



DATE DOWNLOADED: Sat Sep 5 16:08:38 2020

SOURCE: Content Downloaded from [HeinOnline](#)

Citations:

Bluebook 21st ed.

Garrick Chan, *Klayman v. Obama* 957 F. Supp. 2d 1 (D.D.C. 2013), 19 INTELL. PROP. L. BULL. 203 (2015).

ALWD 6th ed.

Chan, G. ., *Klayman v. obama* 957 f. supp. 2d 1 (d.d.c. 2013), 19(2) Intell. Prop. L. Bull. 203 (2015).

APA 7th ed.

Chan, G. (2015). *Klayman v. obama* 957 f. supp. 2d (d.d.c. 2013). *Intellectual Property Law Bulletin*, 19(2), 203-206.

Chicago 7th ed.

Garrick Chan, "*Klayman v. Obama* 957 F. Supp. 2d 1 (D.D.C. 2013)," *Intellectual Property Law Bulletin* 19, no. 2 (Spring 2015): 203-206

McGill Guide 9th ed.

Garrick Chan, "*Klayman v. Obama* 957 F. Supp. 2d 1 (D.D.C. 2013)" (2015) 19:2 *Intellectual Property L Bull* 203.

MLA 8th ed.

Chan, Garrick. "*Klayman v. Obama* 957 F. Supp. 2d 1 (D.D.C. 2013)." *Intellectual Property Law Bulletin*, vol. 19, no. 2, Spring 2015, p. 203-206. HeinOnline.

OSCOLA 4th ed.

Garrick Chan, '*Klayman v. Obama* 957 F. Supp. 2d 1 (D.D.C. 2013)' (2015) 19 *Intell Prop L Bull* 203

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at

<https://heinonline.org/HOL/License>

-- The search text of this PDF is generated from uncorrected OCR text.

-- To obtain permission to use this article beyond the scope of your license, please use:

[Copyright Information](#)

Klayman v. Obama

957 F. Supp. 2d 1 (D.D.C. 2013)

GARRICK CHAN*

BACKGROUND

In June 2013, various international newspaper outlets reported on classified material pertaining to the U.S. government's practices on intelligence and surveillance data collection. The source of these "leaks" was Edward Snowden, a former National Security Agency (NSA) contractor. The initial media report disclosed an order issued by the Foreign Intelligence Surveillance Court compelling Verizon Business Network Services (Verizon Wireless) to produce to the NSA all national and international call records ("metadata"), regardless of whether there was any suspected wrongdoing.

Plaintiffs, subscribers to Verizon Wireless, brought two suits against the U.S. government (the "Government") and various corporate defendants. The first suit, *Klayman I*, refers to phone record data collection and analysis, whereas the second suit, *Klayman II*, addresses both phone and Internet record data collection and analysis. More specifically, "plaintiffs allege that the Government has violated their individual rights under the First, Fourth, and Fifth Amendments of the Constitution and has violated the Administrative Procedure Act ("APA") by exceeding its statutory authority under FISA."¹

PROCEDURAL HISTORY

Plaintiffs initiated suit in 2013 and moved for preliminary injunctions preventing further collection of metadata, and requiring the Government to destroy previously collected call records. The U.S. District Court for the District of Columbia held that it lacked sufficient jurisdiction to opine on the APA claim. However, the court also found that the Plaintiffs had standing to raise a Fourth Amendment challenge, and the Government's past and current practices constituted a Fourth Amendment search. The court held that the Plaintiffs were likely able to meet their burden of proof in showing that the searches were unreasonable, and thus entitled to injunctive relief based on an adequate demonstration of irreparable

* Garrick Chan is a 2016 J.D./M.B.A. candidate at University of San Francisco School of Law.

1. *Klayman v. Obama*, 957 F. Supp. 2d 1, 11 (D.D.C. 2013). "FISA" is an abbreviation for the Foreign Intelligence Surveillance Act of 1978. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. § 1801 et seq.).

harm.

ISSUE

The overarching issue was whether the Plaintiffs' reasonable expectations of privacy were violated when the Government randomly collected and analyzed telephone metadata without obtaining prior consent. More specifically, the case addressed whether the Government exceeded its statutory authority under the APA, and whether it violated its constitutional authority under the First, Fourth, and/or Fifth Amendments of the Constitution.

DECISION

The court granted the preliminary injunction sought in *Klayman I*, but denied the preliminary injunction sought in *Klayman II*. The preliminary injunction prevented the Government from continuing to collect personal metadata and ordered the destruction of any previously collected metadata still in its possession. However, the order was stayed pending appeal.

REASONING

The court began by explaining the statutory background. First, the Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 by Congress "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes."² After the September 11th terrorist attacks, Congress made changes to FISA by passing the USA PATRIOT Act codified at 50 U.S.C. § 1861.³ Section 1861 expanded FISA, by authorizing the Federal Bureau of Intelligence (FBI) to apply for an order requiring the production of "tangible things" as well as the business records of U.S. citizens. However, the USA PATRIOT Act also placed some restrictions on the FBI's collection and analysis of information.

The Government began collecting telephone records in 2006, describing it as a "counterterrorism program." More specifically, the NSA collected metadata records from various telecommunications companies such as Verizon Wireless, and stored the data in a database. Although specific compliance procedures and protocols were established for using the database, there were known instances of governmental noncompliance and unauthorized uses of information.

2. *Klayman*, 957 F. Supp. 2d at 11 (quoting *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013)).

3. The USA PATRIOT Act is a backronym that stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2011.

Plaintiffs alleged that the current program “exceeds the statutory authority granted by FISA’s ‘tangible things’ provision, 50 U.S.C. § 1861, and thereby violates the Administrative Procedure Act.”⁴ However, the Government asserted that the court is precluded from reviewing the Plaintiffs’ statutory APA claim.

First, the court held that § 1861 only extended the right of judicial review to the recipients of production orders. This includes telecommunications companies but does not extend to third-party subscribers, such as the Plaintiffs. Second, the court noted that Congress likely did not intend for third parties to have standing to bring an APA claim because third parties were not supposed to know about the Government’s authority to compel the production of records under § 1861. The court concluded that, although the collection of telephone records and metadata are linked to the subscribers and Plaintiffs’ interests, Congress did not intend for the court to have jurisdiction to hear the third-party claims regarding the Government’s statutory authority under FISA.

Although the court stated it lacked jurisdiction to opine on the Plaintiffs’ APA claim, it did evaluate the Plaintiffs’ challenge to the Government’s constitutional authority. Plaintiffs argued that, absent a clear Congressional prohibition on individual constitutional rights, Congress should not rest on statutory limitations.

When ruling on a preliminary injunction, the court must consider “whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further public interest.”⁵

In this case, the court emphasized the successfulness of the Plaintiffs’ Fourth Amendment arguments. The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”⁶ In *Clapper v. Amnesty Int’l USA*, the Supreme Court found that to have proper standing under Article III of the Constitution the plaintiff must have suffered “an injury [that is] concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.”⁷ In this case, the Plaintiffs met the *Clapper* standard by showing that the NSA had, and would continue to improperly use, its telephone metadata for collection and analysis.

Finally, the court found that telephone metadata collection and

4. *Klayman*, 957 F. Supp. 2d at 19.

5. *Sottera, Inc. v. Food & Drug Admin.*, 627 F. Supp. 2d 58, 76 (D.D.C. 2010).

6. U.S. CONST. amend. IV.

7. *Clapper*, 133 S. Ct. at 1147.

analysis constituted a search within the definition of the Fourth Amendment under the standard set forth in *Smith v. Maryland*.⁸ Also, that the Plaintiffs would likely succeed in showing that the search was unreasonable because they had a reasonable subjective expectation of privacy in their telephone records. As a result, the court found that the Plaintiffs would suffer irreparable harm if the preliminary injunction for relief were not granted. Although the Government often cited to preventing terrorism as a justification for the collection and retention of the data, the court found that telephone metadata collection and analysis is an important issue that significantly affects the public interest.

8. *Smith v. Maryland*, 442 U.S. 735 (1979).