415.956.2828 (t)
415.956.6457 (f)

Robert Dollar Building
311 California Street, 10th Flr.
San Francisco CA 94104

202.777.8950 (t)
202.347.8429 (f)

Victor Building
750 9th Street, NW, Suite 710
Washington DC 20001

ROGERS JOSEPH O'DONNELL

www.rjo.com

Government Contracts
January 2014

Privacy vs. Security – A zero sum game?

By Jeffery M. Chiow[1]

He who would trade liberty for some temporary security, deserves neither liberty nor security.

– Benjamin Franklin

A countryman between two lawyers is like a fish between two cats.

– Benjamin Franklin

There is, and always has been, a tension between privacy and security. Nowhere is that tension more evident than in the cyber realm. As a result of an unauthorized disclosure of classified and sensitive information by an NSA contractor, it is now clear that the policy of the federal government has been, in a nutshell, to collect everything and let the algorithms sort it out.

That this has been a key element of our Government's national security scheme for more than a decade is at the same time surprising and obvious. It is surprising because we seldom stop to think about the richness of the digital dossier each of us creates in a constantly connected world. It seems as if it would take a lot of effort to find us in the digital haystack. Who among us does not use credit cards, send e-mails, text messages or

[1] Jeff Chiow is an Associate in the Washington, DC office of Rogers Joseph O'Donnell whose practice is focused on Government Contracts and Government Investigations with substantial information communications technology (ICT) experience. He is a graduate of the United States Naval Academy and USMC combat veteran of the wars in Iraq and Afghanistan. The author wishes to thank Christina Ayiotis, a Cyber Thought Leader, for providing the opportunity to write this paper, and his colleague Oliya Zamaray for doing the best she could in 45 minutes to compensate for my aversion to Bluebooking.

tweets, grant our smartphone permission to find the nearest gas station, indulge our urge to play Angry Birds,[2] swipe a badge to get through security or use the E-Z pass to bypass Bay Bridge traffic? Better yet, who among us has been more than a few steps away from his or her smartphone for more than a few hours at a time in the past three to five years?

When faced with the charge to prosecute a global war on terrorism, in which a small "cell" or a "lone wolf" could possess the evil intent to inflict mass casualties for a political reason or no reason, it only makes sense to crunch the data.[3] Similarly, the very real security threats posed by cybercriminals and hostile state and non-state cyber combatants demands that 21st Century capabilities be harnessed to identify bad actors and conduct offensive and defensive operations via the same Internet upon which the free flow of commerce and ideas depends. The cyberthreats are so acute that federal contractors whose practices pose a cyber-risk to national security systems can be excluded from federal contracting opportunities[4] and at the President's request, GSA and the Department of Defense are considering how to improve cybersecurity through acquisition.[5]

I. CASE LAW REVIEWING THE TERRORIST SURVEILLANCE PROGRAM

As early as 2002, there were reports of government programs designed to collect and sift through massive data sets of phone records and other electronic information.

---

[2] James Ball, Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data, The Guardian, (Jan. 28, 2014), http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data.

[3] President Obama's Jan. 17, 2014 Speech on NSA Reforms, WSJDigitalNetwork (Jan. 17, 2014), http://www.youtube.com/watch?v=p4MKm2uFqVQ.

[4] Deborah Billings, New DoD Cybersecurity Program Expected To Significantly Affect IT Contractors, Bloomberg BNA Federal Contracts Report (Nov. 19, 2013), http://www.rjo.com/PDF/RSM-FCR%2011192013.pdf.

[5] http://www.pubklaw.com/docs/finalcybersecurity01214.pdf.

Many op-eds and law review articles decried the invasion of privacy and questioned the legality of such massive searches under the First and Fourth Amendments.

The Terrorist Surveillance Program (TSP),[6] disclosed by *The New York Times* on December 16, 2005, was the subject of a 2006 lawsuit by journalists, lawyers, academics and others who alleged, upon information and belief, that their telephone and internet communications were being reviewed without benefit of a warrant or other protections that would preserve their privacy. On August 17, 2006, District Court Judge Anna Diggs Taylor (Detroit, Michigan) declared the TSP program unconstitutional.[7] The Sixth Circuit later dismissed the suit for lack of standing. On February 26, 2013, just over three months before the first unauthorized disclosure of NSA's classified documents, the Supreme Court ruled in *Clapper v. Amnesty International, USA*, 133 S. Ct. 1138 (2013), that attorneys, and human rights, labor and media organizations' challenges to the TSP program were too speculative to satisfy standing requirements. On December 16, 2013, in *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925 (D.D.C. 2013), U.S. District Judge Richard Leon (Washington, DC) found that revelations concerning NSA surveillance had cured the standing problem. Proceeding to the merits, Judge Leon concluded:

> I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware 'the abridgement

6 For a short primer on the Terrorist Surveillance Program, see http://en.wikipedia.org/wiki/Terrorist_Surveillance_Program.

[7] *ACLU v. Nat'l Sec. Agency / Central Sec. Serv.*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), available at http://i.a.cnn.net/cnn/2006/images/08/17/nsa.lawsuit.pdf.

> of freedom of the people by gradual and silent encroachments by those in power,' would be aghast.

Id. at *115. Judge Leon found that the plaintiffs were entitled to injunctive relief, but he stayed the order during the period necessary for an appeal of his decision. Throughout the opinion, Judge Leon pointed out apparent flaws in Government representations about the program, relying in one case upon additional press revelations from continuing unauthorized disclosures.

It must be noted that a different District Court Judge, William H. Pauley, III (New York, NY) issued an opinion 11 days later finding that the plaintiffs had standing but reaching the opposite conclusion on the merits. In *ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863 (S.D.N.Y. Dec. 27, 2013), the court said Fourth Amendment protections were not absolute and credited the Government's argument that it must have all of the data in order to identify those data that can prevent another attack like that which occurred on September 11, 2001.

II. BREADTH OF THE TERRORIST SURVEILLANCE PROGRAM

The program of massive data collection that has evolved from the Total Information Awareness[8] program supposedly scuttled over privacy concerns in 2003, is most impressive for the sheer volume of data that is apparently within the NSA's reach. On January 27, 2014 press reports revealed that the NSA could collect user information from smartphone apps revealing such things as marital status, gender, affluence, travel patterns, *etc*. It appears that there is literally no mode of electronic communication anywhere in the world that is beyond the ability of the NSA to collect. Whereas it was inconceivable that

[8] For an introduction to the Total Information Awareness program, see: http://en.wikipedia.org/wiki/Total_Information_Awareness.

NSA could capture and process such massive data only a few years ago, all indications are that NSA is fast-acquiring the capability to mine truly global datasets.

With the compelling security imperative created by a world full of ill-intentioned state adversaries and non-state actors, it makes perfect sense that those charged with providing the nation's security would feel compelled to identify and track down communications or patterns of behavior that indicate a hostile intent. At the same time, our Constitution grants certain rights to Americans, including the right to privacy and the right to be free from unwarranted searches. All signs point to a sea change in views about the proper balance between security and privacy.

III. THE WAVE TOPS OF FOURTH AMENDMENT LAW

A. Fourth Amendment 101

A detailed review of Fourth Amendment law is beyond the scope of this paper, but a review of the wave tops is in order. Ever since Katz paid his quarter and shut the door of his phone booth in the mid-1960s,[9] ever-evolving modes of communication have been targeted for law enforcement and national security purposes. The expectation of privacy Katz enjoyed, however, has been eroded by norms of behavior, claims of Executive prerogative and the third-party doctrine. In *Smith v. Maryland*, 442 U.S. 735 (1979),[10] the Supreme Court found that police could consult Mr. Smith's phone records without a warrant because he had shared the numbers with a third party, the telephone company. "When petitioner voluntarily conveyed numerical information to the phone company and 'exposed'

[9] *Katz v. United States*, 389 U.S. 347 (1967) (discussing the nature of the "right to privacy" and the legal definition of a "search").
[10] Available at: http://www.oyez.org/cases/1970-1979/1978/1978_78_5374/.

that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information." *Id.*

In 1968, Congress passed Title III creating detailed requirements regarding wiretap warrants. In *United States v. United States District Court* ("the *Keith* case"), 407 U.S. 297 (1972), the Supreme Court reviewed District Judge Damon Keith's (Detroit, MI) decision rejecting the Government's claim that it need not get a wiretap warrant in a case involving a threat to domestic security. Specifically, the case involved the bombing of a CIA office in Ann Arbor, Michigan. The Supreme Court agreed with Judge Keith saying that at least for domestic cases, some judicial approval was necessary, but it suggested the hurdle to getting such a warrant might be appropriately lowered in cases concerning national security. In the wake of the Watergate scandal, Congress went to great lengths to investigate and legislate in the area of wire-tapping in order to ensure that the laws provided a measure of protection against Fourth Amendment intrusions.

B. The Foreign Intelligence Surveillance Court

One outcome of that activity was the passage of the Foreign Intelligence Surveillance Act that created the Foreign Intelligence Surveillance Court (FISA). The FISA court, as suggested by the *Keith* case, was established for the purpose of ensuring review of domestic national security wiretap requests by a Title III court, but applied a standard far less demanding than "probable cause." Essentially, the Department of Justice was obliged to follow a procedure and certify that the procedures had been followed. After September 11, 2001, the USA PATRIOT Act effected some changes to the FISA law, but those changes were insufficient to authorize the TSP, which was at the time, a Special Access Program codenamed Stellar Wind.

C. Executive Prerogative and Legal Drama Surrounding the Terrorist Surveillance Program

Prior to any judicial scrutiny of the TSP, it had to be re-approved by the President and the Attorney General every 45 days. That approval requirement led to a dramatic episode[11] in March, 2004 when then-Attorney General Ashcroft was suffering from acute gall stone pancreatitis at The George Washington University Hospital. The current FBI Director Jim Comey was, at the time, relatively new to his post as Deputy Attorney General – Ashcroft's #2. At the urging of Jack Goldsmith, the new Head of the White House's Office of Legal Counsel, Comey had investigated the legal justification for the TSP and found it lacking. He made his concerns known, including to the program's principal advocate, Vice President Dick Cheney and urged Attorney General Ashcroft not to re-authorize the program just days before the Attorney General was rushed to the hospital.

The Attorney General was very ill and his wife had ordered that he not receive any calls, but President Bush, who had learned that there was some problem with the re-authorization called to say that his Chief of Staff, Andy Card and White House Counsel, Alberto Gonzalez were coming to the hospital. News of their visit was conveyed to Jim Comey who was driving home, but raced to the hospital. As reported in *Washingtonian*:

> Comey beat Card and Gonzales to the hospital and ran up the stairs. The White House duo arrived minutes later and marched straight to Ashcroft's bedside. The FBI security detail, who moments earlier had been working one of the quietest assignments they'd ever had in an otherwise empty wing of the hospital, were suddenly very nervous.
>
> Rallying, the drugged Ashcroft explained why he wouldn't sign

[11] Garrett M. Graff, Forged Under Fire – Bob Mueller and Jim Comey's Unusual Friendship, Washingtonian (May 30, 2013), http://www.washingtonian.com/articles/people/forged-under-firebob-mueller-and-jim-comeys-unusual-friendship/.

> off on the reauthorization and chided the administration: "You drew the circle so tight I couldn't get the advice I needed." He finished by pointing to Comey: "But that doesn't matter, because I'm not the attorney general. There is the attorney general." Jack Goldsmith said later that it was such an amazing scene he thought Ashcroft would die on the spot.

Robert Mueller, then head of the FBI, John Ashcroft, Jim Comey and others had drafted resignation letters, but a deal was struck that eventually led to greater oversight, including, in 2006 and since periodic approval of TSP by the Foreign Intelligence Surveillance Court.

D. The Third Party Doctrine

The third-party doctrine has proven to be a slippery slope as no one can send an e-mail or text message, or check the weather without the assistance of an Internet service provider or a cellular service provider or both. Thus, if the third party doctrine is taken to its logical extreme there can be no expectation of privacy in the "To:", "From:", and "Subject:" lines of e-mails the content of text messages or our search terms. The Government requests at least the metadata associated with such communications as a matter of routine. In a recent report, Verizon[12] indicated that "[i]n 2013, [it] received approximately 320,000 requests for customer information from federal, state or local law enforcement in the United States."[13] In so-called Tower Dumps, Verizon provides to government a list of all cellphones that are communicating with a particular tower at a given time. This may serve as the initial list of

[12] Randal Milch, Verizon Releases First Transparency Report, Verizon Public Policy (Jan. 22, 2014), http://publicpolicy.verizon.com/blog/entry/verizon-releases-first-transparency-report.
[13] Verizon Transparency Report, available at http://transparency.verizon.com/us-data.

suspects who were in the vicinity at the time a crime was committed. Google,[14] AT&T and other Internet and telecommunications service providers[15] have also disclosed Government demands for User data, and under a recent settlement with the Department of Justice, such companies will be able to share limited data about the frequency or volume of such requests. Under FISA, the recipient of a subpoena for records, *i.e.* an Internet or telecommunications service provider cannot disclose the fact of the warrant.

IV. WHERE IS THIS ALL GOING?

A. A Trend Toward Privacy

If the security imperative is so great, and if we willingly share with third parties such things as our location, our e-mails and our intellectual curiosities in the form of Google or Twitter searches, it may not be perfectly clear what privacy interest remains in our digital data. Surely Generals Petraeus, USA (Ret.)[16] and John Allen, USMC (Ret.) would have thoughts on that topic. And President Obama in a speech committing to certain reforms indicated that, in his opinion, the level of information collected and stored by the Government and private industry is "disquieting." The House Judiciary Committee has begun new hearings to evaluate the TSP program, and progressively less speculative Constitutional challenges to NSA surveillance are making their way through the Courts.

---

[14] Transparency Report: Government Removal Requests Continue to Rise, Google Official Blog (Dec. 19, 2013), http://googleblog.blogspot.com/2013/12/transparency-report-government-removal.html.

[15] Brian Fung, The First Phone Company to Publish a Transparency Report Isn't AT&T or Verizon, The Washington Post (Jan. 9, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/09/the-first-phone-company-to-publish-a-transparency-report-isnt-att-or-verizon/.

[16] Alyona Minkovski, Gmail and the FBI Took Down David Petraeus: Why It Matters To You, HuffPost Tech (Nov. 13, 2013), http://www.huffingtonpost.com/2012/11/13/gmail-and-the-fbi-took-do_n_2120469.html.

As Government contractors who are increasingly called upon to provide data analysis or to host data, *e.g.* as cloud service providers,[17] it is useful to understand what the rules are concerning information assurance and privacy. It is certainly true that the rules are evolving. The Federal Information Systems Management Act of 2002 (FISMA) imposes obligations on the federal government and its contractors to protect certain information. Some agencies, like the Department of Veterans Affairs (VA) and the General Services Administration (GSA) have developed contract clauses implementing FISMA, but other agencies have not, and there is no uniform approach. The Privacy Act applies to contractors under some circumstances, but when, and to what extent, is far from clear.[18] A recent DFARS Final Rule[19] and a Proposed FAR Rule[20] also provide some guidance for contractors. The NIST cybersecurity framework, to be released in February 2014 (prior to the 2014 Federal Procurement Institute), will also provide valuable guidance. Due to industry concerns, a Draft Privacy Appendix was removed from the Draft NIST Framework in January 2014 – instead, privacy concepts (but not prescriptions) are to be incorporated into the main document. All of these rules, as well as industry-specific requirements for banking and healthcare sectors, create a patchwork of requirements that are difficult to pin down, much less meet. If a contractor does work for VA and GSA but those entities have different or, worse yet, conflicting information security requirements, does the contractor need to maintain different IT systems for each Agency or each contract? What about the contractor

[17] *See* Joshua S. Parker, *Lost in the Cloud: Protecting End-User Privacy in Federal Cloud Computing Contracts*, Pub. Cont. Law Journal, Vol. 41, No. 2, 385 (Winter 2012).
[18] *See* James McCain, *Applying the Privacy Act of 1974 to Data Brokers Contracting with the Government*, Pub. Cont. Law Journal, Vol. 38, No. 4, 935 (Spring 2009).
[19] Available at http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf.
[20] Available at http://www.gpo.gov/fdsys/pkg/FR-2012-08-24/pdf/2012-20881.pdf.

who bids on work for the States of California and Mississippi and New York City, all of whom may have different legal, administrative or contract requirements concerning information security and privacy?

B. Looking Ahead

This panel is particularly interested in thinking about what our obligations may be. While the federal government's experience has been one in which privacy has taken a back seat to security in the decade-plus since September 11, 2001, there has been movement on several fronts toward promoting the protection of information and the preservation of privacy in a cyber-laden world. In January, a newly formed independent federal agency, the Privacy and Civil Liberty Oversight Board, in a 3-2 decision,[21] declared the NSA's TSP program unconstitutional and suggested claims about the program's contribution to national security were not just exaggerated, but false. On January 28, 2014, Rebecca "Becky" Richards was slated to become NSA's first Director for Civil Liberties and Privacy.[22]

As the balance between privacy and security shows signs of shifting, developments we all should consider include:

1. International Initiatives

- Internet Governance[23]

---

[21] Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Privacy and Civil Liberties Oversight Board (Jan. 23, 2014), http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

[22] Al Kamen, The NSA has a new, first time ever, privacy officer, The Washington Post (January 28, 2014) http://www.washingtonpost.com/blogs/in-the-loop/wp/2014/01/28/the-nsa-has-a-new-first-time-ever-privacy-officer/.

[23] The Global Commission on Internet Governance was announced at the 2014 World Economic Forum in January in Davos. https://www.ourinternet.org/#about.

- EU Privacy[24]
- Cloud Computing Standards[25]

2. Geospatial Data Issues[26]

3. Drone Issues[27]

4. Data Breach Issues – FTC's Role in Establishing Standard of Care; California as a Trendsetter;[28] Congress' new "hands on" approach[29]

5. Privacy Impacts in Healthcare and the Medical Industry

6. Privacy Impacts in Financial Services and the Banking Industry

7. Wind down of the Perpetual "War on Terror" – NSA Reforms

8. Government Contractor-Specific Issues

a. Protection of Unclassified Information (FAR and DFARS)

---

[24] John O'Donnell, EU justice chief attacks European "hypocrisy" on spying, Financial Review (January 29, 2014) http://www.afr.com/p/technology/eu_justice_chief_attacks_european_iQTNHfU1rqxro4YxK3ZMxL.

[25] Available at http://www.gsa.gov/portal/category/102371 (FEDRAMP homepage).

[26] IAPP and CSA announce new strategic alliance (January 16, 2014) https://cloudsecurityalliance.org/media/news/new-conference-csa-iapp/.

[26] Kevin Pomfret & Mike Tully, Privacy Issues Raise Concerns for Remote Sensing, Point of Beginning (January 22, 2014) http://www.pobonline.com/articles/97204-privacy-issues-raise-concerns-for-remote-sensing.

[27] "Bills would regulate drones to ensure privacy" (January 26, 2014) http://www.boston.com/news/local/new-hampshire/2014/01/26/bills-would-regulate-drones-ensure-privacy/OZRc0vetCu47y7geX7thyJ/story.html.

[28] David Navette, California Attorney General Files Lawsuit Based on Late Breach Notification, (January 30, 2014) http://www.infolawgroup.com/2014/01/articles/breach-notice/california-attorney-general-files-lawsuit-based-on-late-breach-notification/#.Uupuwv7x-lI.twitter.

[29] January 29, 2014 Letter to Karen Katz, President & CEO, Nieman Marcus, from House Committee on Energy and Commerce (http://democrats.energycommerce.house.gov/sites/default/files/documents/Katz-Neiman-Marcus-Data-Breach-2014-1-29.pdf). January 28, 2014 Letter to Gregg Steinhafel, Chairman, President & CEO, Target, from Senate Committee on Commerce, Science and Transportation (http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=88b26fe9-f089-4f5e-9191-6e43342a456e).

b. NIST Framework – How Well Has Privacy Been Incorporated now that the Privacy Addendum Was Removed

c. Critical Infrastructure- Is Everything "Covered" Under the NIST Framework?

Contractors should be aware of the rapid evolution of these issues. Within the year, the Supreme Court may consider again, the constitutionality of certain NSA programs. The President has already committed to some level of reform. And Congress may, as in the 1970's, feel compelled to take some action to weigh in on how to preserve privacy without forfeiting security. California and other states are already beginning to legislate in the area of protecting consumer privacy. All of these issues are relevant to contractors who should not simply wait for the next FAR or DFARS rule to come out, but should think of ways to preserve the benefits of security while safeguarding privacy. Government often looks to its contractors to deliver answers to such difficult problems.

The content of this article is intended to provide a general guide to the subject matter, and is not a substitute for legal advice in specific circumstances.