# Designing Against Surveillance

Bruce D. Larkin

This paper is not about technical defenses against surveillance, such as encryption, nor is it about methods to hinder and avoid surveillance. The 'surveillance' that concerns us is that typified by collection and analysis by the US National Security Agency (NSA) and Britain's GCHQ.

A global conversation has been prompted by Edward Snowden's disclosure of selected NSA and GCHQ practices, supported by documents said to be from NSA files. At this writing NSA has not denied that the documents are authentic.

## *The Problem: Technical Blunders*

The US government—its executive, in the first instance, and the 'intelligence community' that it commands and controls—has committed three blunders in building and carrying on NSA's surveillance programs, with long-term, serious consequences. Perhaps because the blunders are technical, concerning the structure and use of the Internet, criticism has been largely confined to exchanges among the technically informed. But the damage is immediate, far-reaching, and beyond recall. It appears that

- NSA has actively worked to weaken, and evade, widely-used tools for encryption.

- NSA has contrived to install 'back doors' in software and hardware.

- NSA has crafted ways to intercept Net traffic on an Olympian scale, with the stated purpose of exploiting communications content and metadata for intelligence purposes …

and it has done all these things in 'secret'.[1]

I term these 'blunders' because they strike at the Net itself, increasingly the backbone of collaboration and economic exchange across the globe. The Net is of extraodinary value to Americans and to the United States: hence undermining it is a profound *blunder*. It is not only personal correspondence that moves on the Net, but also complex negotiations, designs—of devices, of software—of economic value, and money itself—trusted orders to transfer funds. Recall the phrase 'in strict confidence', a reminder of the extent to which many transactions depend upon security of communications.

The quest for ways to solve the problem of security in a world of digital transactions relies heavily on encryption, tamper-proof communication, and the physical integrity of the hardware on which people work and on which the Net runs. The NSA has sought advantage by breaching the purposes and expectations of each of these.

From the narrow vantage of the United States, the NSA's actions cast suspicion on numbers of US software and hardware firms … and above all on companies—for example, Google, Facebook—that handle quantities of their users' Net transactions and data about those users.

This is not about Edward Snowden. It is about NSA hubris and arrogance. It is about disdain for the rights and capabilities of

1. James Ball, Julian Borger, and Glenn Greenwald, "US and UK spy agencies defeat privacy and security on the internet," *The Guardian*, 5 September 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

people in other countries. NSA officials and their political managers lived in a dreamworld in which they could know more about others than anyone would imagine while *no one found out what they were doing*. Oh, there would be suspicions, and occasional newspaper exposes, but the stir would calm down, and their projects prosper.

A return to the *status quo ante* now seems unlikely. And not only for the United States. There are countries—Britain, China, among others—whose authorities have aspired to mimic some of NSA's 'achievements'. They are now on warning.

## *The Problem: Assaults on the Public/Private Distinction*

In what ways do NSA practices challenge long-standing distinctions between the 'public sphere' and a person's place in the 'private sphere'? How does NSA surveillance focus the tension between the State and the People? And how does surveillance impinge on the assumptions and requirements of a democratic polity?

- 'Bulk collection'
- Secrecy
- Dossier compilation
- Leakage and 'misuse'
- Exposure of selves
- Masquerading behind legalities
- Deceptive 'accountability'

These are rather different categories than those circulating in the immediate post-revelation commentaries, dominated by phrases such as 'spying', 'invasion of privacy', 'balance between security and privacy', 'non-US persons', 'intercepts', 'acquisition', and the [US] Foreign Intelligence Surveillance Court. The difference is that the latter terms are rooted in ongoing practice and its justification by the United States government (and even by its critics), whereas the terms on which I propose to focus go to the heart of the question

whether bulk secret surveillance is compatible with political freedom and democratic societies. Explaining each:

• *Bulk collection*. Once upon a time police practiced surveillance of suspected criminals and suspected 'foes of the regime'. Targets were individuals, or at least suspected members of groups. 'Bulk collection', by contrast, is gathering 'data' about everyone, or at least very large numbers of adults *and children*, as they go about their daily affairs and transactions.

What is dangerous about this? See 'Dossier compilation', below.

• *Secrecy*. Government insistence on secrecy goes far beyond the 'sources and methods' of traditional spying. In the world as revealed by Snowden, the people do not know, and cannot find out, what 'information' is held about them. They do not know, and are refused being told, what 'rules' govern surveillance practice and how it works. As a result they cannot challenge 'facts' or process: they cannot confront 'facts' they would know to be false, and cannot contest the process by which those 'facts' are compiled and defined as 'facts about them'.

• *Dossier compilation*. Many commentators have made the point that the *gravest danger* posed by NSA/GCHQ is that methods conceived and engineered today *in a belief that they were aimed only at wrongdoers, to protect the people*, could at some future time be the instruments of a repressive totalitarian state. Is such a state possible? Of course. History is strewn with societies that have fallen under repression. Some call NSA/GCHQ practice already "beyond Orwell."

NSA administrators insist that they take great pains to protect against misuse of data. That is not the point. The point is that NSA is preparing the means by which some later US government could carry on repression against its enemies, real and imagined. And in two ways: first, in associating 'facts' with personal dossiers, in

digital files easily reproduced and retained, and second, by establishing a *pervasive infrastructure of surveillance*.

However commendable their motives, however far from their minds such an outcome may be, today's NSA officials and facilitators are laying the groundwork for a future police state.

• *Leakage and misuse*. Even if the state and society appeared to go on about daily life much as in the past, collection of information even on today's scale enables all sorts of mischief: blackmail, denial of jobs, exclusion from the Federal workforce, being 'listed' on secret lists. We have ample recent examples. FBI chief J. Edgar Hoover was understood to have used information against those whom he disfavored. The example of FBI actions against Martin Luther King, Jr. are well-documented. We read of federal, state, and local employees being warned or punished for accessing personal information about celebrities and people they know. Consider the 'no-fly list'. Consider unexplained delay of citizens returning to the United States, typically refused any reason for their not being promptly admitted.

• *Exposure of selves*. This is close to concerns about 'privacy'. Compilation of dossiers, or gathering 'big data' from which dossiers can be compiled at the click of a button, threatens the individual with loss of control over the ways in which the self is exposed.

• *Masquerading behind legalities*. NSA/GCHQ practice illustrates how an *appearance* of legality can be constructed. Prior practices are stretched. Law is 'interpreted', extending mandates and

secrecies.[2] Judicial decisions center on the margins, the edges, while sidestepping actions that may have been, and be, unconstitutional.

• *Deceptive accountability.* The people are led to believe that 'reasonable men' are exercising scrutiny over secret programs, when in fact they have neither the access nor authority to expose wrongdoing … if they were not complicitous from the outset.

## *Isn't Surveillance Necessary?*

Advocates of surveillance à la NSA/GCHQ make a two part argument: first, that there are evil-doers about, who would do harm if not interdicted, and, second, that surveillance contributes *decisively* to interdiction. The first claim is certainly true, though typically exaggerated. The second is rarely true, if at all.

Exaggerated? The evil-doers repeatedly cited by advocates of surveillance are 'terrorists', drug dealers, paedophiles, and dealers in, or prospective users of, 'weapons of mass destruction'. The problem with their argument is that the number of 'terrorists'—including those who might contribute to nuclear proliferation—is small. And the drug dealers and paedophiles conducting large-scale operations are also few. The oft-cited calamity—a nuclear weapon detonating in a city—would be terrible indeed, but in the almost 70 years of the nuclear era no nuclear weapon, nor sufficient fissile material to make one, has fallen into the hands of evildoers.

2. US Representative James Sensenbrenner, a co-author of the USA PATRIOT Act, explains how 2006 amendments to the Act, about §215 of the USA PATRIOT Act, were twisted to *authorize* bulk collection. Sensenbrenner: ""We had thought that the 2006 amendment, by putting the word 'relevant' in, was narrowing what the NSA could collect. Instead, the NSA convinced the Fisa court that the relevance clause was an expansive rather than contractive standard, and that's what brought about the metadata collection, which amounts to trillions of phone calls." Dan Roberts, "Patriot Act author prepares bill to put NSA bulk collection 'out of business'." http://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill

Is surveillance a *decisive* protection? We don't know—a consequence of abundant secrecy. But we can say that, given what we've been told, convincing evidence of a decisive role for NSA/GCHQ-acquired intelligence is not present. NSA and GCHQ officials claim that information collected has contributed to preventing some 50 or more 'terrorist' actions. Those who follow the main cases are skeptical.

It's true that attackers have succeeded. The Tokyo subway attacks, 9.11, attacks on the metros in Madrid and London, the Mumbai and Nairobi assaults all testify to the ability of organized groups. They gather personnel and weapons and execute carefully timed terror operations. In some cases they have been aided by police and governmental shoddiness: Aum Shinrikyo's Tokyo attacks were preceded by preliminary events that the police failed to pursue, and the 9.11 attack on the United States was anticipated in the headline of the 6 August 2001 President's Daily Brief announcing to GW Bush that "Bin Laden Determined to Strike in US"—a warning that Bush and his entourage evidently ignored. The director of the NSA at this writing, General Keith Alexander, claims that if the NSA had had today's capabilities in 2001 9.11 the attack would have been prevented.[3] But that's only a guess on his part: an "opinion." And it fails to take into account precautions and countermeasures against NSA surveillance that would have been available to the 9.11 attackers.

## *A Public Life? Or 'Zero Defects'?*

Once upon a time a campaign was taken up among manufacturers to build products with 'zero defects'. Motives were good. Better that goods leave the factory with no discernible defects—avoiding costly compensation to buyers and rebuilding confidence. Results

3. General Keith Alexander, in testimony to the Senate Intelligence Committee on 25 September 2013. "In my opinion," General Alexander said, "if we had had that prior to 9/11, we would have known about the plot." Charlie Savage, "Senators Push to Preserve N.S.A. Phone Surveillance," The New York Times, 26 September 2013.

might not be *perfect*—zero—but designing systems and practices with 'zero' as an objective enabled plant managers to spend where reducing defects was most cost-efficient. For example, they could compare the cost of a new automated testing step to the cost of accepting returns due to the defect that, in the absence of the test, were shipped to consumers. They wrung the greatest benefits from urging 'zero defects' without imposing unreasonable contortions on the workforce. That, at least, was the plan.

Society, however, is not a manufacturing floor. There is no 'product', a finite number of items in serial production for sale. Instead there are *conceivable harms* that any person, or group, could choose to impose.

Harms—collaboration withheld, attacks, threats—would be real, if executed, and could be extraordinarily serious. The designated mission of NSA and its partners is to warn of planned harms and provide information enabling the harm to be prevented or contained.

'Intelligence Community' managers face two difficult problems. They do not know what hostile acts they might face, nor by whom hostile acts might be planned and undertaken. They can draw a picture of the most serious possible attacks—those for which the technical prerequisites exist, or could come to exist—and allocate resources against those.

In speculating about attacks the most commonly cited are dispersal of weaponized anthrax or the use of a nuclear weapon on a populated target. Either could be so serious, resulting in tens of thousands of deaths and breakdowns in society and the economy, that prevention is considered a *commanding imperative*. Hence 'national security' requires, it is argued, *whatever means are available* to reduce the probability of prevention's failure.

That takes us to point two. Not knowing who might conceive and execute a consequential attack, everyone is considered a suspect. Emphasis shifts from traditional law enforcement focus on persons *committing suspicious acts* to the far more difficult focus on persons *harboring or revealing suspicious thoughts*. Stereotypes come into play. I do not mean stereotypes of 'Muslims' or

'Pakistanis', alone. I mean that 'analysts' are trained to take a targets' expressed interests, or contacts, or travel, or adopting a critical posture toward the 'analysts' and the institutions they serve, as signs of a significant possibility that the target might plan or contribute to an attack. And hence 'national security' also requires, it is argued, *whatever means are available* to 'harvest' facts about the suspects' transactions and beliefs. To do any less would risk leaving at large a man or woman with hostile intentions.

This posture is rational. It is not contradicted by any physical facts: anthrax can be weaponized, and nuclear weapons can be assembled. Means exist for conspirators to conceal their intentions and commit unspeakable acts: Aum Shinrikyo proves it. But the posture of absolutist 'security' is at the same time irrational, because it renders unrecognizable the 'nation' of the phrase 'national security'. It reminds us of the Vietnam War: "it was necessary to destroy the village in order to save it." It pits State against People.

## *Aims*

A society defines itself by the purposes it enacts, and the means it adopts. We ask "how would we like to live—by what means and to what ends—in a world in which massive intrusion is possible?" Champions of mass surveillance argue that it is needed if we are to be safe, and grudgingly grant some restraint at the fringes. What light would it shed on surveillance to ask instead what society we would choose?

Here are some answers, in light of which mass surveillance can be tested:

- We wish to be free to speak our minds, to persons of our choice.

- We wish to write what we choose and retain our text, confident that it is off-the-record until we share it with someone else.

- We wish to be free to exchange correspondence (including texts and graphics) with others.
- We wish to be free to gather with others and speak freely what is on our minds.
- We wish to be free to hear others and read whatever we choose.
- We wish to be able to spend private time with others, preclusive of monitoring or intrusion.
- We should not be denied a job, or housing, or admission to study or to practice a trade, or be subject to any analogous denial, for reasons that are withheld from us.
- We wish to be free to move from place to place.
- We wish our friends and colleagues the same freedom to join us and to participate in our society.
- We wish to be able to maintain 'commercial secrets' including designs and methods.
- We wish to be free to employ whatever means of encryption or anonymization we choose, to protect the integrity of our communications, and as a precaution against interception and theft.
- We wish to participate in the ordinary political life of the communities in which we find ourselves.
- We wish to live daily life with a sense of being safe and secure.

This list is not complete, but it suggests the expectations that men and women in society ought reasonably to enjoy. We immediately think of obstacles and qualifications. Obstacles: inequalities, abuses, failures of reciprocity, competing desiderata, and the merits of regulation cited as reason to constrain 'wishes'. Qualifications: subject to law, subject to 'balancing' autonomy and intrusion, subject to 'cultural norms', subject to 'good sense'. And the nagging question whether we can have 'safety and security' without granting special powers, threatening the society we wish, to police and intelligence agents.

## *Four Issues of Disagreement: (i) Encryption.*

'Good society' advocates could argue that the NSA should devote its substantial talents in cryptography to building strong and open cryptographic systems for public use.

Why do this? Consider financial transactions: keeping 'money' in accounts, and moving money from one account to another. Without conviction that money transfers would be performed as intended, and that 'accounts' were not subject to concealed changes in the dark recesses of cyberspace, the trust on which society's economy rests would be undone.

Instead of pursuing this path, NSA—we are told by those who have access to the Snowden papers—has sought to undermine encryption wherever it could. It seems to have worked on solving known systems, seeding others with weaknesses, and devising strategies to evade encryption (such as capturing messages before or after the period during transmission to which encryption was applied).

Many specialists judge NSA's anti-encryption strategies as its worst assault, and have noticed the irony that it is the United States and other intense economies that rely most heavily on encryption.

## *Four Issues of Disagreement: (ii) Bulk Collection.*

The objection to bulk collection is that it takes *everyone* as a surveillance target, so that people understand that they are subject to being watched but only the elite—intelligence managers, 'analysts'—know whose data is actually being assessed. In practice, of course—and this is a point that the Intelligence Community makes in describing its activities as benign—there is far too much data being collected than any reasonable number of people could pore over. We thought the creature secret police of East Europe employed vast numbers, as filers and informants, managers and analysts, but imagine what would be required to make sense of data arriving at the rate of 2,000,000,000 items *every day*![4]

The Fourth Amendment's drafters did not envisage bulk collection. The amendment requires of an application for a warrant that it be: "particularly describing the place to be searched, and the persons or things to be seized." 'Everything, everywhere' is not 'particular'.

The Foreign Intelligence Surveillance Court came to an artful finding that bulk collection was legal and met the Fourth Amendment requirements. There was no one in the room to object.

Seizing 'things' requires that a sequence be followed: suspicion, warrant ("probable cause"), collection (seizure), analysis , reporting (results), storage, retention, erasure (if retention is not for an indefinite period). At issue, in NSA's handling of data, was whether 'acquisition' took place when the data was collected, or only when it had been assessed by an analyst. In its intricate provisions distinguishing citizen (and permanent resident) records from foreign records the NSA simply bypassed applying its own rules and those of the FISC to citizen records it held. They could be held for five years, and if encrypted indefinitely. When it was convenient to search for the records of a US citizen the analyst could order such a search, or so it appears. The NSA's sequence became warrant (for bulk collection), collection (seizure), storage, suspicion, analysis/acquisition, retention, decryption (if necessary and possible), erasure (if convenient). Steps were compressed in

4. See Appendix B. Indicative Numbers.

NSA's 'listening' to streamed conversations or other digitals, as the analyst was prompted by appearance of a designated trigger in the stream.

## *Four Issues of Disagreement: (iii) Retention. Dossiers.*

With passage of time, retained files accumulate. The scattered pointers to files from, to, or about a person and his or her contacts become more numerous. The result is something much like the 'dossier' of once-upon-a-time police work, a file of fragments that, taken together, offer a profile of a person of interest. The Snowden papers detail use of contacts to compose the 'profile' of an individual. It may no longer contain plaster impressions of the person's footprint, but it could contain a fulsome record of travel, mobile telephone calls, purchases, and comments on social networks.

It may be troubling, to anyone watched, to imagine that such a dossier exists. In practice, no dossier may yet have been assembled from the 'big data' collected, but it an be assembled at any time by invoking software designed to organize the files and construct a profile.

It is to some degree troubling that a dossier can contain error. Society has ample experience with error in credit reports and 'no-fly' lists. But the most troubling feature of a dossier, or the raw materials from which one an be assembled, is that at some future time the dossier might be employed to coerce or sideline the target, expose her as a prospective political enemy, place her friends and family at risk, or even exclude her from her country of citizenship. Then there is the issue of youthful indiscretions … recorded for posterity. And the power of dossiers to break up political opposition, criminalizing its leadership, silencing it, preventing critique of the party in power: all the liver and kidneys of the one-party state, the totalitarian state, the pure ideological state, and the simple but cruel dictatorship.

## *Four Issues of Disagreement: (iv) Spying on 'Foreigners'*

It seems utterly strange to me that the NSA leadership and its political and military advocates did not expect that its practices would be exposed and NSA defined as a demon out of control. Or, more accurately, believed that whatever practices might be rumored or claimed or encountered could continue to be concealed behind smoke and distortion. After all, charges about NSA and GCHQ and the entire "Five Eyes" had been made before, published in newspapers before, and even exposed by whistle-blowers. So it should not seem so strange to me.

But what I want to stress is that *the scale of NSA operations is so vast, and so globally intrusive, that it permanently cripples the United States as beacon of the rule of law, a government of laws not men, of 'liberty and justice for all.'* Its practices are those of an intelligence-gathering Abu Ghraib, the inmates—prime ministers and ministers of foreign affairs of all states, friendly and contentious—stripped of their dignity and threatened by dogs.

How diplomacy is practiced will change. Officials will rely on novel measures to conserve the conversation and negotiation that is central to building collaboration. And the United States, and Great Britain, will not be trusted. Which country was it that, we are told, set up a computer space for the delegates to a G-20 gathering of which it was host … to trap every keystroke, every Skype call?[5]

It must seem strange to French or German readers that the FISA Court bends over backwards to protect the rights of US citizens but declares NSA free to intrude upon citizens of other countries without limitation. Without limitation. I smell arrogance and ignorance. And I suspect that there are other countries whose

5. Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger and James Ball, "GCHQ intercepted foreign politicians' communications at G20 summits," *Guardian,* 16 June 2013. "Foreign politicians and officials who took part in two G20 summit meetings in London in 2009 had their computers monitored and their phone calls intercepted on the instructions of their British government hosts, according to documents seen by the Guardian. Some delegates were tricked into using internet cafes which had been set up by British intelligence agencies to read their email traffic." http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

governments and militaries and 'Intelligence Communities' would like nothing less than to imitate the practices and collection of the NSA. How will the United States condemn such actions? Which dictatorship's surveillance of dissidents will it be free to contest?

## *Key Terms [i]: Secrecy*

NSA's ostensible aim in fostering a culture of secrecy was to conceal its abilities and practices from malefactors, from 'targets', including foreign governments. There were consequences, some flowing from 'secrecy' itself, others from management's wish to avoid limits on what it could do.

First, NSA and its sister agencies relied on 'security clearances' and thoroughgoing classification of documents (Secret, Top Secret, &c.), managing not only who within the agencies could read a given document but also to which foreign governments, if any, the document could be released.

Second, not everyone in the US government would know what NSA did. And even those who did know could not freely tell others.

Third, in place of the usual mechanisms by which government departments are supervised and controlled, novel mechanism were substituted. New mechanisms *looked like* the familiar ones—a Court, an Inspector General, memoranda setting out rules, and a fabric of required approvals (for example, by Department of Justice officials). I pursue the *appearance* of overview and control in discussing lies and deceptions, below.

Its critics charge that NSA chose to conceal even the broad outlines of what it was doing. What could have been told to the public, because 'general' or widely suspected, not endangering 'sources and methods', was also withheld. But it was precisely 'sources and methods' that NSA had fashioned, refined and

employed that provoked public outrage, and denunciation by foreign governments. The mire into which the Cheney-Bush administration fell in launching war on Iraq and the 'War on Terrorism' is *sui generis*, but it is not inappropriate to observe that the most serious charges against Cheney-Bush also concerned concealment of 'sources and methods': torture, other forms of gross mistreatment, and indefinite detention without charges or recourse. "The end justified the means." And so it was with the NSA and its collaborators.

Secrecy insulated NSA against the flood. But when its programs were disclosed, the dam broke and the waters surged. Up to that point NSA's managers, civilian and military, were the willing audience for NSA and Department of Defense claims that 'national security' and 'preventing another 9.11' trumped all criticism. They were, after all, grownups, 'realists', those who knew the threats, those who understood force and necessity, set apart from the broad American public and conniving foreigners who did not have the truth. Somewhere it is written that the quest for truth flourishes only in the bright light of day. NSA's motto was 'keep them in the dark'.

## *Key Terms [ii]: 'Privacy.' Immunity From Intrusion*

Secrecy, however, is often useful, even necessary, to a good life and a productive economy. When we claim a 'right to privacy' we mean that what we do within some private sphere should be secret from others, unless and until we choose to make it known. We do not tell others, for any of a number of reasons, whatever it may be we think of them. We 'share secrets': we negotiate, with our conversational partners, what we will share and what confidentiality we expect.

At stake in the Snowden disclosures is that NSA has affronted reasonable expectations about our 'private sphere'. We had understood that social life could be carried on in certain ways, privately, only to discover that someone is *able* to watch us as we go about our day's tasks. Leave aside the issue—the fact, for almost

everyone—that no one among the watchers is actually listening to our conversations or passing our name to a search algorithm that will assemble a dossier for her perusal. But they *could*. They *could*. That is what is intrusive. And if the Snowden documents are as true as they appear then intrusion into the 'private sphere' of one of us and the 'private spheres' of our 'contacts' and in turn of *their* contacts is altogether possible. With exceptions in everyday speech—'Peeping Tom', gossip, 'credit checks', surveillance cameras—we assume and are probably safe in doing so that we will observe intrusions into our 'private sphere' and be able to resist or evade or respond. Even 'will you please open your bag?' announces itself. In daily life we imagine that we can actively defend our privacy. The NSA revelations change that. We have lost the belief in immunity from intrusion.

## *Key Terms [iii]: Lies and Deceptions*

The NSA/GCHQ documents, as described, evidence a pattern of misrepresentation, intended to guard the secrecy of the "Five Eyes" and resist limitations on their use of increasingly invasive technical methods. With time they devised new and more ingenious ways to gather 'information'. We could categorize their devices this way:

- representation of new practices as simple extensions of practices (copper wiretaps, 'pen register' hardware) approved by courts and legislatures for decades;

- specious interpretation of the Fourth Amendment, or application of prior judicial interpretations of the Amendment that strip away its plain language. Examples: that the Fourth Amendment protects only US citizens; that the Fourth establishes the standard of 'reasonableness' but after 9.11 what might have been 'unreasonable' before is now 'reasonable'; that the requirements of 'probable cause' and 'particularly

describing the place to be searched, and the persons or things to be seized' do not bar authorization of bulk collection.

- reliance on the secret Foreign Intelligence Surveillance Court and the FISA Court of Review to 'approve' as legal aspects of NSA surveillance;

- claims that NSA and GCHQ activity has exposed serious threats and enabled their interdiction;

  correspondingly, exaggeration of the threat posed by specific people captured and tried;

- actual deliberate misrepresentation in sworn testimony;[6]

- invocation of 'national security';

- diversion to the details and intricacies of 'minimization';

- claims that departure from declared guidelines and approved practices are 'accidental' or an artifact of complicated data management;

- the claim that the issue is Snowden, rather than abuses and conduct of the officials responsible;

6. "Oversight only works when the agency that oversight is directed at tells the truth, and having Mr Clapper say he gave the least untruthful answer should, in my opinion, have resulted in a firing and a prosecution." Representative James Sensenbrenner, referring to Director of National Intelligence James Clapper [who, writes Dan Roberts, "admitted misleading the Senate intelligence committee about the extent of bulk collection of telephone records"]. Dan Roberts, "Patriot Act author prepares bill to put NSA bulk collection 'out of business'." http://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill See also Andrea Peterson, "Patriot Act author: 'There has been a failure of oversight'," *Washington Post*, 11 October 2013, at http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=355538

- orchestration of materials presented to Congressional committees charged with oversight, refusal and delay in presenting those committees or their members with requested information, and blurring the difference between 'informing Congress' and 'informing four members of Congress'.

## *Can We Be 'Secure' Without 'Show All, Tell All'?*

Yes. But to have that we must set aside the 'current model' of intrusion, collection, and retention, and fashion a 'new model'. What would that 'new model' look like? These features:

- Collection ('search and seizure') only by contestable warrant. "Contemporary Fourth Amendment."

- Therefore, no 'bulk collection'.

- Identical protections for US citizens and non-citizens, regardless of location.

- Identical rules for 'content' and 'metadata'.

- Retention limited to ongoing criminal cases, and investigations of foreign and corporate agents.

- Identical protections for encrypted and unencrypted transactions.

- Identical protections for anonymized and non-anonymized transactions.

- Criminalizing intrusion except by warrant. Therefore, no secret 'back doors' to software or hardware, no unwarranted 'wiretaps', no bugs installed except by warrant.

- Criminalizing compilation and retention of a dossier about an individual, except as expressly acknowledged to the subject beforehand and explicitly permitted by law.

- A subject's assured access to any consequential government dossier or decision. 'Consequential': leading to punishment or denial of an advantage. (Except: see 'criminal investigations' below.)

- *Criminal investigations*. Right to timely notification that an investigation has been launched, what crime is suspected, and why investigators believe charges can be proven. (Except: see 'countering secret operations', below.) That is: the point is to deter pursuing criminal intent, rather than pouncing and punishing.

- *Countering secret operations*. On the other hand, the public and the State should not grant advantage to persons or groups intending, having a plan to break the law, to exploit secrecy and assurances of private inviolability. Investigators can draw from two toolboxes: that of conventional policing, and a second of methods that require suspension of 'new model' guidelines. In the case of suspected *secret operations*—say, by a drug gang, or operatives controlled from a foreign embassy, or a free-lance terror conspiracy—investigators would approach a panel, created for the purpose, and ask for an explicit, time-limited suspension of 'new model' guidelines for a well-defined purpose. In effect, they would follow the Fourth Amendment's realistic assumption that there could be "probable cause" in a specific case justifying warranted "search and seizure" of "persons, houses, papers, and effects," but that otherwise "no Warrants shall issue." The burden of proof is on the State.

and especially

- Steep cuts in the funds and personnel of NSA and other military and 'intelligence' operations practicing wholesale collection.

- Devising methods of openness and collaboration with the governments of other countries to practice 'mutual reassurance' that evasion of decryption, bulk collection, and intrusion on governments and international organizations are not taking place.

- Joint work to further strong open encryption and to collaborate in suppressing threats to communications, including financial transfers.

## *The Problem of 'Bad Guys' and the Necessity of Global Collaboration*

Nothing in what is written here should be taken as neglect of evil and evildoers. Society must take prudent precautions, devote resources to its defense, and nimbly identify and prevent specific conspiracies whose members intend to inflict harm on the People and their collective interests.

As it happens, NSA's accumulated means and datafiles, alongside the similar and associated collections of the Drug Enforcement Agency, Central Intelligence Agency, US Postal Service, and other US and UK government bodies, tempt any 'law enforcement' body to value broad collection and ready access. They see a tool useful to 'law enforcement' and value it.

An historical distinction posed a problem. Until the PATRIOT Act was enacted in October 2001, law enforcement eschewed access to 'foreign intelligence' information because two different regimes were applied. Ordinary law enforcement operated under a straightforward understanding of the Fourth Amendment. 'Foreign intelligence' evidence-gathering, on the other hand, enjoyed freedom from the disciplines of the Fourth Amendment. An ordinary criminal case that relied on evidence from a 'foreign

intelligence' case could be thrown out of court. This boundary was called 'the wall' … and a notorious provision of the PATRIOT Act was to bring down that wall. As James G. MacAdams III describes it,

> the Act, among other things, amended the requirement that the applicant for a FISA order certify that ***the purpose*** of the surveillance is to obtain foreign intelligence to require only that the applicant certify that ***a significant purpose*** of the surveillance is to obtain foreign intelligence,[7]

In this 'new era'—distinguished by computers, telecommunications, air travel, and their corresponding vulnerabilities—can society protect itself without adopting the NSA program of vast and inclusive surveillance and dossier-building? Much depends on how the State uses well-established powers. Consider these examples of what is available to the Untied States:

- *Fourth Amendment warrants*, to 'search and seize … papers and effects,' which readily extends to digital files and communications.

- *Customary police methods*. Police, including federal police, assemble evidence to show 'probable cause' that a crime has taken place, or is being planned.

- *Identification*. The United State does not employ France's carte d'identité, or Japan's registration of households. Still, much of the US population holds a passport or driver's license.

---

7 James G. MacAdams III, "The Foreign Intelligence Surveillance Act (FISA): An Overview," http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf, citing 50 U.S.C. § 1804(a)(7)(B).

- *Computers and telecommunications*. If 'bad guys' can take advantage of the 'new era', so can police and counter-intelligence. Messages, dossiers, fingerprints, photographs can all be shared in a matter of moments.

- *An alert public*. In large measure the security of any society depends on the good sense of ordinary people. We can distinguish ordinary vigilance from those forms of monitoring that are as fraught as intrusive surveillance: armies of informers, the 'internal pass', McCarthyism, tracking borrowing at the local library. The post 9.11 slogan "if you see something, say something" skates between what is prudent and what is insidious. On the other hand, we reasonably expect, whether laws mandating reporting were in place or not, outlets selling nitrogen fertilizers from which an Oklahoma City bomb could be constructed to treat an unusual purchase as a reason to call the police.

  But of course even alert counterintelligence and police warnings can be ignored, as the FBI's fumbling of reports of pilot trainees pre-9.11 showed.

- *Collaboration with foreign governments*. NSA/GCHQ justify themselves by self-identifying as the decisive bulwark against terrorist bombs and nuclear proliferation. The very title of the Foreign Intelligence Surveillance Court and NSA's extensive collection activities *outside the United States* point to targets abroad. Collaborations, many preceding 9.11, have since 9.11 been extended and enhanced.

  It would be an interesting research project to compare 'bad guys' identified, or better understood, by use of NSA's collections, with what had become known about them by other governments before being alerted by NSA. The Boston Marathon attack by the Trsarnaev brothers in 2013 took place *despite FSB warnings about the elder brother, Tamerlan*

> *Tsarnaev, issued to the United States and despite FBI interview of the elder brother.* The FSB warnings did not extend to the attack itself. More to the point, however, neither the FBI nor NSA gave any warning of the attack. After the fact, NSA officials claimed a role in developing information about one or more of the Tsarnaevs' contacts in the United State, which of course prompts the question 'was that all they could do?'

It's a tough question how to share with foreign governments while protecting one's own secrets. This question must arise even among the "Five Eyes". Frank Koza's well-publicized memorandum calling for intensive attention to sources at the United Nations in the days leading up to the Iraq War explicitly exempted the United Kingdom from being a surveillance 'target': after all, NSA and GCHQ are partners. It is also a problem for 'coalition operations' among militaries of different countries.

Still, it would be a more tractable problem to negotiate protections for cables and foregoing 'bulk collection' than to negotiate general assurances for 'cyberspace', as some have proposed. Governments need reliable information about their world if they are to shape reasonable policies and not be consumed by ungrounded fears. The Cold War reinforced that lesson. Possible lines to negotiate would grant the expectation that ongoing intelligence collection continue, but that to the extent reassurance could be achieved by other means those means would be increasingly relied on. Recall that the 'NATO-Russia Founding Act' signed in May 1997 provided for Russian representation at NATO.[8]

## *How Can Conflicting Desiderata Be Resolved?*

8 Julianne Smith, "The NATO-Russia Relationship: Defining Moment or Déjà-vu?", Center for Strategic and International Studies and Institut Français des Relations Internationales, November 2008, p. 3.

In the section titled 'Can We Be 'Secure' Without 'Show All, Tell All'?' I've listed a number of measures to bring surveillance under administration by the electorate. I would do away with 'national security letters' and require true 'probable cause' judicial warrants, with Fourth Amendment specifics, to undertake 'search and seizure'. Collecting the text of email or a postal letter ('content') would require such a warrant, naming the individual suspect. Collecting data about a transaction ('metadata') would require the same judicial warrant.

As a principle I would prefer that all persons, US and foreign, were assured the same protections. 'Foreign intelligence' operations cannot be simply wished away. As I've noted, prudent policy must be well-informed, especially about threats imagined to begin abroad. As long as the United States collects abroad Washington must expect that other capitals will collect in the United States. What posture should the White House take toward an effort by—say—China to intercept a US fiberoptic cable, within the United States, and collect all streaming transactions? One guess is that bilateral reciprocity could be applied to collecting on each other.

It is hard to imagine bilateral or global prohibitions. Evasion would be easy, discovery possible, forensic attribution open to dispute. Nonetheless, large-scale bulk collection, requiring vast machine sites and legions of analysts, would be difficult to conceal, depending on scale. Limits could be agreed. An obstacle to restraint is the likely wish of authoritarian states to exercise tight domestic control.

There are other openings for collaboration. As long as there are nuclear weapons, all countries have an interest in nuclear command and control, now tied to digital systems, being secure. All have a similar concern about the technologies associated with chemical and biological weapons. The argument extends to financial transactions. Each of these tasks takes us to encryption.

Knowing that the NSA is said to have sought to weaken and evade widely-used encryption, we can be sure that the ongoing quest for stronger encryption will be in high gear. We do not know where that will lead. To the extent that methods can be found that

are 'open'—that is, hardware and software fully accessible to inspection—adequate confidence may be achieved. But the 'spy v. counterspy' model, the applicable model while State encryption depends on secret systems, ensures rivalry. And I haven't heard of any method to break open a chip and examine its most intricate circuitry … that didn't turn it into incomprehensible dust.

In urging an 'independent body' to oversee that practice honors limitations established by law, I acknowledge that every institution's 'independence' or 'autonomy' is subject to the politics of how it is staffed, funded, and overseen itself. If Congress and the White House fail to sustain its independence, the 'independent body' will become that in name only.

A thumbnail of my recommendations:

[1] transfer retained NSA technical functions, such as providing expertise for US government computer and telecommunications security, to new, small, civilian agencies;

[2] among those agencies, one to promote availability and use of 'best practices' in encryption and transaction management; and acknowledge the public's interest in encryption and anonymization;

[3] place remaining NSA in receivership, releasing staff, freezing operations on stored data, and mothballing facilities;

[4] confine collection about named persons, or of transaction data from which a connection to named persons could be inferred, to that warranted by Fourth Amendment judicial consent; and if surveillance of those suspected of clandestine 'foreign intelligence' or 'infrastructure integrity' threats is to be permitted in law, bring that also under the warrant requirement, warrants subject to expiry, and execution of the warrants subject to independent oversight;

[5] cultivate collaborative relationships with foreign governments (insisting that identifying their nationals—terror suspects and Net mischief-makers—is a task for those governments) with focus on the integrity and security of the Net and encouragement of 'best practices' in encryption and transaction management noted above;

[5] design and implement new means to address the problems for which the Drug Enforcement Agency, Customs and Border Protection and FBI have drawn on 'bulk collection';

[6] in chartering any oversight institutions—a court, Congressional committees, an independent body created by law or executive order—design the institution with real autonomy, so that the post-9.11 surveillance practices are not reconstituted;

[7] strive to place and maintain strict limits on classification: that is, make it a positive objective to design work in encryption, network security, counterintelligence, surveillance, and collaboration with other governments—all those areas which at first glance seem the 'natural' areas of strictly enforced classification—so that the work is *either* performable in the open, or to an important degree in the open, *or* the explicit decisions to classify are subject to review and oversight by the 'independent body' posited above.

# *Appendices*

## *Appendix A. Fourth Amendment to the Constitution*

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

## *Appendix B. Indicative Numbers*

The actual number of interceptions performed by NSA has not been acknowledged or reported. However, there are numbers in circulation which give an idea what 'bulk collection' means and how pressed NSA must be to devise means of rendering incoming 'data' useful. It seems that a single interception can yield numerous 'data'. Examples:

[1] "NSA **acquires** more than **two hundred fifty million Internet communications each year** pursuant to Section 702 … ." [Emphasis added.] Memorandum Opinion, Foreign Intelligence Surveillance Court, 3 October 2011, p. 29.

[2] Ron Nixon, "U.S. Postal Service Logging All Mail for Law Enforcement," *The New York Times*, 4 July 2013. http://mobile.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html

[3] Ron Nixon, "Postal Service Confirms Photographing All U.S. Mail," *The New York Times*, 2 August 2013. "The Postal Service on Friday confirmed that it takes a photograph of every letter and package mailed in the United States — about **160 billion pieces last year** — and occasionally provides the photos to law enforcement agencies that request them as part of criminal cases." [Emphasis added.] http://www.nytimes.com/2013/08/03/us/postal-service-confirms-photographing-all-us-mail.html

[4] A slide revealed by Edward Snowden describes the unclassified Hemisphere Project: "The Hemisphere Project provides electronic call data records (CDRs)

in response to federal, state and local administrative/grand jury subpoenas. The Hemisphere Database contains CDRs for any telephone carrier that uses an AT&T switch . … **4 billion CDRs** populate the Hemisphere database on a **daily** basis." [Emphasis added.]

[5] Snowden slide titled "Buddy Lists, Inboxes.": "NSA collects, **on a representative day, ~500,000 buddylists and inboxes."** [Emphasis added.]

## *Revision History*

2013.10.20 First published to web.

The *Journal of Political Design* is a cumulative digital-only journal. It is my vehicle for extended discussion of the subject, represented by posts to my blog at

http://design.learnworld.com/

where the index to the journal can be found:

http://design.learnworld.com/JPD/index.html

Please direct correspondence and submissions to editor@design.learnworld.com

*Journal of Political Design* [2013.10.20 pp. 1-30.]
URL: http://www.gcdd.net/JPD/[I]-designing-against-surveillance
Article Title: Designing Against Surveillance
Author: Bruce D. Larkin
[Email: editor@design.learnworld.com] [Web: http://design.learnworld.com/JOURNAL/JPD1]
Date received: 2013.10.18. Date issued to the web: 2013.10.20
[Draft: DD.151B]

Bruce D. Larkin is Professor Emeritus of Politics at the University of California at Santa Cruz, and the Convenor and Director of Studies of the Global Collaborative on Denuclearization Design. He is the author of *Nuclear Designs: Great Britain, France, & China in the Global Governance of Nuclear Arms* (1996); *War Stories* (2001); and *Designing Denuclearization: An Interpretive Encyclopedia* (2008).