Cybersecurity and Privacy: The Challenge of Big Data[1]

Abraham R. Wagner
Columbia Law School
Columbia University, School of International and Public Affairs

Introduction

Recent history has seen both the rapid evolution of cyberspace, accompanied by an enormous expansion in terms of users and capabilities, as well as unprecedented technological, economic and social revolutions. These new technologies have also led to a virtual explosion in the amounts of data resident in servers and systems across the globe – often referred to as "big data." Along with a host of benefits, the era of big data has also brought with it a set of challenges in terms of security and privacy that increasingly affect the lives of Americans.[2]

Cyberspace has created a new venue for both crime and warfare. At the same time the availability of "big data" has also provided an opportunity for the commercial sector to analyze and utilize the data for non-criminal purposes which may still pose serious security and privacy questions. Increasingly the links between those that store "big data," commercial users and the Government have come under great public scrutiny while the courts are dealing with new cases where constitutional issues of privacy are being decided.[3]

Overall this paradigm shift is not simply one of technology, but embraces radical changes in the economics of information as well as the culture of modern society. This is easily the most significant change in media since the invention of moveable type in the 15th Century. While Americans have been quick to embrace the new technologies and capabilities they offer, public policy and the legal regime

---

[1] Comments in response to the Office of Science and Technology Policy, Government "Big Data" Request for Information, March 4, 2014.
[2] See Abraham Wagner, *Cybersecurity – From Experiment to Infrastructure* (Defense Dossier, 2012) and *Cybersecurity: New Threats and Challenges* (American Foreign Policy Council, 2013).
[3] See, for example, *In the Matter of the Search of Information Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.* (Magistrate Case No. 14-228 (JMF)). See also Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

are well behind and in need of serious effort.[4] Here the current laws are decades behind the current technologies and the problems that "big data" poses.[5]

It is also the case that Americans themselves see "big data" as well as the security and privacy concerns raised differently than in years past. Greater use of the technologies and increased awareness of potential problems has changed privacy expectations significantly. For their part both state and federal courts have responded to a myriad of cases with a far more encompassing view of the privacy protections afforded under the Fourth Amendment.[6] The current challenge is therefore multi-faceted. As both the government and the private sector continue to collect, analyze and utilize data norms, policies, and statutes are needed which address the privacy and security needs of Americans while promoting the free flow of information in ways that are consistent with these needs.

Evolution of Cyberspace and Big Data

The rapid evolution of cyberspace and the accompanying rise of "big data" has clearly been one of the greatest technological revolutions in recorded history. What began as a Defense Department experiment at the Advanced Research Projects Agency (ARPA – later DARPA) in the late 1960s has transformed almost all aspects of life with new technologies and an explosive growth in e-mail, the web and net-based applications never anticipated.

Security and privacy were not essential elements of the original ARPAnet design. At the outset the ARPAnet was an experiment in optimizing network resources with "switched packet" technology as an alternative to traditional "line switching." E-mail was not even a part of the concept; the web did not yet exist;

---

[4] Policy studies undertaken since the late 1990s have identified serious problems in the infrastructure, but the response by both the government and the commercial sector has proved to be grossly inadequate. See here PDD/NSC-63 *Critical Infrastructure Protection* (1998) and PPD-21 *Presidential Policy Directive - Critical Infrastructure Security and Resilience* (2013). It is striking that these two Presidential directives, coming well over a decade apart, come to the same conclusions with almost nothing have been done in between.

[5] As discussed at greater length below, one good example is the *Electronic Communications and Privacy Act (ECPA)* enacted in 1986 and codified at 18 U.S.C. §§ 2510–2522. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act, 18 U.S.C. §§ 2701-12.

[6] See Harvey Rishikof and Abraham Wagner, *Cybersecurity and Cyberlaw* (Durham NC: Carolina Academic Press, 2014). See also Michael Warner, "Privacy and Security, Yesterday and Today," in *Cybersecurity and Privacy: Report of the Expert Workshop held for the Defense Advanced Research Projects Agency (DARPA)*(Arlington, VA: Institute for Defense Analyses, 2014).

there were no browsers or net-based content; and, there were no early commercial or national security applications.

Apart from DARPA's developmental work, a wide range of users including the Government, commercial firms, educational institutions and others acquired computers connected to various networks adding data at an exponential rate. With the transition to the Internet, networks were given low-cost global connectivity. For the first time in history, the marginal cost of worldwide communications fell to almost zero, as the "web" made it easier for users with new applications and web-based content growing exponentially.

Few entrants into cyberspace were aware of or cared about the myriad of security vulnerabilities which existed in operating systems, server software, middleware, application layers, router software and elsewhere. For well over a decade, the prevailing notion was that if there were problems, it must be somebody else's job to fix them.

Early Vulnerabilities and Security Efforts: The commercial world was quick to adopt the net, offer a vast range of applications, and generate "big data," but was largely unwilling and uninterested in paying to either secure it or provide privacy. Even banks failed to address the problem until they had been robbed of large sums. Government users were not much better as they quickly embraced cost-effective networked systems but failed to address critical vulnerabilities.

Internet programmers recognized vulnerabilities in operating systems as well as server design. Early attacks generally involved malware which disabled vulnerable computers and exploited data which was not protected, stealing larger amounts of data from servers connected to the net. Microsoft distributed "fixes" and "patches" to deal with some vulnerabilities while third party vendors like Norton sold security software that attempted to deal with a wider range of malware, installed firewalls, and gave users regular updates as new threats were identified.

These early entrants into the field saw the threat from malicious net activity and tried to protect users from malware, removing suspicious code such as viruses, worms and Trojans from infected computers. Other firms offered encryption software, such as PGP, enabling their users to protect sensitive files while a secure version of net protocol (:/https) enabled "secure" transactions over the web. In some ways cyberspace was becoming safer and more secure, but the adversarial threat was advancing at an even greater pace as well.

Growing Threats from Home and Abroad: Growth of e-commerce and "big data" brought new demands for privacy and security, while the proliferation of networked systems national security also required secure networks and applications to high standards. Vulnerabilities continued to be identified while new threats were seen on a daily basis. As the financial sector entered cyberspace, lucrative targets for cybercrime emerged as net-based theft from banks and credit card fraud became a booming business. "Big data" became both and a target and commodity.

While the early threats came largely from youthful hackers and disgruntled system administrators, the past decade has witnessed the evolution of far more serious cyber threats from expert criminals as well as well-trained military units assigned to cyberwarfare missions. Debate continues over the range of potential threats, ranging from denial of service to a type of apocalyptic attack often referred to as a "digital Pearl Harbor" which could involve massive denial of net services, widespread theft of data, or possibly the corruption of data being sent over the net.

Security, Privacy and the Law in the *Jones* Era

The first part of the twenty-first century brought a world of new devices, applications and accompanying "big data." At the same time there have been dramatic changes in user expectations of both privacy and security. In addition, various disclosures as well as major studies about government surveillance programs adopted since the 9/11 terrorist attacks have fueled a broader debate over essential security requirements and competing privacy demands.[7]

It generally is agreed that the legal regime for cyberspace is seriously outdated, and generations behind current technologies. Several key cases are currently before the courts, and proposed legislation is before Congress awaiting action. Major concerns exist as to how new Presidential Directives, laws and court decisions will impact on technology development as well as privacy and national security interests. Certainly the technology path will not stop or be reversed. Increasing amounts of what contribute to big data will continue to accumulate on systems worldwide presenting an ever greater challenge to public policy.

---

[7] See Privacy and Civil Liberties Oversight Board, *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* (January 23, 2014). See also *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (12 December 2013). At the same time as these outstanding studies, unlawful disclosures by Edward Snowden first published on June 5, 2013 in the British newspaper *The Guardian* have received widespread media attention and have served to focus additional attention in this critical area.

Increasingly many Americans believe that the Fourth Amendment protects privacy as a right and that freedom and independence may not possible without some semblance of privacy.[8] Earlier Chief Justice Earl Warren predicted the problem that technological innovation has diminished privacy expectations.[9] Justices Douglas, Brandeis and others have also interpreted the Fourth Amendment as providing a fundamental right to privacy that needs to be upheld in order for justice and freedom to prevail through the ages.[10] At the same time, national security requirements have required practices and intelligence operations which in the wake of the 9/11 terrorist attacks have been viewed as critical and more recently have come under increasing attack.[11]

Data privacy suits have increased in number and notoriety in recent years and the issue of "injury in fact" has become an early challenge for privacy plaintiffs to prove. [12] Normally this type of injury is rarely an issue in lawsuits, but is as big an obstacle for data privacy plaintiffs as Mount Kilimanjaro is for hikers.[13] Here the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[14] Further the Stored Communication Act prohibits providers of electronic communication from "knowingly divulging to any person or entity the contents of a communication."[15]

When Congress passed the Electronic Communications Privacy Act (ECPA) in 1986 it was landmark legislation of its time.[16] That was close to three decades ago, and preceded the start of the Internet by several years. Clearly technology has evolved dramatically in these decades in ways never imagined. [17] Still, by 1986, the

---

[8] *Olmstead*, 277 U.S. at 472-73 (Brandeis, J., dissenting).

[9] *Lopez v. United States*, 373 U.S. 427, 441 (1963)

[10] *Osborn v. United States*, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting); *Olmstead*, 277 U.S. at 472-73 (Brandeis, J., dissenting).

[11] See the opinion of Judge Claire Egan explaining the FISA court's rationale for approving the Section 215 telephone records program, *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

[12] *In re Google Privacy Litig*., at *4 (citing *In re iPhone Application Litig*., No. 5:11–md–02250–LHK, 2013 WL 6212591 (N.D.Cal. Nov. 25, 2013)); *Pirozzi v. Apple Inc.*, 913 F.Supp.2d 840, 847 (N.D.Cal.2012).

[13] *Id.* at *4.

[14] 18 U.S.C. § 2511(1)(a); see id. § 2520.

[15] 18 U.S.C. § 2702(a).

[16] 18 U.S.C. § 2707(a)

[17] Christina Bonnington, Apple Mac at 30: See the Evolution of an Icon, *Wired* (Jan. 25, 2014),; Matt Honan, New Tools Show How Deep Glass will Embed in Our Live, *Wired* (Nov. 19, 2013), and

use of computers and network-related technology had grown significantly and individuals had begun using personal computers to access remote networks and data. [18] When Congress passed the ECPA one goal was to reassure industry that its growth would not be constrained by individuals' fears regarding the privacy of their communications and data maintained on computer servers.[19] Under then-existing Supreme Court precedent, it was far from clear that the Supreme Court would extend Fourth Amendment protection to these new technologies.[20]

Legal scholars have criticized the current law at length. Professor Orin Kerr argues that the lack of a suppression remedy has confused courts on how to remedy an unauthorized interception. [21] Others argue that the all private communication and stored data should be protected equally.[22] Still others have shown that under the current language, the same e-mail is subject to different protection depending on whether it is in transit, stored on a home computer, opened and stored in remote storage, unopened and stored in remote storage for 180 days or less, or unopened and stored in remote storage for more than 180 day, with at least one circuit court going so far as to hold that the lack of protection provided to electronic communication after 180 days in temporary storage provision is unconstitutional because it authorizes less than a probable cause warrant standard to search private communication.[23]

For decades now scholars have debated ways to improve the existing legal regime and its intersection with the Fourth Amendment.[24] One side of this debate

---

Amanda Scherker, Family Banned All Technology Made After 1986, *Huffington Post* (Sept. 3, 2013),

[18] Melissa Medina, The Stored Communications Act: An Old Statute for Modern Times, 63 AM. U. L. REV. 267, 290-91 (2013)

[19] *Id.*

[20] *United States v. Karo*, 468 U.S. 705, 721 (1984); *United States v. White*, 401 U.S. 745, 754 (1971).

[21] Orin S. Kerr, A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1243 (2004)

[22] See, for example, Robert A. Pikowsky, The Need for Revisions to the Law of Wiretapping and Interception of Email, 10 MICH. TELECOMM. & TECH. L. REV. 1, 49-50 (2003).

[23] See *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); Marc Zwillinger, Jacob Sommer. *Warshak Decision: Sixth Circuit's En Banc Reversal in Warshak Sidesteps Constitutionality of Stored Communication Act's Delayed Notification Provision*, BNA PRIVACY & SECURITY LAW REPORT, Vol. 7, No. 31, (Aug. 4, 2008).

[24] See Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299-30 (2004); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809-10 (2004); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 749 (2005); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72

proposes a universal search warrant requirement the other argues that Congress is the best suited to enact laws to protect privacy because the Courts are faced with the disadvantage of trying to hit a "moving target," the continuing development of technology, while interpreting a distinct moment in time, the case and controversy before them.[25] Most experts, however, agree that the existing legal regime needs to be modified to improve its application to modern technology and the demands of "big data."[26]

Fourth Amendment Interpretation: Traditionally, the Fourth Amendment right to privacy has been viewed as a property right.[27] Searches of property required a warrant issued by a magistrate supported by probable cause.[28] While Fourth Amendment right to privacy still maintains its foundation in property rights, the Supreme Court has also supplemented property-based privacy rights with a reasonable expectation of privacy outside of any property right.[29]

Current conceptions of privacy are based on the landmark *Katz* case where the Court held that even in a public place, a person may have a reasonable expectation of privacy in his person.[30] Justice Harlan's concurrence in *Katz* has served as the guiding principle for the analysis of whether search violates a reasonable expectation of privacy, establishing two requirements for a reasonable expectation of privacy: (1) a person have exhibited an actual (subjective) expectation of privacy; and (2) the expectation be one that society is prepared to recognize as "reasonable"(objective).[31] Writing for the majority, Justice Stewart, reasoned, "[W]hat a person knowingly exposes to the public, even in his own home or office is not a subject of the 4th Amendment protection."[32] He continued, however, to say, "But what he seeks to

---

GEO. WASH. L. REV. 1208 (2004)

[25] Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299-30 (2004). S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 FORDHAM L. REV. 779, 782 (2005).

[26] Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 65-66 (2003); Solove, *Reconstructing Electronic Surveillance Law*, op. cit.

[27] See *United States v. Jones, 132 S. Ct. 945, 954 (2012)*, *Florida v. Jardines,* 133 S. Ct. 1409, 1417-18 (2013).

[28] *Shadwick v. City of Tampa*, 407 U.S. 345, 354 (1972).

[29] See *United States v. Jones, 132 S. Ct. 945, 954 (2012)*, *Florida v. Jardines,* 133 S. Ct. 1409, 1417-18 (2013).

Katz v. United States, 389 U.S. 347, 360 (1967).

[30] *Id.* at 351.

[31] *Id.*

[32] *Id.* at 351 (majority opinion).

preserve as private, even in an area accessible to public, may be constitutionally protected."[33]

For close to half a century now, *Katz* has served as a foundation for determining whether behavior constitutes a violation of the Fourth Amendment right to privacy. Moving beyond communications, the Court has applied these principles in considering whether here is a reasonable expectation of privacy in "open fields" outside of the curtilage of a home.[34] The reasonable expectation test remains the as to whether there is a reasonable expectation of privacy where there is no property right at issue, such as in electronic communications or data storage.

Exposure to the Public: Cases following *Katz* stand for the principle that what one knowingly exposes to the public is not subject to Fourth Amendment protection.[35] Furthermore, as the Court articulated in *California v. Greenwood*, "An expectation of privacy does not give rise to Fourth Amendment constitutional protection unless society is prepared to accept that expectation as objectively reasonable."[36]

Most recently the Court has issued another landmark privacy decision in *United States v. Jones*, a case involving a GPS tracker attached to a drug dealer's vehicle without judicial approval, and then used evidence obtained through tracking him to convict him. The Court held that the reasonable expectation of privacy test supplements the property based expectation of privacy and therefore the placing of a tracker on the Jeep, an effect, constituted an unlawful search.[37]

Concurring in the decision, Justice Sotomayor reasoned that unrestrained power to assemble data that reveals private aspects of identity is susceptible to abuse, warning that that it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties because it is ill-suited to the digital age.[38] Foretelling the issues of "big data" Justice Sotomayor went on to raise concerns over the comprehensiveness of a record of personal movements and a "wealth of detail about

---

[33] *Id.*
[34] *Oliver v. United States*, 466 U.S. 170, 184 (1984); *United States v. Dunn*, 480 U.S. 294, 305, (1987).
[35] *Katz v. United States*, 389 U.S. 347, 360 (1967).
[36] *California v. Greenwood*, 486 U.S. 35, 39 (1988). In *Greenwood*, held that garbage left at the side of the road is readily accessible to animals, children, scavengers, and other members of the public.
[37] *United States v. Jones, 132 S. Ct. 945, 954 (2012)*.
[38] *Id.* at 954 (Sotomayor, J., concurring); *Smith*, 442 U.S., at 742, 99 S.Ct. 2577; *United States v. Miller*, 425 U.S. 435, 443 (1976).

her familial, political, professional, religious, and sexual associations."[39] To protect the information, however, requires that "Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[40] As Justice Marshall stated, "privacy is not a discrete commodity, possessed absolutely or not at all."[41]

Subsequently *Jones* has been cited by numerous courts considering a range of privacy issues, including numerous federal appellate courts, the Foreign Intelligence Surveillance Court and the Supreme Court itself.[42]

Meeting the Challenge – Toward a National Policy

It is the unfortunate reality that national policy toward cybersecurity during the 1990s, the Internet's first critical decade was in large part either non-existent, badly managed, poorly funded, and in some cases simply absurd. As the net literally exploded in terms of users and applications, and evolving threats were seen, there was little national consensus as to whose responsibility it was to secure cyberspace and respond to the threats. While the Government and the military became large-scale users, and the "pig at the trough," little was done by to protect this vital resource. As a whole, Government saw this as a responsibility of the commercial service providers while Government programs to deal with it were minimal and inadequate.

What the nation failed to see at that time was the reality of the cyber threat problem, mostly from overseas. As national security, government, and finance became large net users they, adding "big data" to the networked world, they became lucrative targets for both major criminal enterprises, as well as foreign military forces who foresaw the potential for cyberwarfare.[43] At the time America focused largely on defense against hackers and lower level threats, and not looking to the larger evolving threat environment.

While the 9/11 attacks themselves had little to do with cyberwarfare or "big data" they did provide a catalytic shock to the government in terms of looking far more seriously at new threats, particularly in the technology space. Cell phone and

---

[39] Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring); See, e.g., *People v. Weaver*, 12 N.Y.3d 433, 441-42 (2009).

[40] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring)

[41] *Smith*, 442 U.S. at 749.

[42] See *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, op. cit., and *Opinion and Order*, No. PR/TT [redacted] (FISA Ct.).

[43] See, for example, *APT1, Exposing One of China's Cyber Espionage Units* (Mandiant, 2013).

Internet use by terrorists and others now became a serious subject of interest. Programs to focus on these technologies which languished in the 1990s received new attention and support. At the same time a number of early cyber-attacks such as Moonlight Maze (from Russia – 1999); Titan Rain (from China – 2004); and others attacking critical systems drove home the reality of increasing threats.

A Strategy for Cyberwarfare: Increasing cyberattacks from foreign groups have raised the specter of cyberwarfare as a realistic area for future conflict. Analysts continue to debate as to how this new type of warfare, which has no geography, differs from the traditional model of kinetic warfare, and what "rules" of warfare apply, and the extent to which the elements of loss of life and destruction of property – the two cornerstones of the kinetic model of warfare – might apply in the cyberwar context.

Cyberspace is Part of a Highly Dynamic World: Cybersecurity has become an essential element of life in the wired world, which is a highly dynamic one where both the technology base and the threats continue to evolve. For some time now this world has moved into an era of "digital everything" with an almost seamless merger of communications, computing, and media of all kinds including "big data" which are largely digital. Coupled with hardware and communications bandwidth that has become increasingly cheap, the marginal costs of communications are free nearly so in many cases, which have caused use of cyberspace to grow by orders-of-magnitude in a few short years.

The enabling technologies and economics have also brought about some major changes in culture. Use of the net, devices, and advent of "big data" have brought about modern cultural artifacts from Internet dating to social awareness streams. Net-based commerce is fast surpassing all other forms, while businesses as well as the government agencies have become almost totally dependent on net based systems.

System architectures are increasingly moving to a cloud concept, while more serious threats from cyber criminals, cyber warriors and cyber terrorists across the globe continue to grow and it is increasingly important that any policy or strategy have effective defense and offensive elements that aid in meeting overall strategic objectives as well as user demands for privacy, security and resilience. Meeting these sometimes competing demands presents an increasing policy challenge.

Building the Technology Base: Implementing a successful national strategy must necessarily start with building the technology base, and in this area largely involves educating people with the skills necessary to meet the emerging challenges. It is also

an area that simply requires the "best and the brightest" to create the type of software and other technologies required. Educating the necessary to meet this challenge requires a new level of commitment to the nation's universities, possibly using the model of the Eisenhower Administration in responding to the Cold War challenges of the "space race."[44]

This model for cyberspace and "big data" makes good sense, and it is reasonably certain that the universities are not going to meet this challenge utilizing only internal resources. In the current economic climate event the major private universities are constrained, while most public universities are under enormous economic pressure. While there is sound logic that shows there are increasing numbers of jobs in cyberspace, the fact does not seem compelling enough to overcome the level of inertia in education today.

Acceleration of Government Programs: Notwithstanding budgetary pressures, it is increasingly clear that the Government cannot continue to be "the pig at the trough" in terms of massive net use; fail to adequately fund effective security programs; and maintain the false expectation that the private sector will recognize the full scope of the problems and remedy them. Efforts to protect the net and "big data" need continued strong and increasing support. Not all of these tasks can be left to the Defense Department and the intelligence agencies. Without exception all other Government agencies have become major users of cyberspace and need to become partners in its ongoing protection.

Partnership with Industry: Aside from limited government funding, one reason national policy on cyberspace failed in the 1990s was a basic misunderstanding of the role industry could and would play in securing the net and protecting "big data." There were unreasonable expectations that industry would recognize the vulnerabilities and fix them. It was believed that it was not essential for the Government to support this in a meaningful way and that user demands, from both the public and private spheres, would drive industry to meet the challenge, a belief that was only partially correct. What was done was largely inadequate, and insufficient to meet the threats that evolved.

---

[44] At that critical point in history the nation undertook a series of coordinated initiatives starting with substantial government investment in science and math education, under the National Defense Education Act (NDEA). The government initiated new technology agencies, such as the Advanced Research Projects Agency (ARPA), the National Science Foundation (NSF) and others.

Policy now requires a more realistic approach to industry involvement on several levels. It is essential to recognize that industry built cyberspace and created "big data" – and they will fix it, irrespective of who pays. By and large the Government can only write checks – not computer code. Even in the most sensitive areas the actual work is out-sourced to commercial firms with few programmers being Government employees.

Here the nation needs to move to a model where the technology companies that dominate cyberspace are made a more integral part of the process. The model what was highly effective in dealing with the communications firms for decades is a useful one that has not been effectively employed where cyberspace is concerned. Certainly some of the traditional telecoms are "within the tent" but many of the most important and critical firms are not. In the final analysis the nation needs to look ahead at what the solution is going to be, and work back from that, making sure that the technology base and the supporting industrial base can meet the very real threats and challenges ahead.

Another key element of this partnership needs to be with the holders of "big data" including the financial sector; the health services industry; as well as the telecoms and internet service providers who hold increasingly large amounts of "big data." One aspect of this partnership needs to be the timely and accurate provision of threat data coming from government sources and vice versa.[45] Another is a far broader national policy and legal regime that recognizes the role that industry servers and clouds have in maintaining "big data" and protecting both the privacy of users and the security of their data.

These are by no means simple issues. They continue to involve a number of complex technical, legal and financial considerations all of which are in a constant state of change. Here the challenge presented by the Office of Science and Technology Policy represents a useful way to engage a wide range of Americans in the process of developing an effective national policy in this most critical area.

[45] The current Defense Industrial Base (DIB) effort is one useful approach, but a far more extensive set of program is needed.