## UNITED STATES DISTRICT COURT SOUTHERN DISTRICT NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION.

Plaintiff,

- against -

JAMES CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

### **ECF CASE**

Index No. 13 Civ. 3994 (WBP)

# BRIEF OF AMICUS CURIAE PEN AMERICAN CENTER IN SUPPORT OF PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION AND IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Facsimile:

Edward J. Davis Linda Steinman Eric Feder DAVIS WRIGHT TREMAINE LLP 1633 Broadway, 27<sup>th</sup> Floor New York, New York 10019 Telephone: (212) 489-8230

Attorneys for Amicus Curiae PEN American Center

(212) 489-8340

### **TABLE OF CONTENTS**

			<u>P</u>	<u>age</u>	
INTEREST (	OF AM	ICUS (	CURIAE	1	
SUMMARY	OF AF	RGUMI	ENT	1	
ARGUMEN	Γ			3	
I.	THE	PEN D	DECLARATION ON DIGITAL FREEDOM	3	
II.	THE IMPACT OF MASS GOVERNMENT SURVEILLANCE ON THE CRITICAL ZONE OF PRIVACY NEEDED FOR FREE EXPRESSION				
	A.	The 1	History of Abuses of Surveillance	7	
	B. Self-Censorship, Communication, and Creativity				
		1.	Government Surveillance as a Curb on Creative Thought and Expression	11	
		2.	Writers' Frameworks for Understanding the Dangers of Surveillance	13	
III.	THE HIGH SENSITIVITY OF TELEPHONE METADATA 1				
	A. Telephone Metadata's Capacity to Reveal Associations and Private Information				
	B.	The	Particular Risks for Writers and their Contacts	19	
IV.	BALANCING FREEDOM AND SECURITY				
CONCLUSIO	ON			22	

### TABLE OF AUTHORITIES

Page(s)
Federal Cases
Clapper v. Amnesty Int'l, 133 S.Ct. 1138 (2013)8
Memorandum Opinion of the United States Foreign Intelligence Surveillance Court (Oct. 3, 2011)
Olmstead v. United States, 277 U.S. 438 (1928)
Osborn v. United States, 385 U.S. 323 (1966)
United States v. Jones, 132 S. Ct. 945 (2012)
United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012)17
United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297 (1972)6
Other Authorities
PEN International Charter (1948)
PEN Declaration on Digital Freedom (2012)
Declaration on Digital Freedom: FAQs, http://www.pen-international.org/pen-declaration-on-digital-freedom/declaration-on-digital-freedom-faqs/
Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755 (1976)9
James Bamford, The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America (2008)
James Bamford, The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization (1982)9
Jeremy Bentham, <i>The Panopticon Writings</i> (Miran Bozovic, ed., 1995)14
Matt Blaze, <i>Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)</i> , Wired (June 19, 2013)18

Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 St. Rev. 1373 (2000)	
James Debelak, Why the NSA's Gathering of Metadata Matters, Seattle Times (June 15,	2013) 17
William O. Douglas, Points of Rebellion (1969)	13
Michel Foucault, Discipline and Punish (1975)	16
Lyndon B. Johnson, <i>Remarks at the Swearing in of Ramsey Clark as Attorney General</i> (10, 1967), http://www.presidency.ucsb.edu/ws/?pid=28123/	
Franz Kafka, The Trial (1925)	15, 19
Jane Mayer, <i>Verizon and the N.S.A.: The Problem With Metadata</i> , New Yorker (June 6, http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html	
Victor Navasky, Naming Names (1980)	8
Robert O'Harrow, No Place to Hide (2006)	9
George Orwell, 1984 (1949)	13
PEN American Center, <i>Two Views on How Surveillance Harms Writers</i> , http://www.pen.org/blog/two-views-how-surveillance-harms-writers (Sept. 3, 2013).	7
Letter from Gary Pruitt to Attorney General Eric Holder (May 13, 2013), available at http://www.ap.org/Images/Letter-to-Eric-Holder_tcm28-12896.pdf	20
Adrienne Rich, Arts of the Possible (1971)	11
Natalie Robins, Alien Ink (1992)	7
Julian Sanchez, On Fiction and Surveillance (May 14, 2012), http://www.pen.org/nonfiction/julian-sanchez-fiction-and-surveillance	13, 14
Bruce Schneier, The Eternal Value of Privacy, Wired (May 18, 2006)	15
David K. Shipler, The Rights of the People: How Our Search for Safety Invades Our Lib (2011)	
Larry Siems, <i>A Blacklisted Screenwriter on American Surveillance</i> (Aug. 30, 2013), http://www.pen.org/blacklisted-screenwriter-american-surveillance	8
Daniel J. Solove, Five Myths About Privacy, Washington Post (June 13, 2013)	16, 17
Daniel I Solove The Digital Person (2004)	15 16

### Case 1:13-cv-03994-WHP Document 47-1 Filed 09/04/13 Page 5 of 27

Lars Svendsen, A Philosophy of Fear (2008)	21
Melvin I. Urofsky and Philip E. Urofsky eds., Selections from the Private Papers of Justice	
William O. Douglas 162 (1987)	21

### **INTEREST OF AMICUS CURIAE**

PEN American Center is a non-profit association of writers that includes poets, playwrights, essayists, novelists, editors, screenwriters, journalists, literary agents, and translators ("PEN"). PEN has approximately 3,700 members and is affiliated with PEN International, the global writers' organization with 144 centers in more than 100 countries in Europe, Asia, Africa, Australia and the Americas. PEN International was founded in 1921, in the aftermath of the first World War, by leading European and American writers who believed that international exchange of ideas was the only way to prevent disastrous conflicts born of isolation and extreme nationalism. Today, PEN works along with the other chapters of PEN International to advance literature and protect the freedom of the written word wherever it is imperiled. It advocates for writers all over the world who are persecuted because of their work.

The interest of *amicus* in this case is in ensuring that the rights of writers in the United States under the First and Fourth amendments are upheld.

#### **SUMMARY OF ARGUMENT**

The parties will undoubtedly provide the Court with a thorough analysis of the relevant law. The aim of this *amicus* brief is different. PEN's purpose is to highlight for the Court the worrying impact on writers and other public intellectuals of the comprehensive nationwide collection of telephone call records by the National Security Agency ("NSA"). The government's collection of information about every phone call made or received in the United States intrudes upon a personal zone of privacy that is essential to freedom of expression and association.

Writers need to be secure in their privacy and personal freedom to continue to play their critical role in our democracy as thinkers, investigators, dissenters, and advocates for change.

Their work depends on exchanging ideas with others. The "metadata" the government collects

for millions of phone calls has the potential to reveal sensitive information about writers and other public intellectuals and about the communications they engage in. Writers who espouse unpopular ideas and people who challenge government actions must be especially concerned that they can be identified and exposed. PEN members have been subject to surveillance themselves and have studied the effects of surveillance on authors and society. PEN members have also reflected on the effects the NSA program has on their own work. PEN is profoundly concerned that the expectation of privacy that has allowed our culture to flourish and enabled us to govern ourselves will be eroded if we become accustomed to knowing that the government keeps records of all our communications and can compile detailed pictures of our private lives, our work, and our associations. In those circumstances, our communications will become cramped, the scope of thought will shrink, and our democracy will be debased.

The enormous volume of data placed in the government's hands creates a temptation to use it that few governments can resist, and history does not justify having high hopes for restraint. American writers over the last century have been the targets of government surveillance, intimidation, and at times even persecution. Government intelligence and law enforcement agencies have conducted illegal, unconstitutional surveillance, very often in the name of security, paying special attention to writers whose views challenge those in power. Abuses have occurred not only during the McCarthy era and while the FBI was directed by J. Edgar Hoover, but in every administration through the present day. In 2011, the Foreign Intelligence Surveillance Court ("FISC"), which was established to ensure that the NSA did *not* overstep legal and constitutional boundaries, found that the NSA was using telephone metadata in ways that went beyond anything the court meant to authorize, and that the government had repeatedly misled the court when describing its core programs of telephone and Internet

surveillance. *See* Memorandum Opinion of the United States Foreign Intelligence Surveillance Court at 16 n.14 (Oct. 3, 2011), *available at* http://www.scribd.com/doc/162016974/fisa-court-opinion-with-exemptions/ ("FISC Opinion").

Against that historical backdrop, the NSA's accumulation of records of every telephone call poses a real and present danger to freedom of association and expression. As writers have warned for generations, people who are aware that every move they make is being recorded by a government bureaucracy – even an ostensibly benign one – inevitably censor themselves. This country was founded on the principle that government must allow the people the breathing room necessary to think and discuss and express their own ideas. The government's mass collection of data about private calls inhibits communication and self-expression and prevents the full flowering of creative thought, endangering self-governance and the freedoms we prize.

### **ARGUMENT**

#### I. THE PEN DECLARATION ON DIGITAL FREEDOM

Since its founding, PEN (like International PEN) has actively campaigned to counter the inhibiting effects that government actions, such as surveillance, can have upon free expression.

The PEN International Charter, ratified in 1948, states:

PEN stands for the principle of unhampered transmission of thought within each nation and between all nations, and members pledge themselves to oppose any form of suppression of freedom of expression in the country and community to which they belong, as well as throughout the world wherever this is possible.

PEN Charter ¶ 4, available at http://www.pen-international.org/pen-charter/.

Over the past several years, PEN has become increasingly concerned by the dramatic expansion of government surveillance in the digital age. PEN's members have recognized that "as digital media have expanded the ability of individuals to disseminate information, opinions, and ideas, they have also increased the number of individuals who are vulnerable to persecution

for their writings, and they have provided governments and private entities new means to access and monitor individual information and expression." In September 2012, at the PEN International Congress in Gyeongju, Korea, the Assembly of Delegates – representing 20,000 writers – adopted the PEN Declaration on Digital Freedom (the "PEN Declaration"). One of the four principles enshrined in the PEN Declaration directly addresses government surveillance:

3. All persons have the right to be free from government surveillance of digital media.

PEN Declaration, *available at* http://www.pen-international.org/pen-declaration-on-digital-freedom/declaration-on-digital-freedom-english/.<sup>2</sup>

The PEN Declaration explains why freedom from government surveillance of our electronic communications is crucial:

a. Surveillance, whether or not known by the specific intended target, chills speech by establishing the potential for persecution and the fear of reprisals. When known, surveillance fosters a climate of self-censorship that further harms free expression.

The Declaration then sets out the implications of this principle for governments around the world:

- b. As a general rule, governments should not seek to access digital communications between or among private individuals, nor should they monitor individual use of digital media, track the movements of individuals through digital media, alter the expression of individuals, or generally surveil individuals.
- c. When governments do conduct surveillance in exceptional circumstances and in connection with legitimate law enforcement or national security investigations any surveillance of individuals and monitoring of communications via digital media must meet international

<sup>&</sup>lt;sup>1</sup> See Declaration on Digital Freedom: FAQs, http://www.pen-international.org/pen-declaration-on-digital-freedom/declaration-on-digital-freedom-faqs/ ("FAQ").

<sup>&</sup>lt;sup>2</sup> The four principles are based, in part, on the UN Guiding Principles on Business and Human Rights, the UN Human Rights Committee General Comment No. 34, the Silicon Valley Standard, and the Global Network Initiative Principles. *See* FAQ.

due process laws and standards that apply to lawful searches, such as obtaining a warrant by a court order.

- d. Full freedom of expression entails a right to privacy; all existing international laws and standards of privacy apply to digital media, and new laws and standards and protections may be required.
- e. Government gathering and retention of data and other information generated by digital media, including data mining, should meet international laws and standards of privacy, such as requirements that the data retention be time-limited, proportionate, and provide effective notice to persons affected.

### PEN Declaration ¶ 3.

PEN submits this brief to amplify these principles in light of the mass collection of telephone data by the government. The NSA's sweeping data collection violates every one of them.

# II. THE IMPACT OF MASS GOVERNMENT SURVEILLANCE ON THE CRITICAL ZONE OF PRIVACY NEEDED FOR FREE EXPRESSION

To make original contributions to public discourse, writers must be confident that they are protected by a zone of privacy. The Constitution protects that zone of privacy. As the FISC explained, "[a] person's 'papers' are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter, telephone or email, a person's private communications are akin to personal papers." FISC Opinion at 74-75. President Lyndon Johnson declared that "[e]very man should know that his conversations, his correspondence, and his personal life are private." *Remarks at the Swearing in of Ramsey Clark as Attorney General* (March 10, 1967), http://www.presidency.ucsb.edu/ws/?pid=28123/. The freedom to communicate with whomever one chooses, away from the prying eyes of the state, is an essential condition for creativity and serious writing, and especially for the expression of dissent, through fiction and non-fiction alike.

More than eighty years ago, Justice Brandeis eloquently explained the connection between freedom from government intrusion and freedom of thought and expression:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Our Fourth Amendment rights to freedom from intrusion are thus bound closely to our rights under the First Amendment to freedom of association and freedom of expression. See, e.g., United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297, 314 (1972) ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."). Justice Sotomayor recently echoed these concerns when she observed that "[a]wareness that the Government may be watching chills associational and expressive freedoms." United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

As the PEN Declaration explains, government surveillance impairs free expression in two ways. First, "[s]urveillance, whether or not known by the specific intended target, chills speech by establishing the potential for persecution and the fear of reprisals." PEN Declaration ¶ 3.a. Second, "[w]hen known, surveillance fosters a climate of self-censorship that further harms free expression." *Id.* Philosopher Kwame Anthony Appiah, a former president of PEN, has illustrated the ways the possibility of surveillance impedes the free exchange that is necessary for the development of ideas:

Jeremy Bentham, the great nineteenth century British moral philosopher, was the first modern intellectual to argue in English that the treatment of gay people under the law – which made sodomy a capital crime – was

wrong. But he knew that if he revealed his opinion he would be in danger. Imagine if he had thought that he could not even explore the idea in his private writings, in correspondence with his friends. Yet that would have been exactly his situation if he lived today and used his laptop and his email.

Great moral advances begin often as radical ideas, ideas that would lead those who have them to be subjected to obloquy or even to violence. Serious thinking is done by writing and by exchanges of ideas with others. In a society that lived through the abuses of state power against Dr. Martin Luther King Jr. we cannot think that we will only be endangered if we are in the wrong. I have sometimes thought, myself, as I reflected on issues about the morality of terrorism and our responses to it, that I must censor myself in my most private writings because I cannot be sure that my writings will not be spied upon, misconstrued, used against me.

PEN American Center, *Two Views on How Surveillance Harms Writers* (Sept. 3, 2013), http://www.pen.org/blog/two-views-how-surveillance-harms-writers. The harm of self-censorship is real, though it may be difficult to discern and impossible to quantify. There is no database of thoughts that have not been shared or ideas that have not been exchanged.

### A. The History of Abuses of Surveillance

For writers, the dangers of government data-collection are far from imaginary.

Throughout the twentieth century, the FBI maintained active surveillance and investigation files on more than 150 writers, including many of our most celebrated authors, playwrights, and poets, such as James Baldwin, Truman Capote, Willa Cather, John Cheever, T.S. Eliot, William Faulkner, F. Scott Fitzgerald, Dashiell Hammett, Lillian Hellman, Ernest Hemingway, Sinclair Lewis, Jack London, Henry Miller, Eugene O'Neill, Dorothy Parker, Carl Sandburg, Gertrude Stein, John Steinbeck, James Thurber, Thornton Wilder, Tennessee Williams, Thomas Wolfe, and Richard Wright. *See* Natalie Robins, *Alien Ink* (1992). As PEN member Robins concluded, although this practice was often the result of a combination of "paranoia," "conspiracy," "monumental bureaucratic overkill" and agents "simply doing their job," "one thing is certain: most of the writers were watched because of what they thought." *Id.* at 17.

Throughout history, writers, artists, and public intellectuals have been particularly susceptible to intrusive surveillance and scrutiny, especially during times of heightened national tension. In the United States during the McCarthy era, for example, writers and artists suspected of having Communist leanings were interrogated by Congress and the FBI and blacklisted if they did not inform on their colleagues. Writers like Walter Bernstein were visited frequently by the FBI, often once or twice a month for years. Their neighbors were asked about their visitors. Their garbage was examined. They had to mask their identities to find work. *See* Larry Siems, *A Blacklisted Screenwriter on American Surveillance*, http://www.pen.org/blacklisted-screenwriter-american-surveillance (Aug. 30, 2013) ("Bernstein Interview"); *see also generally* Victor Navasky, *Naming Names* (1980).

The Foreign Intelligence Surveillance Court that issued the Order at issue in this case was itself established because law enforcement and intelligence agencies have been found time and again to have abused their surveillance powers in such ways and to have misused information obtained for otherwise lawful purposes. Congress created the FISC to act as a safeguard, in response to reports issued by the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee"), a bi-partisan group of lawmakers established in 1975 "in the wake of widespread abuses of authority by intelligence agencies." *See generally* Brief of Former Church Committee Members and Staff as *Amici Curiae* Supporting Respondents and Affirmance at 4, *Clapper v. Amnesty Int'l*, 133 S.Ct. 1138 (2013) (No. 11-1025). The Church Committee's reports detailed how "intelligence excesses, at home and abroad [were] found in every [presidential] administration" and described the particularly "notorious example[]" of how the FBI under J. Edgar Hoover "targeted Dr. Martin Luther King, Jr., in an effort to 'neutralize' him as a civil rights leader." *Id.* at 9-13.

The Church Committee recognized that the NSA in particular had "potential to violate the privacy of American citizens [that was] unmatched by any other intelligence agency." Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755, at 202 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755\_II.pdf ("Book II"). Senator Frank Church, the chair of the Committee, observed in 1975,

[The National Security Agency's] capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide.

Robert O'Harrow, *No Place to Hide* 10 (2006). The Committee found the record of NSA so troubling that, as James Bamford recounts, its draft report rejected the "NSA's appeal to the Congress and the public that they simply trust us" as "totally unjustified when viewed in the light of the Agency's long record of privacy violations." *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization* 387 (1982).

The NSA's ability – and tendency – to engage in mass warrantless surveillance of innocent Americans has only grown since then. *See, e.g., id.*; James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* (2008). Today, as many reports have revealed, the NSA is engaged in surveillance on a scale and to a degree previously unimagined, and the NSA has evaded legal safeguards established to protect privacy. In the 2011 decision mentioned above, the FISC found that the NSA had misled the court on multiple previous occasions as to the nature and scope of the information it had sought to collect. The court found that the NSA had been collecting information for several years knowing that its authorization was based on a false understanding by the court, and that was "the third instance in less than three years in which the government has disclosed a substantial misrepresentation

regarding the scope of a major collection program." FISC Opinion at 16 n.14. In one instance, the court determined that its authorization of the "bulk acquisition of telephone call detail records" for more than three years had been "premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception . . . buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." *Id*.

Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively."

Id.

In other words, J. Edgar Hoover may no longer be using FBI surveillance to harass political enemies, but the NSA has not been able to resist the temptation to make unlawful use of the information it has collected. Quite recently, it has "systematically" ignored legal safeguards and mined its massive stores of information in ways that overstepped legal bounds, and it has even misled the court that was established to prevent such abuses. In light of the history and the abuses that continue today, writers have every reason to worry about the government's voracious collection of so much sensitive information.

### B. Self-Censorship, Communication, and Creativity

The very collection of the information impairs freedom, even when writers are not directly intimidated or suppressed, and even if the information is never used. As the PEN Declaration states, "[f]ull freedom of expression entails a right to privacy." PEN Declaration ¶ 3.d. The knowledge that so much information is being gathered and stored is enough to inhibit the free exploration and exchange of ideas. Writers have richly illuminated the ways mass

government surveillance inevitably influences people's minds and their interactions with one another. Philosophers, novelists, scholars, and others have analyzed the ways surveillance affects the ability to write and limits the ideas and information that become available to society at large.

# 1. Government Surveillance as a Curb on Creative Thought and Expression

Creativity requires breathing room to flourish fully, and we have benefitted as a people from the freedom our Constitution protects, but mass surveillance of private information is inimical to free thinking and productive exchange. In describing the creative process, poet and PEN member Adrienne Rich emphasized the importance of a sense of freedom to consider the unorthodox:

For a poem to coalesce, for a character or an action to take shape, there has to be an imaginative transformation of reality which is in no way passive. *And a certain freedom of mind is needed*... Moreover, if the imagination is to transcend and transform experience, it has to question, to challenge, to conceive of alternatives, perhaps to the very life you are living at that moment.

Adrienne Rich, Arts of the Possible 20-21 (1971) (emphasis added).

PEN member David Shipler has explained how the mere collection of information by the government necessarily creates dangers for thinkers and restricts the freedom of mind, just by endowing the government with the capacity to intimidate and suppress:

Privacy is like a poem, a painting, a piece of music. It is precious in itself. Government snooping destroys the inherent poetry of privacy, leaving in its absence the artless potential for oppression. At the least, if the collected information is merely filed away for safekeeping, a weapon is placed in the hands of the state. If it is utilized, acute consequences may damage personal lives. Even where government is benign and well-meaning – a novelty that neither James Madison nor Tom Paine imagined – the use of everyday information about someone's past to predict his behavior can lead to obtrusive mistakes known as "false positives" in the jargon. Worse, the power of surveillance tempts the executive branch to aim at political opponents or "others" who seem "unpatriotic." This is especially so when

courts and legislatures retreat and fail to check and balance, for the vacuum they leave will be filled by expanding executive authority.

David K. Shipler, *The Rights of the People: How Our Search for Safety Invades Our Liberties* 294-95 (2011).

Social scientists have confirmed that the awareness of surveillance reduces the variety of ideas people entertain and express:

[T]he experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines. But rough edges and sharp lines have intrinsic, archetypal value within our culture. Their philosophical differences aside, the coolly rational Enlightenment thinker, the unconventional Romantic dissenter, the skeptical pragmatist, and the iconoclastic postmodernist all share a deeprooted antipathy toward unreflective conformism. The condition of noprivacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.

Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1425-26 (2000) (citing psychological studies indicating that "lack of privacy makes people less inclined to experiment and less inclined to seek help").

Walter Bernstein, the screenwriter who survived blacklisting in the 1950s, recalls how the climate of fear constrained creativity, and he sees worryingly similar effects of the NSA's mass surveillance today:

Everybody was careful [in the era of blacklists]. It was not a time for risk-taking on the part of most people. In my area, in television, . . . [writers] stayed away from politics . . . [T]here was a general feeling of 'you don't stick your neck out.'

\* \* \*

I think it is reasonable to feel that [writers] are in some way under surveillance [today] even if it's not directly against them. . . . It's not a healthy atmosphere, certainly. It's not an atmosphere that helps create creativity or lets the mind run free. You're always in danger of self-censorship, of saying, 'no, I won't try this . . . or it'll alienate the government.'

Bernstein Interview. Government surveillance can thus destroy the sense of privacy that is essential to the freedom to create, even without any active harassment of writers. Especially given the long history of abuse, the mere knowledge that private information is being collected by the government restricts communications and suppresses expression that relies on the free exchange of thoughts.

### 2. Writers' Frameworks for Understanding the Dangers of Surveillance

Writers have often created fictional worlds more extreme than reality to warn the public of their concerns about the prying eyes of a powerful state and to underscore the critical importance of privacy to human creativity and freedom. Their works have illuminated the dangerous shift of power that surveillance brings about.

The author Julian Sanchez has observed that, when we discuss surveillance and privacy, "we speak a language borrowed from fiction." Julian Sanchez, *On Fiction and Surveillance*(Introduction to PEN World Voices Festival panel: "Life in the Panopticon: Thoughts on Freedom in an Era of Pervasive Surveillance") (May 14, 2012), *available at*http://www.pen.org/nonfiction/julian-sanchez-fiction-and-surveillance. The most common literary reference points for state surveillance are, of course, Big Brother and the Thought Police, from George Orwell's dystopian novel, *1984* (1949). *See, e.g.*, William O. Douglas, *Points of Rebellion* 29 (1969) ("Big Brother in the form of an increasingly powerful government and in an increasingly powerful private sector will pile the records high with reasons why privacy should give way to national security, to law and order, to efficiency of operation, to scientific advancement and the like."). By depicting a totalitarian society ruled by an all-knowing government, Orwell vividly illustrated the dangers posed by a powerful surveillance state.

Other writers have explored the power of surveillance alone, without the coercive government repression depicted by Orwell in 1984. For example, the title of the PEN World

Voices Festival panel discussion moderated by Julian Sanchez refers to another literary symbol of surveillance, the "Panopticon" – a design devised by the British philosopher Jeremy Bentham for a circular building for a prison or other institution, with a central observation tower to permit guards to observe inmates in their cells at all times without letting the inmates know whether they were being watched or not. Bentham called it "a new mode of obtaining power of mind over mind, in a quantity hitherto without example." Jeremy Bentham, *The Panopticon Writings* (Miran Bozovic, ed., 1995). The idea of the Panopticon aptly illustrates how the NSA's comprehensive collection of telephone call data affects our society, even if we never learn whether one particular record or another is actually examined.

The French philosopher Michel Foucault used the concept of the Panopticon as a metaphor to analyze modern structures of power, in his work *Discipline and Punish* (1975). (The original French title is striking here: *Surveiller et Punir*.) Like Bentham, Foucault recognized that actual surveillance is not necessary to achieve the desired effect of control. The mere knowledge that, at any given moment, one *could* be watched is sufficient: "Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power." *Id.* at 201. Foucault concluded that individuals subject to the constant possibility of surveillance – whether in a building or in society at large – come to internalize "the constraints of power," censoring themselves and permitting whoever is in authority to exert more and more control with less and less physical force:

By this very fact, the external power may throw off its physical weight; it tends to the non-corporal; and, the more it approaches this limit, the more constant, profound and permanent are its effects: it is a perpetual victory that avoids any physical confrontation and which is always decided in advance.

*Id.* at 202-03.

The NSA's vast data collection amounts to panoptic government surveillance. We know that information about every telephone call can be seen, but we do not know for sure whether anyone is looking at information about us. Foucault underlines the unavoidable effect that the very knowledge of surveillance has on human beings. People come to behave as if they are actually being watched, without knowing whether they are or not, and thoughts that could be viewed as disruptive are avoided or suppressed. Security expert Bruce Schneier has elaborated on this concern:

[I]f we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that – either now or in the uncertain future – patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts.

Bruce Schneier, *The Eternal Value of Privacy*, Wired (May 18, 2006).

Another literary analogue for government surveillance today is found in the work of Franz Kafka. *See* Daniel J. Solove, *The Digital Person* 27-55 (2004). In Kafka's *The Trial* (1925), an individual, Joseph K., is suddenly informed that he is under arrest without any explanation. He discovers that "[a] vast bureaucratic court has apparently scrutinized his life and assembled a dossier on him. The Court is clandestine and mysterious, and court records are 'inaccessible to the accused.'" Solove at 36. He engages in a maddening and largely fruitless quest to understand the charges against him and who brought them.

The Trial captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to Joseph K.; decisions are made based on this data, and Joseph K. has no say, no knowledge, and no ability fight back. He is completely at the mercy of the bureaucratic process.

Solove at 38.

As Professor Solove explains, the "Kafka-esque" danger of surveillance data is not necessarily that government agencies will be "led by corrupt and abusive leaders," but rather that government collection of information

shift[s] power toward a bureaucratic machinery that is poorly regulated and susceptible to abuse. This shift has profound social effects because it alters the balance of power between the government and the people, exposing individuals to a series of harms, increasing their vulnerability and decreasing the degree of power they exercise over their lives.

*Id.* at 178. History has shown that the NSA is poorly regulated and vulnerable to abuse (*see* II. A., above), but even if the information the NSA gathers were never misused, the mere possibility of being persecuted or discriminated against for exploring ideas that may be deemed dangerous – or for communicating with people who are deemed dangerous – raises the stakes for writers and hampers the free thought that is so necessary to creative expression.

#### III. THE HIGH SENSITIVITY OF TELEPHONE METADATA

At first blush, the surveillance at issue in this litigation may seem relatively benign, particularly when compared to practices that may seem more intrusive, such as tapping phones or surreptitiously reading emails. Under the Order being challenged, the government is not authorized to listen in on phone calls – it is authorized to collect only the "telephony metadata" for the calls. But the metadata, especially when aggregated, reveal highly sensitive information, and the information is particularly sensitive for writers.

## A. Telephone Metadata's Capacity to Reveal Associations and Private Information

As privacy and security experts across the board agree, telephone metadata can reveal extremely private facts about a person and provide a map of associations across the country and around the world.

Whom someone is talking to may be just as sensitive as what's being said. Calls to doctors or health-care providers can suggest certain medical

conditions. Calls to businesses say something about a person's interests and lifestyle. Calls to friends reveal associations, potentially pointing to someone's political, religious or philosophical beliefs.

Even when individual calls are innocuous, a detailed phone record can present a telling portrait of the person associated with a telephone number. Collect millions of those records, and there's the potential to trace the entire country's social and professional connections.

Daniel J. Solove, *Five Myths About Privacy*, Washington Post (June 13, 2013). "Even a single call to an abortion clinic or a whistle-blower hotline can expose highly personal information." James Debelak, *Why the NSA's Gathering of Metadata Matters*, Seattle Times (June 15, 2013), *available at* http://seattletimes.com/html/opinion/2021192466\_jameladebelakopedxml.html.

Privacy and security expert Susan Landau has explained some of the surprising revelations that can result from examining telephone metadata:

[I]n the world of business, a pattern of phone calls from key executives can reveal impending corporate takeovers. . . . And information from cell phone towers can reveal the caller's location. . . . [It] can also reveal sensitive political information, showing, for instance, if opposition leaders are meeting, who is involved, where they gather, and for how long. Such data can reveal, too, who is romantically involved with whom, by tracking the locations of cell phones at night.

Jane Mayer, *Verizon and the N.S.A.: The Problem With Metadata*, New Yorker (June 6, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html.

In many ways, telephone metadata can be likened to the GPS tracking data that law enforcement officers have sought to use. As the D.C. Circuit explained, in a decision that was ultimately affirmed by the Supreme Court, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." *United States v.* 

Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012). Justice Sotomayor, concurring in the affirmance, noted that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future." United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring). Justice Sotomayor also questioned more broadly "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Id. at 957. She explained:

This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the email addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Id.

Like GPS data and Internet tracking information, a list of the calls people have made has the potential to "expose[] something deeper":

Metadata is our context. And that can reveal far more about us – both individually and as groups – than the words we speak. Context yields insights into who we are and the implicit, hidden relationships between us. A complete set of all the calling records for an entire country is therefore a record not just of how the phone is used, but, coupled with powerful software, of our importance to each other, our interests, values, and the various roles we play.

Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, Wired (June 19, 2013), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/. Raw telephone metadata can easily be analyzed by computer software for retroactive surveillance.

Under the Order here, every telephone customer, like Joseph K. in *The Trial*, knows there is a detailed dossier containing highly personal information about him in the hands of a vast, secretive government bureaucracy. Although it may be likely that no one has bothered to assemble that dossier for a given individual, the potential is always present. A human guard may or may not be watching from the Panopticon's tower at a particular time, but the government's comprehensive collection of metadata and its ability to piece together information about particular people make us subject to the panoptic effect more than ever before. PEN is concerned that, if such surveillance becomes the norm, our tolerance for intrusions will naturally rise, and the zone of privacy will shrink further as people become accustomed to knowing that their communications are monitored. Ideas will not be aired and tested. Our discussions will have fewer sparks. Culture will contract, and the conditions that allow democracy to thrive will erode.

#### B. The Particular Risks for Writers and their Contacts

The government's collection of this type of information is especially damaging to writers and freedom of expression. Writers of non-fiction often depend on confidential sources to inform their work. Not only whistleblowers, but anyone who fears physical harm or economic retribution may wish to remain anonymous. When it was discovered recently that the Department of Justice had sought calling information for the phones of several employees of the Associated Press (the "AP"), Gary Pruitt, President and CEO of the AP, wrote to Attorney General Holder stating, "These records potentially reveal communications with confidential sources across all of the newsgathering activities undertaken by the AP during a two-month

period, provide a road map to AP's newsgathering operations and disclose information about AP's activities and operations that the government has no conceivable right to know." Letter from Gary Pruitt to Attorney General Eric Holder (May 13, 2013), *available at* http://www.ap.org/Images/Letter-to-Eric-Holder\_tcm28-12896.pdf. From victims of domestic abuse to witnesses of corporate crime, sources are far less likely to talk to authors if data on their phone conversations is being collected and stored.

The prospect that telephone metadata can reveal the entire web of a writer's associations and interactions – and the contacts of all the writer's contacts, and their contacts – will inevitably limit and deter valuable interactions. Writers in the United States who support human rights or who communicate with human rights activists, for instance, are acutely aware of the dangers that comprehensive telephone metadata may create. The government's records of calling activity may permit reprisals or sanctions to be visited on writers, or on people with whom they speak, or on those people's families and friends, here and in other countries where they may be more vulnerable. Even more broadly, because writers develop ideas through conversations, including conversations with radicals, dissidents, pariahs, victims of violence, or even outlaws, chilling their exchanges will impoverish thought.

### IV. BALANCING FREEDOM AND SECURITY

PEN does not discount the rationale for the type of surveillance the Order permits: that it makes law enforcement and intelligence gathering easier and more effective, and that the government must be vigilant to act against threats to the lives and property of Americans. But, throughout our history, we have been faced with the temptation to sacrifice liberty for the sake of security. As far back as our nation's inception, Alexander Hamilton warned that "[t]he continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their

civil and political rights. To be more safe, they at length become willing to run the risk of being less free." Federalist No. 8 (Alexander Hamilton). In our haste to protect ourselves, our nation must not destroy what has made it unique.

Precisely because it is legitimized via fear one can claim that "the war against terror" is a greater danger to democracy than terrorism itself. . . . We can perhaps say, along with the philosopher Giorgio Agamben, that we live today in a permanent state of emergency, where the reference to serious dangers almost works like a trump card – and the card trumps recognized democratic rights.

Lars Svendsen, A Philosophy of Fear 122-23 (2008).

Even seemingly small sacrifices of privacy may gradually but fundamentally alter the balance between liberty and security over time. As Justice Douglas warned,

As nightfall does not come all at once, neither does oppression. In both instances, there is a twilight when everything remains seemingly unchanged. And it is in such twilight that we all must be most aware of change in the air – however slight – lest we become unwitting victims of the darkness.

Melvin I. Urofsky and Philip E. Urofsky eds., *Selections from the Private Papers of Justice William O. Douglas* 162 (1987). Writing in 1966, Justice Douglas foresaw the dangers that would grow as the capabilities of surveillance technology advanced:

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. . . . These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen – a society in which government may intrude into the secret regions of man's life at will.

Osborn v. United States, 385 U.S. 323, 341, 343 (1966) (Douglas, J., dissenting).

Even where sacrifices of liberty are sought for legitimate ends, we should not lose sight of the fundamental values at stake. The words of Justice Brandeis remind us:

Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Olmstead, 277 U.S. at 479 (Brandeis, J., dissenting).

Recent reports have suggested that the NSA's surveillance efforts go far beyond the telephone metadata at issue in this case. But the metadata collection program alone significantly intrudes into the privacy of ordinary citizens, with grave consequences for freedom of expression and association as well as privacy. For writers, the effects are not only practical and direct – because it is more difficult to communicate privately – but also subtle and indirect – because the sense of privacy essential to free expression is so compromised. Our pursuit of security should not blind us to the costs of sacrificing the liberty we seek to protect.

### **CONCLUSION**

For the foregoing reasons, *Amicus Curiae* PEN believes the plaintiffs' motion for a preliminary injunction should be granted and the defendants' motion to dismiss denied.

Dated: New York, New York September 4, 2013

Respectfully submitted,

DAVIS WRIGHT TREMAINE LLP

By: /s/ Edward J. Davis

Edward J. Davis (ED 1266)

Linda Steinman (LS 5906)

Eric Feder (EF 8016)

1633 Broadway, 27<sup>th</sup> Floor New York, New York 10019 (212) 489-8230

Attorneys for Amicus Curiae PEN American Center