NSA Management Directive # 424: Secrecy and Privacy in the Aftermath of Snowden

George R. Lucas, Jr

Naval Postgraduate School (Monterey)

> *"…[Snowden] argued that he had helped American national security by prompting a badly needed public debate about the scope of the intelligence effort. "The secret continuance of these programs represents a far greater danger than their disclosure," he said. He added that he had been more concerned that Americans had not been told about the N.S.A.'s reach than he was about any specific surveillance operation."*
>
> *"So long as there's broad support amongst a people, it can be argued there's a level of legitimacy even to the most invasive and morally wrong program, as it was an informed and willing decision," he said. "However, programs that are implemented in secret, out of public oversight, lack that legitimacy, and that's a problem. It also represents a dangerous normalization of 'governing in the dark,' where decisions with enormous public impact occur without any public input."* (*New York Times*, Friday 18 Oct 2013)

I. Public Security and the Principle of Informed Consent

Whatever else one might say concerning the legality, morality, and prudence of his actions, Snowden is right about the notion of publicity and informed consent, both of which constitute the hallmarks of democratic public policy in the aftermath of Kant (Rawls, Habermas, O'Neill, Lucas, etc). In order to be morally justifiable, any strategy or policy involving the body politic, we might summarize, must be one to which they would voluntarily assent, when fully informed about it. *[Note: One interesting and vexing problem is to show how this principle works collectively in a democracy: i.e., how it applies to the body politic or General Will, as opposed merely to the protections accorded individuals in a liberal state. Is it, for example, a necessary feature of any morally justified rule of law, that such a regime requires full transparency, an absence of secrecy, and in particular, mitigates against policies of "clandestine" laws and policies? What about those undertaken in behalf of public security: e.g., inter-state espionage, but also undercover police work; confidential inter-state agreements, etc?]

What, however, is inherent in being fully informed? Much literature on informed consent dwells on the problematic nature of voluntary consent, given both inequalities in power (and in

vulnerability of subjects or victims of a policy), and the uncertain epistemic features of information about both the contents of the policy, and the risks associated with pursuing it. Physicians, for example, routinely object that laypersons cannot voluntarily consent to treatment, because they are often unable to appreciate the risks and costs (*vis a vis* benefits) of complicated medical procedures, and are in any case frequently so traumatized by their illness or physical vulnerability as to be willing to consent to almost anything. *[Most recently, such a controversy has arisen over the informed consent (or lack thereof) in experimental treatment of prostate cancer during an NIH-funded study at Columbia University conducted in the 1950s using homeless men from the Bowery in NYC.] In other areas of scientific inquiry, as in anthropological field research, "informed consent" is rejected or resisted both on account of a mistaken impression that it "involves signing a release form of some kind" (what we might term "procedural-IC"), and even more, over concerns that the subjects of study, once fully informed about it, will either withhold their permission for it as an unwarranted intrusion on cultural privacy (sacred custom), or, perhaps even worse, will cease to "act naturally" and start instead to "perform" for the external observer, thus ruining the authenticity of field data collected (Lucas 2009).

So, what position should we adopt regarding the prospects of giving "collective informed consent" to a policy of cyber surveillance whose technological sophistication and scope stagger the imagination, and whose implications neither we, nor those implementing the policy, can possibly foresee? Not only do "we" (i.e., the collective body politic) lack the technological sophistication to fully appreciate all the dimensions involved in the workings of this policy, but, as in the dilemma of anthropological field work above, "we" may need to be deliberately blind to some of the features of the surveillance, lest both we (the protected) and those seeking to harm us

(criminals, terrorists, agents of adversarial nations) all begin to alter our respective behaviors in response to the surveillance (in which case it loses some or all of its effectiveness).

Let me propose that the approach embodied in a number of generally accepted and morally justified practices may offer some insight into our current cyber dilemma. I have in mind a variety of otherwise diverse practices that embody secrecy and even clandestine activities, in addition to straightforward respect for confidentiality: e.g., patients asked to participate in a "double-blind" medical experiments; undercover agents working as part of a domestic police effort to apprehend criminals (e.g., drug dealers) or prevent the fomenting of criminal conspiracies; tenure deliberations and blind peer review in academic institutions engaged in the pursuit of scientific research; confidential agreements among heads of state in the pursuit of policies clearly in their respective public's interests; and perhaps, less clearly, espionage agents of rival states engaged in "HUMINT" and "SIGINT" (human and communication or "signal" intelligence) activities that constitute more of a tolerated practice that falls outside of the normal bounds of law and morality, and is allegedly carried out in the name of state security and defense.

If successful, these analogies sadly will not undo the grave damage that the pursuit of secret policies governed by secret laws and courts, as revealed in the purloined Snowden files, may have done to the public's trust in the workings of its government. But examining these analogies may help in the public discussion that this whistle-blower apparently hoped to encourage concerning (in his own words) even policies that might seem "evasive and morally wrong" on other grounds. The common feature of these otherwise-disparate analogies is that the NSA program of massive surveillance (just like double-blind medical experiments, for instance) could (and, I believe, should) involve seeking to inform, and to obtain voluntary consent, from subjects

who are (collectively) to be the object of a study or experiment (or security surveillance) regarding *certain features of which they knowingly and voluntarily consent to remain ignorant*, for the sake of the validity of the experimental results (or, in the present case, for the sake of the effectiveness of the surveillance). We might say that certain procedural details in all of the purportedly analogous instances remain undisclosed, or "secret," but that the general policy itself (the experiment, undercover police work, or big-data surveillance) is not "secretive." Its EXISTENCE and OPERATION are disclosed, and the nature of the risks generally entailed are fully explained to those affected by it, or in behalf of whose welfare the policy is carried out.

II. "Das Leben der Andern"

If these analogies work, we would then need to start over by fully disclosing the generic working features outlined in the heretofore secret memorandum, "NSA Management Directive #424." This, in sum, is all that Snowden's stolen and disclosed files have thus far revealed, albeit in bits and starts ("PRISM" in June, "XKEYSCORE" in July, and the Enterprise Knowledge System and data-chaining most recently, coupled with the extent and scope of data collection of various types throughout this time).

"Mainway," for example, is the code name of the hardware facility, the massive database storage unit located somewhere in Utah, into which NSA has, at least since 2010, and possibly as early as 2006-07, been collecting or storing some $2x10^9$ "record events" per day: logs or records of telephone and cellphone calls, tweets, facebook posts, emails, internet-site visits, GPS coordinates, and so forth. When fully functional (Snowden's public disclosure of this memorandum reveals), the capacity of the site will exceed 10 times that amount daily (20 billion

records). The Enterprise Knowledge System, consisting of a variety of programs like “PRISM” and “X-Keyscore,” constitutes the means by which this enormous trove of so-called “meta-data” is “mined” or analyzed.

“Data-chaining,” the primary task of PRISM, is the linking up into a variety of patterns of these enormous amounts of otherwise individual and seemingly-random, obscure,* and even trivial “record events.” *[I choose and flag this designator specifically, since the relative obscurity of otherwise-public events of these sorts has been found to have a unique stat us in domestic U.S. law, even while specific kinds, such as telephone call-logs or “luds,” were deemed to be in the public domain, with no presupposition of privacy attached, in a 1979 Supreme Court ruling.] The result is a kind of topographical mapping of patterns of movement and communication that filters out or excludes the meta-data of most of us -- unless those can conceivably be gathered up into a pattern that is interesting…or suspicious.

The result might be helpfully compared to the kind of post hoc “whiteboard” that former CIA-interrogator “Brenda Lee Johnson” and her team of priority homicide investigators would assemble following a murder [Kira Sidgwick, “The Closer” (2006-11) TNT cable network]. Except that this “murder-board” would resemble theirs “on steroids,” encompassing a degree of detail and a diversity and quantity of different kinds of data that would vastly exceed the capacities of human investigators. There is one other important difference: while “LAPD Priority Homicide” assembled their murder-board in the aftermath of a serious criminal act, this analysis is attempting to detect a conspiracy in-the-making, in advance of its actual occurrence. This constitutes the kind of preemptive self-defense that is permitted under domestic law in certain restricted situations to foil criminal conspiracies, but which is outlawed under international law in the case of inter-state conflict.

"X-Keyscore" is another program that reviews these connects and assigns resultant score (X= ?), similar to a FICO credit score, that can be calculated in principle for each and every person whose data are incorporated in the data base. Just as a FICO score can be computed by a credit bureau by gathering and analyzing a wide array of otherwise disparate data concerning our economic "health" and financial transactions, so our KEYSCORE offers a quantitative measure of what we might term our "suspiciousness" or surveillance-worthiness. That score may ultimately help human analysts determine whether there might be probable cause for a closer scrutiny of any of the non-random patterns of our communication discerned in the otherwise-discrete, mathematically-driven data-mining of our personal "record events."

The very scope and ambition of this effort may elicit immediate and horrified comparisons with Stasi surveillance programs in East Germany – as detailed in the moving and troubling Oscar-winning German film, "The Lives of Others" (Das Leben der Andern, Berlin, 2006). Certainly that comparison was foremost in the public reaction to Snowden's revelations within Germany itself. While I will argue against such comparisons, still it is the case that the advent of cyber surveillance as a form of preemptive national self-defense highlights two very critical, and as yet poorly understood features of cyber conflict in general.

Firstly, in law and ethics, we distinguish clearly between domestic law enforcement and its monopoly on the use of force under a rule of law, and international armed conflict, in which domestic laws and the rule of law itself have been seriously eroded. A critical feature of the advent of cyber conflict is that it has blurred the distinctions between what were once very different, and relatively clearly distinguishable levels of activity and conflict. Serious cyber crime and cyber espionage, however, are increasingly straying into an area in which nations can,

with increasing plausibility, declare these the equivalent of an armed attack by another state, including a state harboring the spies or criminals.

Secondly, another, even more important difference is that the pursuit of cyber strategy, and the employment of cyber weapons and tactics, have been largely under the control of intelligence agencies and personnel, whose rules of engagement are very, very different from those of conventional military combatants, or from agents of domestic law enforcement. Spies and espionage agents are generally engaged in activities that do not rise to the level of a "threat or use of force" under international law, let alone of armed conflict between states, but many of which constitute criminal acts in the domestic jurisdictions within which they take place. Conventional war, by contrast, is understood to occur within zones of combat in which the conventional rule of law has broken down, and to which only the international law of armed conflict applies. This latter legal regime is far more tolerant than domestic law regarding the permission to pursue conflict with deadly force *[e.g., complaint of McMahan, Rodin]; however, LOAC does entail certain rules, such as non-combatant immunity and proportionality, that do not arise as constraints in the pursuit of espionage. Likewise in domestic law enforcement, unrestricted surveillance, not to mention use of force, fall under strict legal regimes with accountability, oversight, and at least some degree of transparency, including (most importantly) challenges and adversarial review of the policies and procedures pursued.

All of these firewalls and their resulting safeguards have been seriously eroded with the advent of relentless and unrestricted cyber conflict over the past decade. Thus far, this fundamental distinction regarding Rules of Engagement and the different cultures involved in this new form of unrestricted warfare has not been fully acknowledged, lt alone well-understood. *Cyber war is unrestricted warfare carried out by spies and espionage agents who do not think*

themselves bound by any legal restraints, rather than by conventional combatants trained in the Law of Armed Conflict. Unrestricted warfare is NOT legally permissible or morally justifiable in the conventional case, but it is routine practice among agents of espionage. In cyber conflict, and in planning for it, many of the weapons and tactics are specifically designed to operate against civilians and civilian (non-combatant) targets, a feature that would be illegal, and decidedly immoral, in the conventional case *[as my NPS colleague, Neil Rowe, a computer scientist and cyber expert, first pointed out].

III. Defense of the State and its Citizens, versus Oppression and Political Control

The intent of the state or its security and intelligence organizations in conducting such surveillance seems of paramount importance, quite apart from the fear of corrupting influence such powers may come to exert over the individuals and organizations permitted to utilize them. In the present case, we encounter a clear conflict between a hitherto reasonably well-established and accepted norm – viz, privacy – and the alleged violations of that norm through the mining of "meta-data" by the U.S. National Security Agency. All this is in a state of disarray at the moment, as we sort out who has done what, and with which, and precisely to whom, not to mention what the local constable or furniture mover (let alone the French President and the German Chancellor) think of it all.

Through a peculiarity of the history and evolution of the internet, much of the world's internet traffic travels across routes and through internet switches that lie geographically within the U.S. Hence this country is in a unique position to monitor and survey, not only its own internet traffic, but that of the globe. It a well-established fact that the denizens of cyberspace, no matter of what nationality, have a strong anarchist and libertarian streak. So the outrage over the revelations that the NSA was "monitoring" email, facebook postings, Skype calls, and other telephone and

internet communications has been palpable in some quarters. We might take this as strong evidence that the norm of privacy is widely valued from a philosophical perspective as an important right, a kind of exercise of individual autonomy, that ought to be strongly protected. *[CHRON Higher ed author]

Defenders of the practice of email packet-sniffing and meta-data mining more generally, however, reply that there is a second important norm: the security of innocent by-standers. That is to say, we might be found to have a legitimate tension or conflict between a longstanding and widely (although NOT universally) accepted norm of privacy – one that functions with especial vigor in the cyber domain – with a second, and at least as important norm: namely, that ordinary people minding their own business, and who have done nothing especially wrong, do not deserve to be unduly subject to grave but avoidable risks of harm. The second I will term the security norm, and this often appears in the writings of human rights experts as one of the most basic and fundamental of human rights, and, I might add, one of the chief functions of just and minimally-rights-respecting governments: the security of life, person, and property of citizens. *[In a star-crossed and ill-timed Amsterdam Law Forum article -- published, ironically, on 5 June 2013, the same day that the first of Snowden's revelations appeared under reporter Glenn Greenwald's by-line in THE GUARDIAN -- I argued simply that the security of rank and file citizens of all nations might require some relaxation or compromise of the norm of privacy in the cyber domain, not realizing that this conflict had been settled in favor of greater security by agents of our government, out of sight of, and hence lacking the full knowledge and consent of, those allegedly being protected.]

This tension between these two norms is hardly new or unfamiliar. It was, after all, one of the U.S. "Founding Fathers," Benjamin Franklin, who observed that a people that would sacrifice privacy (liberty) for the sake of security will end up with little of either. But Franklin was not, I think, referring to security in the deeper sense that I am now. He was denouncing a cowardly and risk-aversive desire for preserving the existing political status quo at all costs, as opposed to standing up for justice and basic human rights. In our own time, threats to, or violations of privacy have been strongly resisted not merely as an intrusion upon personal liberty, but as an ominous foreboding of increasingly totalitarian or authoritarian control. Hence, if the U.S. monitors the patterns of email traffic among and between foreign nationals now in an effort to combat terrorism and criminal conspiracies, what is to prevent it from opening and reading those emails, or actually listening to those telephone conversations tomorrow, and perhaps [as in the chilling film cited above] moving from merely voyeuristic intrusion to the suppression for political purposes of all free speech and action?

We might reply that the degree of plausibility and severity of the threat justifies the degree of severity of our collective response to it. As with the formation of the TSA in the aftermath of 9/11, or as in the 1950s civil defense campaign against the threat of thermonuclear war, we would likely be willing to accept considerable inconvenience, and attendant limitations or abrogation of freedom and privacy, IF the threat of harm were severe enough – notwithstanding Ben Franklin's warnings on this topic. And wemight be well instructed to review the consequent grave threats to liberty and privacy that our government perpetrated in response (e.g., Hoover's FBI wire-tapping; McCarthyism).

I don’t think thatthis is an impossible puzzle to solve, nor that acknowledgement and response to a grave perceived threat need degenerate into the kind of fear and hysteria that fostered those abuses of government power in the 1950s and 60s. What is required to guard against the hysteria and abuses is, of course, due process, and in particular, adversarial review. Some transparency (e.g., that we are in fact doing this, and why, and who is exercising accountability and oversight, if not precisely how) is also desirable to prevent arbitrary abuses of privilege. It is also important to distinguish between types of intentions. For all the denunciation of the U.S. by the Chinese, in particular, *[NY Times, July 2013] there is no attempt or intent to attempt to “lock down” the internet, control dissent, or otherwise pry into people’s personal lives and beliefs in an effort to control their political expression.

The idea that this is an inevitable outgrowth of public oversight is, at best, an unproven speculation, and at worst, utter nonsense. It is a serious equivocation to compare or draw a necessary and inevitable parallel between the past behaviors of corrupt or authoritarian regimes, and the future intentions and behaviors of basically democratic and minimally rights-respecting regimes. The intent of the Chinese is not to protect individuals from harm, but to control them against their will. The intent of the U.S. is precisely NOT to control or intrude on individuals’ private lives, but perform its legitimate duty to protect citizens from an unreasonable threat of harm. I think the failure in the U.S. case was not in doing what some thought needed to be done for the sake of security, but for sneaking around to do it, and avoiding a very clear public responsibility to seek the understanding and consent of the governed to do so. I realize that consent would have been difficult to obtain, but that’s no excuse for utterly lacking faith in the public collectively to be

able to recognize and distinguish valid motives and procedures from invalid ones, even if a few fringe individuals stubbornly persist in ignoring essential differences.

Accordingly, we might conclude, espionage and surveillance designed to prevent criminal conspiracies or outright warfare, and which aim purely at attribution and denial of anonymity rather than invasions of individual privacy, may be morally permissible if, and only if:

- the focus of the surveillance is limited insofar as possible toward legitimate security objectives and military targets, and the sole purpose is to prevent armed attack or its equivalent;
- the harm threatened is genuine, reasonably well-defined, with legally-defined "probable cause" attached to its alleged perpetrators under surveillance;
- there is suitable transparency, oversight and accountability for the program of surveillance, with full adversarial review of the legal permissions ultimately granted;
- the individual privacy of third parties and by-standers is not invaded, or is harm done to civilians or their property
- ***the security surveillance efforts are known to, and approved by, the public surveilled (informed consent)***

This is hardly a complete or sufficient list of guiding precepts, but I believe this list encompasses some of the "lessons learned" from the Snowden fiasco. It would be an abuse of the legal permission defined above, for example, for a human "cyber warrior" to listen in to Skype conversations between private adults engaged in no crime, or to read their emails for amusement, let alone to impede their free activity or interfere with their political rights of free expression. That such things were permitted to occur, and that the general outline of the program itself was not acknowledged by the political establishment, have both done serious harm to public trust. This can be restored only by adhering in the future to basic principles of sound security as outlined above, including the orientation of administrators of such program

– “cyber warriors” [Matthew Beard, Notre Dame/Australia]– to a basic code of conduct that will serve to guide and limit their actions to justifiable objectives.

[Additional materials on anonymity versus privacy, my particular hobby horse]

2011 cyber conference at AFRI featured a civilian cyber expert working with the FBI and international Interpol agents to round up a huge ring of Russian-based cyber thieves, using precisely the techniques we now, thanks to Snowden, know of as PRISM and XKeyscore. That is, the cops studied the Facebook transmissions of the thieves, and from the patterns and publicly-accessible content of their postings and transmissions were able to track them down and arrest them. I asked at the time if Mark Zuckerberg was on board with this. The answer from the civilian cyber expert was that he didn't think Zuckerberg would want this successful sting to be generally known, but that the technique (classified) was highly effective. Now we know it was PRISM and that law enforcement officials were using these techniques to fight crime on the internet. Did they violate the criminals' right to privacy in doing so? Did the criminals have such rights? Under what legal regime? Were bad precedents set, or unacceptable practices tolerated for the sake of the justified ends they sought? So we have the usual mess to clean up and clear up, once we are on to the nature of the problem. As I say, however, the basic nature of the criminal activity, is quite familiar, common, and generic: suddenly we feel as if we've seen all this before, especially, when all is said and done, the theft of other people's money (Willy Loman) – the internet is where the money is! So we discover that we can classify the criminal acts, even if some old cons take new forms on the internet, and figure out how to prevent them, combat them, and apprehend the criminals, while striving ourselves to remain respectful of individual rights, liberties, and the boundaries of the law – the age-old dilemma of constabulary forces everywhere.

One of the most essential differences or distinctions is that between legitimate privacy and anonymity.[1] There is an enormous conceptual equivocation at work here, one frequently commented on, that seriously impedes informed public discourse on internet security. Internet vigilantes, such as the members of Anonymous, do not distinguish between the two, and seem to act as if anonymity itself were a precious right to be protected. Meanwhile, I've had fellow college professors tell me with a straight face that voting in an election is "anonymous!" "No it's not!" I'll reply. You stand in a public line at the local polling place with your neighbors, at least some of whom know you by sight or by name; you have to produce a voting registration card, and check it against a printed database of registered voters. In fact, we know who you are, where you live, possibly what political party you're registered to support, we know that you voted and when you voted….there's only one thing we don't know, that is none of our business: whom or what you voted FOR. That's private, and NONE of it is "anonymous." The same is true with your sending of postal mail: you as sender, the addressee, date and time of posting, etc – all are known or can be easily noted. But the CONTENTS of the letter is private and protected by law, and cannot be infringed without a legal court warrant. There are other examples that clearly distinguish privacy, and the right to privacy, from anonymity, to which I would argue we have no special right whatsoever.

That's important, as I argue in my ill-fated editorial, because all the talk of "meta-data mining" and the PRISM stuff is largely an infringement (by a computer program, in fact) on your anonymity,

[1] M. Chawki, Anonymity in Cyberspace: Finding the Balance between Privacy and Security, Droit-Tic, Juill. 2006 [available at http://www.droit-tic.com/pdf/Anonymity_Cyberspace.pdf. Accessed 29 July 2013]; Y. Akdeniz, 'Anonymity, Democracy, and Cyberspace', *Social Research*: *An International Quaterly, 69 (*2002): 223-237; G.R. Lucas, Jr., "Privacy, Anonymity and Cyber Security," AMS LAW FORUM 5, no. 2 (Spring 2013): 107-114.

not on your privacy. It's not the content of your phone calls or facebook postings we care to monitor, only the pattern of communication and transmission, just like the Postmaster. If the latter has one of the mail sorters report that you are getting a suspiciously large number of "plain brown envelopes" that look like they might be child pornography, the Postmaster has a duty to report this to the authorities, who might then obtain a warrant to open one of the packages to determine if, indeed, you are breaking the law. That's how meta-data mining works at the post office, and also how so-called "packet sniffing" works on the internet. No human is examining your non-public posts, nor listening in to your skype calls. *[Libertarian colleague's objection: listening to servicemen's pillow talk – my rejoinder, they're breaking the law and violating procedure, and should be severely punished!!] Frankly, I find the current commercial attempts to use your cell phone to track your movements, behavior, reactions, and purchasing patterns in a store to be VASTLY more an invasion, not just of your anonymity, but of your privacy, without knowledge or consent, than anything the NSA is doing to combat terrorism or industrial espionage. I think the public needs and deserves to know that, and I think the public and internet users especially, given the age of tweets and facebook publicity, needs to learn to draw these distinctions more carefully. We have wilfully surrendered aspects of our privacy on the internet already through our own voluntary (if not fully informed or prudent) choices and decisions. That's not a license for "big government" to take even more of it, without our knowledge and consent, but it is surely a mitigating factor in fueling the hysteria that Mr. Snowden's revelations have unleashed.