A EUROPEAN APPROACH TO THE UNITED STATES CONSTITUTIONAL PRIVACY

Wm. Bruce Wray

I. INTRODUCTION

An intrinsic concept to a right to privacy was expressed in America at least as early as 1890, when Samuel Warren and Louis Brandeis wrote *The Right to Privacy*.¹ In that article, they detail the evolution of the common-law doctrines from tangible property to intangible rights, based upon conditions "necessary or helpful to worldly prosperity."² Dealing specifically with a right of publication, Warren and Brandeis note that “[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.”³ In like form, the current change to political, societal, economic, and technological developments necessitate evolution of the constitutional right of privacy in the United States. However, there is no express right to privacy in the United States, and indeed, neither the Constitution nor the Bill of Rights included the terms “privacy” at all.⁴ Despite this, the Supreme Court has held an inherent right to privacy deriving from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.⁵

This article will discuss the recent revelations of the NSA’s Bulk Telephony Metadata Program, as well as the Prism Program, and the litigation that immediately preceded and followed as a result of those revelations.⁶ The article will then identify current United States Supreme Court precedent related to the Fourth Amendment prohibition against “unreasonable search and seizures.”⁷ The article will next contrast this approach with the expansive right to privacy constitutionally protected through various courts in Europe.⁸ Finally, this article will review the use and influence of foreign and international law on American constitutional issues and suggest the

² Warren & Brandeis, supra note 1, at 197.
³ Warren & Brandeis, supra note 1, at 193.
⁵ See generally U.S. CONST., supra note 4: Slemmons Stratford & Stratford, supra note 4, at 17 (stating, despite the absence of the term “privacy” from the U.S. Constitution, the Supreme Court has found various privacy interests deriving from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments).
⁶ See infra note 10-41 and accompanying text.
⁷ See infra note 42-61 and accompanying text.
⁸ See infra note 62-72 and accompanying text.
United States Supreme Court adapt the privacy standards, and the tests utilized to assess them, currently provided in European nations.\(^9\)

**II. BACKGROUND**

On June 5, 2013, the Guardian newspaper published a copy of a court order issued by the Foreign Intelligence Surveillance Court (FISC) that directed Verizon Wireless to provide ongoing daily access to the National Security Agency (NSA) for all telephone call information, known as metadata, both foreign and domestic.\(^10\) This publication was the first among many revelations about the widespread collection, retention, and mining of data within America, affecting data from both domestic and foreign communications.\(^11\) Beyond access to telephony metadata, the revelations also include details of the NSA’s Prism program, with claimed direct access to central Internet corporations, their servers, and the content they provide or receive from their users.\(^12\) These revelations led to several lawsuits alleging infringement of constitutionally protected interests, specifically the Fourth Amendment’s protection against “unreasonable search and seizure.”\(^13\)

In *Clapper v. Amnesty International USA*\(^14\), decided prior to the major revelations about domestic data collection, the United States Supreme Court held petitioner Amnesty International lacked the requisite Article III standing to bring suit because the alleged injury in fact was tied to an objectively reasonable likelihood that their communications would be acquired under 50 U.S.C. § 1881(a) at some point in the future, rather than a present injury.\(^15\) In *Clapper*, Amnesty International USA and others sued the Director of National Intelligence, the Director of the National Security Agency and Chief of the Central Security Service, and the Attorney General of the United States, presenting a facial challenge to the newly added 50

---

\(^9\) See infra note 73-119 and accompanying text.


\(^13\) See Klayman v. Obama, CV 13-0881 (RJL), 2013 WL 6598728, at *1, *1 n.2 (D.D.C. Dec. 16, 2013) (deciding a consolidated case and referencing additional cases across the country related to NSA surveillance); see also *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013) (predating the recent revelations about the NSA’s domestic data collection programs).

\(^14\) 133 S.Ct. 1138 (2013).

\(^15\) *Clapper*, 133 S.Ct. at 1143.
U.S.C. § 1881(a), a new provision within the Foreign Intelligence Surveillance Act that authorized surveillance targeting non-United States persons. The United States District Court for the Southern District of New York granted the Government’s motion for summary judgment, reasoning that the plaintiffs’ abstract fear that they would be under surveillance failed to satisfy Article III standing. After that opinion was reversed at the United States Court of Appeals for the Second Circuit, the United States Supreme Court granted certiorari to review the issue of Article III standing. The Court affirmed the District Court’s ruling that plaintiffs lacked Article III standing, finding that plaintiffs’ “theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be ‘certainly impending.’” The Court, finding the plaintiffs lacked Article III standing, never addressed the constitutionality of surveillance authorized under 50 U.S.C. § 1881(a).

On June 6, 2013, one day after the Guardian’s articles release, the first of two suits was filed that resulted in a preliminary injunction granted in Klayman v. Obama. In Klayman, Klayman and four other plaintiffs brought two suits against both federal defendants, including agencies and individual executive officials, and private defendants, including telecommunications and Internet firms and their executives, alleging statutory and constitutional violations. The United States District Court for the District of Columbia held in Klayman that plaintiffs had Article III standing, as Verizon customers, and had shown a likelihood of success on the merits that the NSA’s Bulk Telephony Metadata Program constituted a search under the Fourth Amendment, warranting a preliminary injunction. In reaching the constitutional issue, the District Court found that Congress had not satisfied the heightened showing to preclude judicial review of Klayman’s constitutional claim, as required under Webster v. Doe, because it had not expressly barred judicial review of third party claims regarding 50 U.S.C. § 1861. The

---

17 McConnell, 646 F. Supp. 2d at 645.
18 Clapper, 133 S.Ct. at 1146 (“because of the importance of the issue and the novel view of standing adopted by the Court of Appeals, we grant certiorari . . . and we now reverse”).
19 Id. at 1143.
20 Id. (“Respondents seek a declaration that § 1881a is unconstitutional, as well as an injunction against § 1881a-authorized surveillance. The question before us is whether respondents have Article III standing to seek this prospective relief”).
21 See Klayman, 2013 WL 6598728 at *1; see also Greenwald, supra note 10 (revealing NSA bulk surveillance); see also Greenwald & MacAskill, supra note 12 (outlining timeline of revelations for NSA bulk surveillance).
23 Id. at *2, *14-15.
25 Id. at *13-14.
District Court, however, found that Klayman's statutory claims under the Administrative Procedure Act (APA) were bared from judicial review by implied Congressional intent in establishing a detailed procedure for judicial review.\(^{26}\)

The District Court in *Klayman* distinguished the United States Supreme Court case of *Smith v. Maryland*\(^ {27}\), by finding that case's analysis related to installation and use of a pen register to track a single phone number inapplicable to the present case.\(^ {28}\) In contrast, the present case involved a longstanding relationship between the NSA and telecom companies, under the NSA's Bulk Telephony Metadata Program, to “produce to the NSA on a daily basis electronic copies of call detail records, or telephony metadata.”\(^ {29}\) The District Court relied upon the recent Supreme Court decision in *United States v. Jones*\(^ {30}\), which likewise distinguished *United States v. Knotts*,\(^ {31}\) a prior Supreme Court decision.\(^ {32}\) In *Jones*, the Supreme Court found that law enforcements use of a Global Position System (GPS) device placed on a vehicle to track its movements for nearly a month violated Jones's reasonable expectation of privacy.\(^ {33}\) The Court in *Jones* did this without disturbing the decision from *Knotts* that use of a tracking beeper, placed in a container delivered to Knotts and used to track that containers movements, did not constitute a search under the Fourth Amendment.\(^ {34}\) The district court then contrasted the *Smith* decision based on the twenty-first century technology that now allows these records to be stored and analyzed for years, technologies that are “cheap in comparison to conventional surveillance techniques and, by design, proceed[] surreptitiously” and without the ordinary constraints on “abusive law enforcement practices: limited police...resources and community hostility.”\(^ {35}\)

The district court in *Klayman* also concluded that the nature and quantity of information available from telephony metadata today far outstrips the limited information available to police when *Smith* was decided in 1979, based on the ubiquity of the phones and their expanded use by American citizens.\(^ {36}\) Cell phones today function as multipurpose devices, including providing maps and directions, text

\(^{26}\) Id. at *11-12; See also 50 U.S.C. § 1803 (designating the process by which district court and appellate court judges are assigned by the Chief Justice of the United States to the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Court of Review (FISCR), two new courts created by the Foreign Intelligence Surveillance Act (FISA)).

\(^{27}\) 442 U.S. 735 (1979).

\(^{28}\) *Klayman*, 2013 WL 6598728, at *18.

\(^{29}\) Id. at *18-19 (citing to the Government brief's description of the collection scheme).

\(^{30}\) 132 S.Ct. 945 (2012).


\(^{32}\) *Klayman*, 2013 WL 6598728, at *18-19.


\(^{34}\) Id. at 951-52 (distinguishing its decision from the court in *Knotts*, 460 U.S. at 276 (1983)).

\(^{35}\) *Klayman*, 2013 WL 6598728, at *20 (quoting Justice Sotomayor's concurrence in *Jones*, 132 S.Ct. at 956).

\(^{36}\) Id.
messaging, Internet access, and music players. The scope of information available to the government now reveals an “entire mosaic” about a person, that “reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,” and that provides “a vibrant and constantly updating picture of the person’s life.” Based upon this analysis and presentation of the facts, the District Court found the NSA’s Bulk Telephony Metadata Program constituted a search under the Fourth Amendment.

A. AMERICANS CONSTITUTIONAL PRIVACY DOCTRINES

Modern United States Supreme Court precedent related to Fourth Amendment incursions begins with the 1967 case of Katz v. United States, where the Court stated, “the Fourth Amendment protects people – and not simply ‘areas’ – against unreasonable search and seizures.” In Katz, the Court held that Katz’s reasonable expectations of privacy were violated when Federal Bureau of Investigation (FBI) agents placed a listening device on the exterior of a public telephone booth from which Katz had placed calls and discussed illegal wagering information between Los Angeles and Boston and Miami. Distinguishing prior cases tied to “constitutionally protected areas,” the Court noted that, “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” The Court declined to restrict Fourth Amendment protection to purely tangible items or technical trespasses under local property law, but found that the “Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied upon while using the telephone booth and thus constituted a ‘search and seizure’ with the meaning of the Fourth Amendment.”

The United States Supreme Court later limited this personal protection against information when that information was given to a third party, such as bank deposit records and telephone pen registries, finding the petitioner “takes the risk, in revealing his affairs to another, that the information will be conveyed by that

37 Id.
38 Id. at *21.
39 Id. at *21 (quoting Jones, 132 S.Ct. at 955 (Sotomayor, J., concurring)).
40 Id.
41 Id. at *22.
43 Katz, 389 U.S. at 353.
44 Id. at 359 (“Because the surveillance here failed to meet [the] condition of antecedent justification, and because it led to the petitioner’s conviction, the judgment must be reversed”).
45 Id. at 349 (discussing facts of Katz).
46 Id. at 351.
47 Id. at 353.
person to the Government.”\textsuperscript{50} In \textit{United States v. Miller}\textsuperscript{51}, the Court held that access by the Department of Alcohol, Tobacco, and Firearms (ATB) to bank records of accounts held by Miller\textsuperscript{52} did not constitute a violation of his Fourth Amendment rights.\textsuperscript{53} The Court reasoned that because “[a]ll of the documents obtained, including the financial statements and deposit slips, contain only information voluntarily conveyed to the bank and exposed to their employees in the ordinary course of business,” they lack an legitimate expectation of privacy.\textsuperscript{54}

Similarly, in \textit{Smith v. Maryland}\textsuperscript{55}, the United States Supreme Court held the installation, without a warrant, of a pen register against a suspect's phone number\textsuperscript{56} did not constitute a violation of his Fourth Amendment rights.\textsuperscript{57} In \textit{Smith}, the Court noted that the test identified in \textit{Katz} was “whether the person invoking its protection can claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’ that has been invaded by the government’s actions.”\textsuperscript{58} The Court in \textit{Smith} distinguished the listening device employed from \textit{Katz} because the pen registers do not acquire the contents of the communications, as they only disclose the telephone numbers that have been dialed—[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by the pen register.”\textsuperscript{59} Based on the limited information disclosed by a pen register, the Court then isolated the constitutional claim to be whether Smith had a “legitimate expectation of privacy” in the numbers he dialed.\textsuperscript{60} Ultimately, the Court relied upon \textit{Miller} in finding that Smith had assumed the risk that voluntarily conveying numerical information to the telephone company and exposing that information to their equipment, through the ordinary course of business, could result in its disclosure to the police.\textsuperscript{61}

\section*{B. \textbf{THE EUROPEAN APPROACH TO THE RIGHT TO PRIVACY}}

The right to privacy in Europe is based on a tacitly different approach.\textsuperscript{62} The Council of Europe, setup following the Second World War, outlined the European Convention for the Protection of Human Rights in 1950 that recognized the right to privacy as a fundamental

\begin{itemize}
  \item[50] \textit{Miller}, 425 U.S. at 443.
  \item[52] \textit{Miller}, 425 U.S. at 437-438 (detailing ATB access to bank records).
  \item[53] \textit{Id.} at 439-440 (holding “there is no intrusion into any area in which respondent had a protected Fourth Amendment interested.”).
  \item[54] \textit{Id.} at 442.
  \item[55] 442 U.S. 735 (1979).
  \item[56] \textit{Smith}, 442 U.S. at 737 (describing the actions taken by the police to collect this information).
  \item[57] \textit{Id.} at 745-746 (rendering the decision of the court).
  \item[58] \textit{Id.} at 740.
  \item[59] \textit{Id.} at 741 (quoting \textit{U.S. v. New York Tel. Co.}, 434 U.S. 159, 167 (1977)).
  \item[60] \textit{Id.} at 742.
  \item[61] \textit{Id.} at 744.
  \item[62] Slemmons Stratford & Stratford, \textit{supra} note 4, at 19.
\end{itemize}
human right. Specifically, Article 8 of the European Convention on Human Rights outlines the express right to respect for private and family life as:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Additionally, the European Data Directive, adopted in 1995, and the General Data Protection Regulation, proposed in 2012 to supersede the Data Directive, both embody the principle that privacy is a fundamental human right. The European Court of Human Rights (ECHR) has applied this right to privacy to both public and private actors, and considers “any information about a person, no matter how banal or how widely known,” to be private so long as it is “systematically stored and collected.” This right to privacy extends to public behavior, “if it is recorded and disseminated in a manner that could not have reasonably been anticipated by the individual concerned.” In assessing an interference with this right to privacy, the ECHR has defined a three-fold test for legality:

That three-fold test is:

First, if the processing is done by a public authority or for a public purpose, it must be authorized by a law,

---

63 Slemmons Stratford & Stratford, supra note 4, at 19.
67 Id.
68 Id.
accessible to the public, with precise enough provisions to curb arbitrary government action and to put citizens on notice of possible incursions into their private sphere. Secondly, the purpose of the interference must be legitimate. Namely, the purpose must be related to one of the categories listed in Article 8. It must be “in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Thirdly, the interference with private life must be proportional. The proportionality inquiry generally consists of three distinct steps. Is there evidence the government action can achieve the stated purpose? Is the government action necessary for accomplishing the stated purpose or would alternative means accomplish the same purpose with a lesser burden on privacy rights? And even though there might be no alternative means for accomplishing the same purpose, is the burden on the right to privacy nonetheless intolerable, requiring the law to be withdrawn?

Governmental abuses of Europeans’ personal records experienced during the Second World War may in part explain the complacency of American law, as compared with European law, when faced with “massive governmental database on personal records.” During the Second World War, Nazi forces attempted to utilize governmental files from census data to conscript specific citizens for the war effort, “underpin[ning] the law of information privacy in Europe today.” Preventing these abuses and the dangers of large-scale governmental collection of personal information is the objective of European privacy law.

C. FOREIGN AND INTERNATIONAL INFLUENCES ON AMERICAN CONSTITUTIONAL UNDERSTANDING

American courts long have utilized foreign and international law “as relevant but nonbinding sources,” dating back to early decision on the Eighth Amendment “cruel and unusual” punishments. The case of Wilkerson v. Utah in 1878 specifically considered death penalty practices “prevailing in other countries,” in

69 Id.
71 Id.
72 Id.
74 99 U.S. 130 (1878).
finding death by shooting acceptable under the Eighth Amendment.\textsuperscript{75} The Supreme Court continued this practice of referring to foreign law when assessing challenges involving “cruel and unusual” punishment.\textsuperscript{76} In 2005, the Supreme Court decision of \textit{Roper v. Simmons}\textsuperscript{77} referenced “the overwhelming weight of international opinion against the juvenile death penalty,” noting that while not binding, it does provide “respected and significant confirmation for [the Court’s] determination.”\textsuperscript{78} Further, the Court stated, “[i]t does not lessen fidelity to the Constitution or pride in its origins to acknowledge that the express affirmation of certain fundamental rights by other nations and peoples underscores the centrality of those same rights within our own heritage of freedom.”\textsuperscript{79}

Beyond death penalty cases, a number of opinions from Supreme Court Justices have referred to the United Nations Charter and the Universal Declaration of Human Rights.\textsuperscript{80} In \textit{Zemel v. Rusk}\textsuperscript{81}, the Court analyzed the requirements of due process implicit in the Secretary of State denying Zemel a passport to authorize travel to Cuba.\textsuperscript{82} In that decision, the Court noted the 81st Congress’ Senate Document quoting the Universal Declaration of Human Rights, Article 13, which covers travel with the country and a right to leave and return to the country.\textsuperscript{83} Likewise, in \textit{Kennedy v. Mendoza-Martinez}\textsuperscript{84}, the Court discussed the “drastic consequences of statelessness” and cited to numerous international sources, including the Universal Declaration of Human Rights, Article 15, which affirms the right of every individual to retain a nationality.\textsuperscript{85}

\section*{III. ARGUMENT}

The United States Court of Appeals for the District of Columbia, and ultimately the United States Supreme Court, should affirm the preliminary injunction granted in \textit{Klayman v. Obama}, reaffirming a constitutional right of privacy in light of the evolving role of technology in American life and the systematic monitoring by

\begin{flushleft}
\textsuperscript{75} Wilkerson, 99 U.S. at 134-135 (citing to “Simmons, Courts-Martial (5th ed.), sect. 645: Griffith, Military Law, 86;” additionally, considering Blackstone’s and Archibold’s Treatise based on English law).
\textsuperscript{76} See Jackson, supra note 73, at 109-110 n.4, n.7 (outlining additional decisions listing both positive and negative references to foreign and international law).
\textsuperscript{77} 543 U.S. 551 (2005).
\textsuperscript{78} \textit{Roper}, 543 U.S. at 578.
\textsuperscript{79} \textit{Id}.
\textsuperscript{81} 381 U.S. 1 (1965).
\textsuperscript{82} \textit{Zemel}, 381 U.S. at 14.
\textsuperscript{84} 372 U.S. 144 (1963).
\textsuperscript{85} Mendoza-Martinez, 372 U.S. at 162 n.16.
\end{flushleft}
the United States government of its own citizens, and should adapt the three-fold test from the European Court of Human Rights when evaluation governmental information collection.

A. CURRENT CONSTITUTIONAL PRIVACY AS APPLIED TO KLAYMAN

At present, the United States Supreme Court precedent defines any expectation of privacy that is protected by Constitutional constraints. In *Katz v. United States*, the Court stated, “the Fourth Amendment protects people – and not simply ‘areas’ – against unreasonable search and seizures.” The Court has limited this personal protection against information given to a third party, such as bank deposit records and telephone pen registries, finding the petitioner “takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.” In *Clapper v. Amnesty International USA*, decided prior to the revelations of NSA data collection, the Court was faced with surveillance activities under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1881(a), but declined to reach the constitutionality issue by finding the respondents lacked Article III standing based on the mere possibility of future injury.

The United States District Court for the District of Colombia in *Klayman v. Obama*, addressing the lack of concrete and particular injury from *Clapper*, found the *Klayman* plaintiffs had Article III standing because “as Verizon customers, [the plaintiffs] telephony metadata has been collected for the last several years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention.” In ruling the District Court had jurisdiction to hear the constitutional claims, despite having no authority to review the APA claims, the District Court stated that Congress “may not hang a cloak of secrecy over the Constitution,” despite Congressional intent “for the conduct to remain secret by operation of the design of its statutory scheme.” Thereafter, the District Court next considered the requested preliminary injunction

---

86 See U.S. CONST., supra note 4.; Sleimonials Stratford & Stratford, supra note 4, at 17 (stating the term “privacy” is not in the U.S. Constitution but that the Supreme Court has found various privacy interests deriving from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments).


88 *Katz*, 389 U.S. at 353.

89 *Miller*, 425 U.S. at 437.

90 *Smith*, 442 U.S. at 735.

91 See *Miller*, 425 U.S. at 443.


93 The revelations of widespread data collection of domestic and foreign telephony metadata occurred on June 6, 2013, whereas the *Clapper* decision was rendered on February 26, 2013. Compare Greenwald, supra note 10, with *Clapper v. Amnesty International USA*, 133 U.S. 1138 at 1143 (2013).

94 *Clapper*, 133 S.Ct. at 1143.


barring records collection under 50 U.S.C. § 1861. The District Court in *Klayman* analogized that “the almost-Orwellian technology” used by the Government to store and analyze phone metadata for every telephone user in the United States was “unlike anything that could have been conceived in 1979.”

Justice Sotomayor’s concurrence in *United States v. Jones* was heavily relied upon by the District Court in *Klayman*, yet Justice Sotomayor went further, stating:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may “alter the relationship between citizen and government in a way that is inimical to democratic society.”

Justice Sotomayor’s concurrence further suggests that the Court may need to reconsider the premise that “an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,” finding that approach ill-suited in the digital age. Justice Marshall, dissenting thirty-four years ago in *Smith v. Maryland*, stated that “[p]rivacy is not a discrete commodity, possessed absolutely or not at all.” Noting that “unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance,” Justice Marshall would instead apply the reasonable expectation of privacy from *Katz* based on the risks an individual “should be forced to assume in a free and open society.”

### B. The European Approach to the Right to Privacy

The approach outlined by Justice Marshall, and echoed by Justice Sotomayor, resonate with the European approach to the right to privacy. The United States, which lacks a broadly defined constitutional approach constraining government collection, has instead only targeted legislative policies at subject-specific

---

98 Id. at *5-6 (accepting, for purpose of the preliminary injunction analysis, the Government’s description of records collection under 50 U.S.C. § 1861).
99 Id. at *20.
100 132 S.Ct. 945 (2012).
101 *Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurred) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).
102 Id. at 957.
103 442 U.S. 735 (1979).
104 *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).
105 Id. at 750.
information held by private entities.\textsuperscript{106} In stark contrast, the European approach has outlined “a set of rights and principle for the treatment of personal data, without regard to whether the data is held in the public or private sector.”\textsuperscript{107} This European approach recognizes that “[e]ven in a world in which, thanks to technology, acquiring knowledge about others is virtually effortless, personal autonomy must be respected.”\textsuperscript{108}

Under European law, a governmental data-mining regime similar to the NSA’s would be illegal, failing both procedural and substantive privacy guarantees.\textsuperscript{109} Procedurally, an independent governmental agency would be charged with oversight and enforcement powers to ensure the privacy ramifications of the government initiative are fully debated and widely understood, and to assist in detecting andremedying privacy violations.\textsuperscript{110} Substantively, data could only be collected to a more narrow purpose and retained for limited duration, as opposed to the five-year window available to the NSA.\textsuperscript{111} Furthermore, under national data protection regimes, using Germany as an example, there must be “imminent and specific endangerment” of a serious offence before any data-mining could occur.\textsuperscript{112} Beyond these safeguards, European law includes a right of access for an individual to review their information for factual correctness and to ensure compliance with the guarantees of privacy law.\textsuperscript{113}

The German Constitutional Court applied these principles in 2006, after German police forces had compiled common terrorist profiles from various data sources following the September 11th attacks in New York City.\textsuperscript{114} In assessing the proportionality of this legally sanctioned data-mining, the Constitutional Court found a legitimate national security purpose and that data-mining was a suitable and necessary means to obtain that goal, but determined the program was still unconstitutional because the burden on the right of informational self-determination was not proportionate to the public ends pursued.\textsuperscript{115} Specifically, absent actual facts demonstrating an “imminent and specific endangerment” of a terrorist attack, general fear of terrorism in the wake of September 11th did not justify this intrusion upon the privacy right.\textsuperscript{116} The program could not stand in light of the established right to privacy.\textsuperscript{117}

\textsuperscript{106} Slemmons Stratford & Stratford, supra note 4, at 17.
\textsuperscript{107} Id.
\textsuperscript{108} Bignami, supra note 66, at 138.
\textsuperscript{109} Bignami, supra note 70, at 635.
\textsuperscript{110} Id.
\textsuperscript{111} Id.
\textsuperscript{112} Id. at 636.
\textsuperscript{113} Id.
\textsuperscript{114} Id. at 653-654.
\textsuperscript{115} Id. at 654.
\textsuperscript{116} Id. at 654-655.
\textsuperscript{117} Id.
C. APPLICABILITY OF EUROPEAN LAW IN UNDERSTANDING CONSTITUTIONAL PRIVACY

Following the Second World War, human rights-based constitutionalism has resulted in a growth of applicable international human rights law, with “more tribunals issuing reasoned constitutional decisions.” 118 Given this growth of deliberate international discourse on human rights, and that “cautious comparativism within this framework is consistent with past interpretive practices,” 119 United States courts should look to and adapt the three-fold test from the European Court of Human Rights when evaluating governmental information collection, and therefore should affirm the preliminary injunction granted by the district court in Klayman.

IV. CONCLUSION

This article discusses the revelations from the NSA’ Bulk Telephony Metadata Program and the Prism Program, as well as the litigation that immediately preceded and followed these revelations. 120 The article then reviewed the current United States Supreme Court precedent related to the Fourth Amendment prohibition against “unreasonable search and seizures,” 121 The article next contrasts this approach with the European approach to the right to privacy, with illustrative cases where it has been constitutionally protected through various courts in Europe. 122 Finally, this article reviews the use and influence of foreign and international law on American constitutional issues and suggests the United States Supreme Court adapt the privacy standards, and the three-fold tests utilized to assess infringement of those privacy rights, as currently provided in European nations. 123

Article 12 of the 1948 Universal Declaration of Human Rights states, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” 124 This express right to the protection of the law should be extended by the United States Supreme Court to curb large-scale data gathering by the United States Government against its own citizens. By adapting the broad approach to the right to privacy enforced throughout Europe, and affirming the wisdom of Justices Marshall and Sotomayor, the United States Supreme Court should affirm the preliminary injunction granted in Klayman v. Obama.

118 Jackson, supra note 73, at 111.
119 Id. at 128.
120 See supra note 10-41 and accompanying text.
121 See supra note 42-62 and accompanying text.
122 See supra note 63-72 and accompanying text.
123 See supra note 73-119 and accompanying text.