media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 3/2016

ANDREA SERENA*

Apple v. FBI, or the Role of Technology on the Functioning of the Law

SUMMARY: 1. The Facts. - 2. The Arguments. - 3. A Final Comment.

1. *The Facts*

On February 16,[1] a Magistrate Judge of the Central District of California ordered Apple to help the FBI unlock the iPhone of Syed Farook, one of the killers of the San Bernardino carnage.

The Department of Justice relied in its request on the 1789 All Writs Act, a gap-filling federal statute that gives judges broad powers to ensure their orders are fulfilled, such as compelling a landlord to produce the keys of an apartment subject to a search warrant. As a matter of fact, its wording is fairly short and broad:

* Combined Bachelor and Master of Science in Law Candidate, Bocconi University

[1] The case is officially named *In re Matter of the Search Warrant of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*.

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

"The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

Subsequently, on February 25 Apple presented a motion to vacate, which is a request for a court to withdraw a judgment or order that it issued, which will be subject to hearing on March 22.

2. *The Arguments*

In a case like this, a bit of context is needed. Usually, if law enforcement needs some data into a locked iPhone, it just has to send the phone to Cupertino with a search warrant to get access to it. However, in September 2014 Apple released new encryption in its latest operation system, iOS 8, in response to the privacy earthquake of the Snowden revelations, making impossible for themselves to unlock an iPhone as the passcode itself is now encrypted in the device, and Apple does not keep them in any central database. Moreover, after ten wrong guesses of the password, subjects to progressive delays between them, all the data in the iPhone is automatically erased. Nonetheless, although the information is encrypted, the software controlling the smartphone is hackable, that means modifiable even if locked. That is exactly what the FBI and the court are demanding Apple to do: rewriting iOS 8 to unable the delay periods and the erasing feature, so to be able to "brute force" the passcode quickly. The authority of the judge to impose such obligation is based on the All Writs Act, whose application is based on the 1977 New York Telephone Company case[2], where the Supreme Court laid down a test to evaluate the legality of those orders. The judge must verify that (1) the company must be related to the case; (2) the order must not place an unreasonable burden on it; (3) company's assistance must be necessary. In her application to the court, Department of Justice's Attorney Eileen Decker believes that (1) Apple is not

[2] *United States v. New York Telephone Co.* 434 U.S. 159

"removed" from the case at hand having manufactured the phone; (2) to modify software it is not burdensome for a company who writes code as its core business; (3) the data in the iPhone cannot be recovered in any other way, making necessary Apple's involvement.

Apple contested the judge's decision on several grounds. Firstly, it argues that the burden put on it is too large, as it requires writing a new version of iOS (ironically called GovtOs), with all the internal procedures and human resources costs involved. Moreover, although the FBI's denials, Apple warned against the government trying to establish here a powerful precedent, with the aim of using it in hundreds of other similar trials, as in the meantime declared to the news by local officials across the country. This will have a double effect: forcing a continuous cooperation of Apple on the matter (undue burden) and expanding the scope of the All Writs Act in an unprecedented way. The latter point has been recognised in a similar case in NYC, where on February 29, a magistrate judge rejected a request for an AWA order by the DOJ on a drug dealer's iPhone. Judge Orestein held that:

«What the government wants here goes beyond the well-established duties of citizens to aid law enforcement — by, for example, turning over evidence or giving testimony — because Apple doesn't actually possess the information on the iPhone that the government seeks. The order the government has proposed would also violate the Fifth Amendment, which imposes a limit on the assistance that law enforcement may compel of innocent third parties who don't actually have the information the government is after — a limit the government has crossed in this case.

[…]

The government's position also produces a wholly different kind of absurdity: the idea that the First Congress might so thoroughly undermine fundamental principles of the Constitution that many of its members had personally just helped to write or to ratify. Its preferred reading of the law — which allows a court to confer on the executive branch any investigative authority Congress has decided to withhold, so long as it has not affirmatively outlawed it — would transform the AWA from a limited gap-filing statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by

Congress's superior ability to prohibit or preempt. I conclude that the constitutionality of such an interpretation is so doubtful as to render it impermissible as a matter of statutory construction.»

Significant the comment to this made by the American Civil Liberties Union[3]:

«It doesn't take a constitutional scholar to understand that there is a limit on the government's power to conscript third parties into the service of law enforcement. That's the kind of limit that distinguishes a democratic government from a police state.»

What Orestein is calling upon is that the legitimate claims of the Justice Department should not be addressed by the judiciary, but subject to a legislative solution through Congress.

Furthermore, Apple said that the order violates its Fifth Amendment right to be free from arbitrary deprivation of its liberties, as it will erase every limit on the usages of the AWA, leaving completely aside the original purpose of the law. In addition to this, the tech corporation and the Electronic Frontier Foundation, in its amicus brief to the court, have put through another defence based on First Amendment's rights. The EFF explained that iOS is designed to accept only iOS code digitally signed by Apple, and since 3 million phones were stolen in 2013 alone, the protection this procedure provides proves to be fundamental. The First Amendment prohibits the government from compelling unwilling speakers to speak and subjects to strict scrutiny, the most stringent standard of judicial review in the US, any mandate requiring people to speak. As in 1996 the Ninth Circuit Court of Appeals recognised computer code as protected speech[4], by forcing Apple to write and sign new iOS code, the court is also compelling Apple to speak—in violation of the First Amendment.

Lastly, Apple defence refers to a 90s piece of legislation, the Communications Assistance for Law Enforcement Act, which requires telecommunications carriers to assist law enforcement in performing electronic surveillance on their digital networks pursuant to court order or other lawful authorization. Thus, they say, as the AWA applies only if there is

[3] Sweren-Becker, E. *Why We're Defending Apple*.
Retrived: 11/03/16, from: https://www.aclu.org/blog/speak-freely/why-were-defending-apple
[4] Daniel J. Bernstein et al., v. United States Department of State et al. 176 F.3d 1132

no other statute addressing the issue, the fact that CALEA regulates those kind of activities automatically excludes the usage of the AWA. The DOJ addressed this matter sustaining that Apple is not a telecommunication carrier, unfortunately, CALEA applies also to manufacturers of telecommunication equipment, which Apple definitely is. As noticed[5] by Albert Gidari of the Center for Internet and Society at the Stanford University, Section 1002(b)(1) of the Act prohibits law enforcement agencies to order to manufacturers specific design of equipment or sotware configuration, including security features; a clear limitation on court's powers under the AWA, but precisely what the FBI has obtained in California. On top of that, the wording of Section 1002(b)(3) proves to be essential:

«(2) Encryption

A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.»

While the DOJ says that this provision force carriers to decrypt communications if they hold the decryption keys, exactly what they want Apple to do, the article means also something more: it permits carriers to develop encryption for which they do not retain the keys, precluding the government to dictate that such measures contain encryption.

3. *A Final Comment*

In this lawsuit, legal and technological aspects are inextricably tied together, proving once again Lessig's foresight in theorizing the disrupting consequences the digital world has on

[5] Gidari, A. *Calea limits the All Writs Act and protects the security of Apple's phones*. Retrieved: 11/03/16, from: http://cyberlaw.stanford.edu/blog/2016/02/calea-limits-all-writs-act-and-protects-security-apples-phones

the functioning of our physical world laws[6]. Besides, this trial can be seen as a manifestation of the endless fight between East Coast code (legal regulatory design) and West Coast Code (environmental regulatory design), between the governmental agencies from Washington, D.C. and the tech companies from Silicon Valley, in a battle that will shape our fundamental rights in the future.

Indeed, many commentators fears that once this "backdoor" in iOS is created, it will be at disposal of criminals and authoritative regimes worldwide, with potential chilling effects on freedom of expression in particular.

As Yochai Benkler from Harvard Law School puts it in an article appearing on the Guardian on February 22[7]:

«Apple's design of an operating system impervious even to its own efforts to crack it was a response to a global loss of trust in the institutions of surveillance oversight. It embodied an ethic that said: "You don't have to trust us; you don't have to trust the democratic oversight processes of our government. You simply have to have confidence in our math." […] The problem with the FBI's approach is that it betrays exactly the mentality that got us into the mess we are in. Without commitment by the federal government to be transparent and accountable under institutions that function effectively, users will escape to technology. If Apple is forced to cave, users will go elsewhere. American firms do not have a monopoly on math»

The legitimacy the governmental power will be able to attract on itself will define the outcome of this battle, which started, irony of fate, only a few weeks after the 20th anniversary of the Declaration of the Independence of Cyberspace by John Perry Barlow (among other things co-founder of the EFF). Cyberspace went from being a promise of liberty to enabling the biggest mass surveillance system ever existed, but what's next? Perhaps on March 22 we will know the answer.

---

[6] Lessig, L. (1999) *"Code and Other Laws of Cyberspace"*. New York: Basic Books.
[7] Benkler, Y. *We cannot trust our government, so we must trust the technology*. Retrieved: 11/03/16, from: http://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi