, D. (1999 May 23), 'Click Here', New York Times. Retrieved March 15 2007, from http://query.nytimes.com/gst/fullpage.html?res=9A0DE3DB113FF930A15756C0A96F958260.

Hardt, M. & Negri, A. (2006), *Multitude: War and Democracy in the Age of Empire* London: Penguin.

Hayles, N. K. (2005), *My Mother was a Computer: Digital Subjects and Literary Texts* Chicago: Chicago University Press.

Lessig, L. (2004), *Free Culture: How Big Media uses Technology and the Law to Lock Down Culture and Control Creativity* Harmondsworth: Penguin.

McCullagh, D. (1999, May 17), 'The First True Cypherpunk Novel', *Wired.* Retrieved March 15, from http://www.wired.com/news/culture/0,19720-0.html.

Piper, F. & Murphy, S. (2002), *Cryptography: A Very Short Introduction* Oxford: Oxford University Press.

Zielinski, S. (2006), *Deep Time of the Media: Toward and Archaeology of Hearing and Seeing by Technical Means*, trans. Gloria Custance, Cambridge, Mass.: The MIT Press.

[1] The name of this software – Virgil's 'a new order of the ages' – is, of course, most associated with the reverse side of The Great Seal of the United States. Ironically appropriated here, it names the cryptographic tool used to resist the intrusive gaze of the nation-state.

[2] The description of PGP by William Crowell (Deputy Director of the USA's National Security Agency) suggests similarities between it and Stephenson's fictional Ordo: 'If all the personal computers in the world – approximately 260 million computers – were to be put to work on a single PGP encrypted message, it would take on average an estimated 12 million times the age of the universe to break a single message' (Cited in Singh, 1999, p. 317).