AMSTERDAM LAW FORUM
VU UNIVERSITY AMSTERDAM

Opinion

Privacy, Anonymity, and Cyber Security

George R. Lucas, Jr.[*]

Introduction

U.S. President Barack Obama, in his annual 'State of the Union' address to the American public on the 12th of February 2013, pleaded specifically for legislation that would address the grave security threats to vital national infrastructure posed by relentless cyber-attacks, while simultaneously protecting the privacy of individual U.S. citizens. His very public plea in this respect was the most recent voice in a rising chorus of concern from political and military leaders in Europe, include the U.K., and elsewhere, lamenting the explosion of cyber espionage (military and industrial), the theft of state secrets and technological innovations, and the increasing vulnerability of the world's energy, financial, and transportation sectors to potentially devastating cyber-attacks.

President Obama's recent address thus confronts us once again with a controversial and as-yet unresolved question. To what degree would rank and file citizens of democratic nations be willing to surrender some measure of each individual citizen's privacy in order to protect themselves collectively against cyber snooping, internet criminals, corporate espionage, and potentially devastating cyber-attacks against their nation's power grid or air traffic control systems, launched by terrorists or 'rogue' nations like Iran or North Korea? Shouldn't any nation and its citizens be willing to take reasonable precautions for the sake of greater security now, precisely so that they can avoid having to make far more difficult decisions later, regarding (for example) the kind of 'kinetic' (i.e., conventional military-force) retaliation that cyber-attacks, cyber harm, and retaliation in self-defense might otherwise require?

I. Sectors of Vulnerability

All this depends, of course, on precisely what measures proponents of greater internet security might actually require. There are three main sectors of vulnerability in any nation's cyber domain: (1) government and military; (2) industrial (including energy, finance, communications and transportation); and (3) individual users in the civilian or private sector, who may interact in myriad ways with either of the two foregoing sectors, as well as with each other. By far the greatest ongoing and persistent vulnerabilities come from individual users in this last sector. It was, for example, an individual technician in Iran's Natanz facility who was suspected of inadvertently spreading the 'Stuxnet' worm worldwide by taking home an infected laptop from work, and using it to communicate with family and associates.[1] As in epidemiology, the vector of infection of a computer virus – and for that matter, the ability of an enemy agent to infect and control individual computers as 'zombies' in a massive 'botnet'

[*] *Professor of Ethics & Public Diplomacy, Naval Postgraduate School. Distinguished Chair in Ethics, U.S. Naval Academy.*

[1] Note that this is one of many speculative theories about how the 'worm' escaped from Natanz after the attack, allegedly launched by Israel and/or the U.S. For a complete account of these events, see D. E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York: Random House 2012.

– is almost entirely a matter of one infected, unprotected individual user inadvertently spreading the virus to other unsuspecting and similarly unprotected users.

Most national militaries and military agencies, and most agencies of national government, in marked contrast, have moved over the past several years to adopt more secure systems and policies, either as a consequence of attacks they themselves have suffered, or as a result of their observations of the serious national security breaches or vulnerabilities in allied nations. Private and quasi-national industries like utilities, transportation, communication and finance have made preliminary strides to improve their information security, but are reluctant to take decisive measures that would prove costly, and perhaps also inconvenient to clients and customers. This is an area that will almost certainly require government intervention, legislation, and perhaps funding.

Apart from the costs and inconvenient administrative burdens imposed upon private industry, the remaining obstacle constantly cited by political leaders in democratic and rights-respecting states, however, is the protection of individual privacy. This is an especially sensitive and seemingly intractable problem, inasmuch as advocates of virtually unrestricted internet freedom object that any measures to enhance internet security will invariably compromise the privacy of individual users. Ironically, it is the individual, private sector of the cyber domain that is most insistent on protections of privacy, even though that sector collectively constitutes the source of the greatest remaining vulnerability of any nation to a cyber-attack.

II. Security Measures for Individual Internet Users

Two factors thus stand in the way of enhanced security, and render the citizens of many nations vulnerable to grave and serious cyber assaults that might do them irreparable harm: (1) the increased costs of such measures, and (2) the intrusions on individual privacy that might result. Figuring out how to bear the costs, and how to distribute the resulting financial and administrative burdens of enhanced security in the industrial sector are strictly matters of public policy that, on their face, appears amenable to rational solution. Governments might provide legislative impetus accompanied with basic financial incentives (through the tax system, for example), while the remaining costs could be apportioned to the industries and their paying customers, all of whom would benefit substantially from these enhanced security measures.

The dilemma of individual privacy, however, is diffuse, ambiguous, and highly emotional. It will not be so easily solved. As noted above, however, this concern is confined almost exclusively to the 'third sector' of the cyber domain described earlier. There is no reasonable expectation of privacy in either of the first two sectors: e.g., when individual employees are using military, government, or even industrial resources to conduct official business. It is only when private individuals are conducting seemingly private transactions – communicating with one another, handling their personal financial affairs, perhaps paying their annual taxes, or conducting sales and commerce on the information superhighway – that the concern for privacy comes to the fore. Individuals do not want their purchases, their preferences, their finances, or their private communications with family and loved ones revealed or made public, or become subject to scrutiny by agents of the nation's security sector. This is, I believe, the most difficult obstacle to cyber security that thoughtful individuals and policy makers must seek to address.

One promising avenue of discussion might be to clarify just what dimensions of privacy are at risk in the quest for greater cyber security, and determine further just how great that risk actually is. This becomes a far less difficult and abstract exercise, however, when we consider

the privacy implications of the concrete, feasible, security measures that have actually been proposed.

In addition to the numerous measures instituted or proposed in the government and private-industrial sectors (none of which pose immediate threats to individual privacy), two additional security proposals pertain to individual users of the internet. If implemented, these two specific measures promise to be extremely effective and relatively straightforward to operationalize. Both have been vehemently opposed by critics, however, as posing grave threats to both privacy and individual liberty.

The first proposal would require that internet service providers (ISPs, such as Verizon or Comcast, Sympatico or Orange) verify, upon an individual's connection or 'handshake' with the provider, that the individual user has installed the latest security software (currently available from most ISPs at no charge, for recommended but voluntary installation). Under this altered regime, an unsafe or unsecured individual user would not be permitted public access to the 'information superhighway', just as an unsafe vehicle would be prohibited from driving on public thoroughfares.

Secondly, and even more controversially, a nation's intelligence and surveillance architecture (such as that of the National Security Agency in the U.S.) could be harnessed to institute routine, random 'packet-sniffing', using mathematical algorithms to scan the enormous volume of a nation's email and other internet traffic, especially at key 'trunk points' of entry into the national system, for abnormal or suspicious patterns of communication. This does not involve a human user reading or scanning the contents of those communications. Instead, a complex mathematical algorithm essentially 'data-mines' the immense volume of traffic for patterns of contact: an IP address in the host country receiving, for example, an unusually large volume of communications from three international sites suspected of being used by terrorists. In this instance, the pattern would be flagged for human scrutiny and, if it appeared that international terrorists might be communicating with the site of a financier in the host country, a warrant would be sought to examine the contents of the communications further, to see if money was flowing from an agent or organization in the host country to finance international terrorist operations.

As stated, however, both of these last measures are strenuously resisted by internet privacy advocates at present as constituting or threatening serious violations of individual privacy. If, critics argue, even in a country like the United States, the Federal Bureau of Investigation (FBI) is already able to intercept and examine the private correspondence of even powerful individuals like the (former) director of the Central Intelligence Agency and the Commanding Officer of NATO's ISAF forces in Afghanistan (as was widely publicized in November of 2012)[2], what hopes do the rank and file citizens, even in allegedly democratic and rights-respecting states, have against intrusions by government agencies into their private lives, especially if these more sweeping, automated, and randomized cyber security measures are enacted?

III. Privacy versus Anonymity

The battle lines thus shape up largely as a conflict between those who favour greater security and control of the internet on the one hand (in order to lessen a nation's vulnerability to what might well become a horrific attack of unimaginable proportions), and those on the other

[2] See for example, David Kleidman, "The Tragedy of John Allen and the Petraeus Scandal," *Newsweek*, 5 March 2013, at: http://www.thedailybeast.com/newsweek/2013/03/04/the-tragedy-of-john-allen-the-petraeus-scandal.html. (Accessed on 22 April 2013)

hand who believe that this entire issue of cyber vulnerability has (like "Y2K") been greatly exaggerated, and represents little more than an ongoing attempt by the institutions and agencies of government to infringe on individual privacy and liberty.

I believe, however, that we cannot resolve this issue constructively until we first learn to distinguish legitimate privacy (and any rights individuals might reasonably claim to privacy), from *anonymity* — something entirely different, with which privacy is often confused, and to which I would claim we have no 'right' whatsoever. Such distinctions are essential if we are to develop a workable and ethically justified set of policies that protect against cyber-attacks. Much of the seemingly intractable controversy rests upon the confusion or conflation of these concepts. If we can sort out that confusion, I believe we might, together, more calmly agree on a reasonable roadmap toward greater cyber security — one that leaves our privacy and essential personal liberties fully intact.

How might we proceed to do this? First, we need to recognize that the concern of internet advocates to protect individual internet privacy invariably equates privacy with anonymity, the ability of individual internet users to conceal their personal identities from public or government scrutiny. But privacy is neither identical to, nor does it necessarily entail or require, anonymity.

Privacy itself seldom involves attempts to cloak one's actions from public scrutiny, let alone does it seek to avoid responsibility or accountability for the legality, moral propriety, or the harmful consequences of one's actions. Privacy is merely a demand that the requirements for public security and individual accountability *not spill over into otherwise unreasonable intrusions into one's personal beliefs or activities that have little or no relevance or consequences for the public*. The concern over the FBI's recent investigation of the otherwise private email correspondence of two prominent U.S. government officials was, in the end, whether the deliberate or inadvertent intrusion into their private lives was warranted by any threat to national security or potential breach of their respective public duties that this correspondence might reveal, for which either might justifiably be held accountable.

Privacy, therefore, as the right (or claim) of non-interference in personal thoughts and actions is not, and ought not to be, viewed with suspicion. The same is decidedly *not* the case with anonymity. In general, claims of anonymity for individuals mirror the claims of governments and organizations to secrecy and lack of transparency: both are generally sought as a license to hide possible mistakes, mischief, violations of law, or even outright corruption. Demands for anonymity serve principally to cloak our activities from observation, solely in order to evade detection and avoid being held accountable for them. As such, demands for anonymity should always be viewed with the deepest skepticism and suspicion.

The infamous shepherd, Gyges, in Book II of Plato's *Republic*, did not acquire and use his 'magic ring' in order to protect his privacy, but to gain the capacity for complete anonymity, and thereby escape all accountability for the consequences of his subsequent unscrupulous actions. In precisely that spirit, NATO's much-heralded anti-corruption "Building Integrity"[3] campaign among its partner nations and allies follows the U.K.-based organization Transparency International in stressing "integrity, transparency, and accountability" as the watchwords of conduct for individuals in government and industry. Anonymity, however, is precisely the opposite of transparency. And the emphasis on anonymity among internet users

[3] See http://www.nato.int/cps/en/natolive/topics_68368.html and T. Tagarev, *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices,* Geneva: Geneva Centre for the Democratic Control of Armed Forces 2010.

is little more than an invitation to thereby escape accountability and to act with impunity. This undermines, rather than promotes, integrity.

To state the contrast with the utmost clarity: anonymity involves the desire to *hide the identity* of the perpetrator of actions that may have *grave and harmful public consequences*, while privacy is merely the demand that the public not interfere in an individual's thoughts or actions *that have no practical public consequences* or significance whatsoever.[4] That is an enormous conceptual difference. And it is important to clarify this difference, inasmuch as most demands for 'internet privacy' turn out to be demands for anonymity instead — even to the point of asserting, with a straight face, that *anonymity itself* constitutes some sort of right.

Asserting that everyone has a fundamental right to anonymity (over and above their right to privacy) is an astonishing claim — patently unprecedented, ridiculous, and (with one important exception) almost entirely without justification. The attempts of a self-proclaimed 'hacktivist' to steal data, or to reveal otherwise private or confidential information, or to deface or destroy an organization's web site – let alone the demands of a pedophile for anonymity in order to engage, without detection or accountability, in patently criminal activities using the internet — are not at all equivalent to the reasonable desire of an individual consumer, for example, not to have his or her personal, private, and fully legitimate product preferences 'captured' by commercial surveillance software or cellphone apps and divulged, in turn, without permission, to commercial and business organizations for purposes of 'targeted marketing.'

Privacy is a broad demand that society, commerce, and the government stay out of such personal matters that are *none of their business*. Anonymity, with one important exception, by contrast, is a very focused demand that society and governments be prevented from discerning even merely the identity of individuals who appear to be engaged in sinister and malevolent activities – harmful, destructive, and criminal activities, *whose deterrence is everyone's business*!

To suggest that these are in any way equivalent, or even commensurate concerns is itself either a monumental misunderstanding of both, or, more likely, a deliberate equivocation on the part of advocates of internet anonymity *who seek to resist any restrictions whatsoever, even of the most reasonable sort,* on their activities. Proponents of anonymity do *not* seek to protect their own or others' privacy. Instead, *they seek to hide their very identity itself*, in order to escape accountability for their actions, believing falsely that, in cyber space, unlike physical space, they are entitled to do whatever they please, to whomever they please, without fear of consequences.

IV. The Sole Justification for Anonymity

This attitude about anonymity must be vigorously contested, especially in light of the grave consequences of the obstacles it otherwise presents for effective cyber security. I would like to propose in response, as a general rule, that we come to recognize that, apart from one important exception, *there is no legally justified nor morally legitimate activity pursued anonymously, that could not just as well be pursued with full transparency and disclosure in public*.

[4] Suggested reading: Y. Akdeniz, 'Anonymity, Democracy, and Cyberspace', *Social Research*: *An International Quaterly* 2002-69, pp. 223-237 or newspaper commentaries such as B. Johnson, 'Is There a Difference Between Privacy and Anonymity?', *The Guardian,* 14 June 2007 at: http://www.guardian.co.uk/technology/2007/jun/14/guardianweeklytechnologysection

That sole exception to this general rule pertains to a relatively few but very well-defined contexts characterized by radically unequal distributions of power. Individual citizens dwelling within ruthless totalitarian and brutally repressive societies constitute the clearest example of such asymmetries of power. Such citizens might reasonably lay claim to anonymity, or desire to preserve their anonymity on the internet, in order to express responsible (if divergent) political opinions within the confines of otherwise reasonable public political discourse concerning the governance and welfare of the nation and of their fellow citizens. And in such cases, which are unfortunately widespread, *it is never "'anonymity' for its own sake that such individuals claim as a right, but merely a protection they require against persecution.* They need this protection precisely in order to prevent unjustified infringement of their other authentic rights (both their right to privacy itself, as well as to free expression of otherwise reasonable and divergent political opinions, without fear of bodily harm or persecution).

A second, familiar example of this sole exception pertains to employees within government or large industries engaged in morally justifiable 'whistle-blowing' in an attempt to expose corrupt or dangerous practices within their organization, or even to express reasonable dissent from established policies. And even within this generally justifiable exception of unequal power relationships, anonymity still can be abused, and its resulting freedom from accountability used by unscrupulous employees instead for morally unjustifiable attempts to 'leak' confidential information or slander the reputations of supervisors or fellow employees. Thus even in these exceptional cases, claims for the protection of anonymity ought to be viewed with grave caution.

It is a measure of the extreme irony of this otherwise cynical and pernicious equivocation that anarchist and hacktivist internet groups like Anonymous and Wiki-leaks demand, and attempt on their own recognizance to enforce, a degree of transparency on the part of governments and the public that they refuse to acknowledge or practice themselves. Although both groups attempt to portray themselves merely as whistle-blowers in service to the public, their activities might be usefully contrasted with the publication by former U.S. Defense Department consultant and military analyst, Daniel Ellsberg, of the so-called "Pentagon Papers" in 1971.[5] Mr. Ellsberg made no claims to a right of anonymity! And anonymity in any case could have been ensured as a whistle-blower simply by concealing his identity as he passed along the classified government documents to the major newspapers to which he divulged them. Neither did he or his severest critics claim that his actions had anything whatsoever to do with 'personal privacy.' Instead, his was an act of civil disobedience, deliberately and publicly defying U.S. law regarding the custody of classified documents, in order to 'blow the whistle' on covert and questionable military activities about which he firmly believed the general public had every right to know. His public act (even for many who disagreed with his judgment) was an act of courage and principle.

The actions of Anonymous and Wiki-Leaks, by contrast, often strike the wider public merely as acts of random vandalism, more akin to teenagers spray-painting graffiti on public buildings – little more than a public nuisance, save when the lives and welfare of innocent persons are inadvertently and thoughtlessly placed at risk — or, even worse, vigilantism, with all the wrongful harm and injustice that routinely accompanies such one-sided and self-appointed 'law enforcement.'

V. Restricting Anonymity, but Preserving Privacy, in the Quest for Internet Security

[5] Wikipedia, the online encyclopedia, offers a complete account of Ellsberg and the "Pentagon Papers" incident, at: http://en.wikipedia.org/wiki/Daniel_Ellsberg.

The distinction between privacy and anonymity are important, primarily because it is *not the violation of individual privacy*, but merely *a somewhat greater restriction on individual anonymity*, that greater internet security requires. The two measures discussed above (the 'handshake' and 'packet sniffing,' respectively) merely threaten to disclose the identity of communicators, not the content of their communications, and so override user anonymity without necessarily compromising privacy. We should therefore inquire in conclusion whether this limitation or restriction (not of privacy, but of anonymity) would constitute an unprecedented or harmful thing in itself.

Consider, for example, that the contents of the letter I write and send through conventional mail are private, and not to be opened, inspected, let alone divulged without my voluntary consent - or, otherwise, without an application by legitimate law enforcement authorities, backed with substantial evidence and submitted to an independent judiciary, in order to obtain a legal warrant. *My identity as the letter-writer, however, is evident to anyone*, including neighbors who see me put my envelope in a nearby postal box, or postal personnel who handle it. While I have a right to privacy regarding the contents of that piece of mail, I am, as a practical matter, far from anonymous as the correspondent. A government's postal personnel, for example, who collect and sort the mail, are perfectly within their rights and public obligations, should they happen to discern suspicious behavior on my part (such as addressing my mail to known terrorists, or receiving mail from known or suspected purveyors of pedophilic materials), of duly reporting their suspicions to appropriate authorities, who must then seek additional evidence to warrant any further request to examine my mail more closely.

I cite this wholly familiar and uncontroversial example, because, by analogy, the email and automated data 'packet sniffing' sought by government authorities to enhance internet security are entirely identical to this kind of normal public scrutiny of my otherwise private correspondence. The contents are not revealed, nor is intrusion into these private matters desired. Rather, it is solely *suspicious patterns of contact* that are revealed in this otherwise private flow of information. And, if and when these patterns are detected or suspected, investigating authorities would then be required to go through an additional, rigorous screening or vetting procedure. These procedures ensure that 'due process' and responsible diligence have been followed when allowing authorities to undertake a closer and more thorough investigation of the significance of these patterns, precisely in order to protect my right of privacy from such investigation or intrusion. All this would be more than sufficient to deter or frustrate criminals or spies, or to detect terrorist networks, without any appreciable limitation on, or invasion of, any individual's privacy. In fact, such security measures on the internet would do little more than put in place in that domain the kind of security and safeguards we already have in place with respect to conventional mail delivery (as well as with the transportation of goods and services nation-wide). What could be wrong with that?

Likewise, the preliminary 'handshake' between my private computer and a public internet service provider does not (as it turns out) violate my privacy, though it surely compromises my anonymity. To demand, in that initial contact, that the ISP scan my personal laptop or computer in order to detect the presence (or absence) of appropriate internet security software, prior to permitting my further access to the public internet, is hardly different from demanding of otherwise private, individual drivers that they obtain a driver's license, and have their cars equipped with suitable safety equipment (like brake lights and seat belts), before venturing from their private property onto the shared public highway. In both cases, this very modest abrogation of their privacy and freedom of action serves their own greater interests, while providing for the safety and security of others.

Indeed, the confused and often hysterical and exaggerated concerns for individual privacy at the expense of greater public safety and security on the 'information superhighway' closely resemble the similar concerns regarding the proper use of actual highways and public thoroughfares at the dawn of the automobile age in the late 19th and early 20th century. Attempts to regulate the presumed privacy and freedom of individuals to travel in whatever conveyance they pleased, obeying whatever rules of the road they chose to acknowledge, were likewise, at first, strenuously resisted. And the initial result was that public thoroughfares in Europe and America, at the dawn of the 20th century, closely resembled the 'information superhighway' at the dawn of the 21st: a bewildering, chaotic, and lawless frontier, a "war of all against all," in which each individual asserted his rights to freedom and privacy regardless of the resulting grave risk of harm posed to others.

Traffic regulation, however, proved not to be a violation of privacy or an unwarranted limitation of individual freedom (at least, not an unreasonable limitation). Simply demanding that all conveyances on public highways be equipped with appropriate safety equipment, and operated by properly-trained and licensed drivers, obeying reasonable legal constraints designed largely for their own safety and convenience, finally (and rather obviously) served the best interests of all concerned, without sacrificing the most salient features of privacy and freedom of action.

I foster a similar hope that, beyond the present climate of hysteria, fear and confusion, reasonable constraints likewise proposed for the 'information superhighway,' solely for purposes of safety and security, will soon meet with similar acceptance. Otherwise, just as the terrorist attacks against the U.S. in September 2011 resulted in subsequent serious assaults upon individual privacy and liberties, so a disastrous cyber-attack of similar proportions may well force far more draconian and burdensome measures on everyone.