American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
http://asrjetsjournal.org/

United States Versus Microsoft Corp.; Should U.S. Online Privacy Statutes Apply Abroad?

Saif Almutairi*

Widener University, Delaware Law School, S.J.D. program, 4601 Concord Pike, Wilmington, DE 19803
Email: Almutairis12@yahoo.com

Abstract

The United States v. Microsoft Corp. deals more broadly with the issue that should U.S online privacy statutes apply abroad or not, than it deals with the issue of Whether a U.S corporation that chose to store its data abroad has to comply with U.S. warrant issued based on probable cause to render its data that is fall within U.S corporation's control. Nevertheless, Congress only has the power to enact statutes that could be applied abroad. However, U.S. privacy online statutes should not be interpreted by courts to apply abroad because that will violate the presumption against extraterritorial and create a contradiction between authorities. Therefore, the final rule in this case must be in favor of Microsoft.

Keywords: *privacy; Fourth Amendment; Stored Communication Act; Extraterritorial application; Presumption against extraterritoriality.*

1. Introduction

Although the case of *United States v. Microsoft Corp*. deals with the issue of Whether a U.S corporation that chose to store its data abroad has to comply with U.S. warrant issued based on probable cause to render its data that is fall within U.S corporation's control, *United States v. Microsoft Corp*. deals more broadly with the issue that should U.S online privacy statutes apply abroad or not. The issue begun when the district court issued a warrant under SCA to seize and search e-mail content that was suspected to be used by drug dealer to sell and distribute its drug. The government delivered the warrant to Microsoft's headquarter in U.S. and Microsoft executed the warrant partly and rendered data that has in its servers in U.S. and refused to render content of that e-mail because it is located abroad and complying with U.S. warrant will violate the presumption against extraterritoriality. [1] The district court ruled in favor of the government stating that the warrant does not violate the presumption against extraterritoriality. The court concluded that the SCA Act authorizes the court to issue overseas warrant. The court believed that the test for producing documents using a subpoena is "control not location". Therefore, the court ruled that SCA warrant is hybrid warrant which means it issues like a warrant and executed like a subpoena and that because it executed by a service provider not a law enforcement. [2].

---

* Corresponding author.

The court of appeals vacated the district court judgment and ruled in favor of Microsoft stating that the warrant violate the presumption against extraterritoriality. The court of appeals believed that the goal of SCA is to protect the user's privacy and the language of the statute does not refer to an extraterritorial application of its warrant. The court stated that Congress used the term "warrant" to provide more of privacy protection by requiring third party to conduct pre-disclosure scrutiny. Id. Thus, the warrant limitation and other constitutional requirements still apply. The court of appeals concluded that District Court has no authority to enforced SCA warrant against Microsoft [1]. The Supreme Court vacated the court of appeals judgment and held that there is no dispute remained between parties as long Congress enacted CLOUD Act that amended SCA [3].

2. Background

2.1. Fourth Amendment and the Stored Communication Act

"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'" [4]. Thus, to keep property possession and to preserve personal privacy are the two interests protected by the 4th amendment which "a seizure pertains to the first interest, and a search pertains to the second". Therefore, a reasonable expectation of privacy could be a claim against government action that will invoke the 4th amendment protection. [4]. The test of expectation of privacy under the 4th amendment is whether (1) there is a subjective expectation of privacy, and (2) that subjectivity is recognized or prepared to be recognized by the society [5]. Governmental action that may constitute searching and seizing within the context of the 4th amendment is almost considered to be at the heart of any issue's analysis dealing with violating the 4th amendment [5]. Thus, the test of violating searching within the context of the 4th amendment is whether there is an infringement of the expectation of privacy that is been recognized by the society as a reasonable [6]. Whereas, the test of violating seizing within the context of the 4th amendment is whether there is "some meaningful interference with an individual's possessory interests in that property" [6]. Due to the rapid technology development and lacking federal provisions to protect privacy of electronical communications were reasons, among others, that lead congress to pass the Stored Communication Act (SCA) in 1986 [7]. The SCA covers two types of information and providers. In terms of information, it covers content and non-content information [8]. Content information refers to the meaning or the core of that communication whereas, non-content information, also known as metadata, refers to non-core information of the communication like name, address, etc. Therefore, content information has higher degree of privacy than non-content information. [8]. In terms of providers, two types of providers are covered by SCA which are Electronical Communication Service (ECS) and Remote Communication Service (RCS) providers. ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications" [9]. Whereas, RCS is defined as "storage and processing services provided to the public that utilizes electronic communication systems". § 1:23.Right of privacy—Electronic Communications Privacy Act (ECPA), Oh. Arrest, Search & Seizure § 1:23. The SCA goal is to provide protection for the stored communications network account holders by limiting provider's voluntary disclosure and set forth procedures or requirements for government to compel involuntary disclosure [7]. Section 2702 of SCA prohibits "… the provider of a wire or electronic communication service [to knowingly disclose]to the public … the contents of any communications while in electronic storage by that service to any person other than the addressee or intended recipient" [7]. In the other hand, section 2703 states the requirements needed to be taken from the

government in order to compel a disclosure of a stored electronic communication. [7] . To compel involuntary disclosure, a government can use; (1) a subpoena, (2) a court order, and (3) a warrant. [10]. The warrant considered to be the strongest means, among others, to obtain information because it discloses any information related to the account whether content or non-content information. To issue a warrant, an approval of a judge is needed as well as complying with the Federal Rules of Criminal Procedures which requires a probable cause. [10].

2.2 Extraterritorial application

Due to the mobility of data around the world, a problem of searching and seizing data located not within U.S. territory arise. A presumption exists among federal courts that federal statutes does not apply abroad [11]. However, cases with transnational features (one conduct happened in territory and the second not) have been difficult to be resolved which makes courts wandering when federal statutes should be apply abroad [12]. To do so, courts took approach to resolve transnational features cases and set forth steps for extraterritorial application of federal statutes. Two steps to determine whether a statute applies extraterritorial; (1) the rebutted of the presumption against extraterritoriality, (2) the domestic application of the statute to the involving case [13]. In order to determine whether the presumption against extraterritoriality is rebutted, the court look to whether Congress make clear indication that a statute apply extraterritorial [13]. And in order to determine whether there is a domestic application, the court looks to the focus of the statute [13]. If the conduct that relevant to the focus of the statute occurred in U.S., then the extraterritorial application is allowed regardless of others conducts where occurred and if the conduct that relevant to the focus of the statute occurred abroad, then the extraterritorial application is not allowed regardless of the other conducts [11].

3. Arguments

The issue began when the district court issued a warrant that is been served to Microsoft's headquarter in U.S. asking Microsoft to seize and deliver data located outside U.S [1]. Microsoft complied with the warrant partly and rendered non-content information that has in its servers in U.S. and refused to access and delivered information that is located outside U.S. [1]. Microsoft argument was that the search warrant has territorial limitations and thus cannot be executed abroad because it violated the presumption against extraterritoriality that relies on the focus conduct of SCA which is protecting a "user's privacy" [1]. Microsoft believed that rule 41 of federal criminal procedures limits the application of a warrant within the U.S. territory, and apply it abroad will violate the presumption against extraterritoriality, international law as well as Ireland law [14]. The government argued and stated that as long the statute is silent in regard to extraterritoriality, then there is nothing prohibit SCA warrant to be applied abroad. The government invoked a previous court's ruling that used subpoena to produce documents located abroad. [14]. The government believed that the SCA is silent about extraterritoriality principles and the focus conduct is "compelled disclosure" which is limited to § 2703 not to the entire statute because § 2701 and § 2702 regulated different actors and actions [15].

§2701 prevents unauthorized access, § 2702 prevent knowingly disclosure to the public and § 2703 deals with compelled disclosure. Therefore, the focus conduct in this case is "compelled disclosure" which makes the SCA

warrant operated like a subpoena that can be applied abroad [16]. Microsoft disagreed and stated that the statute focus conduct is "user's privacy" and the absence of extraterritorial application does not create abroad application permission [17]. Also, SCA warrant cannot be similar to subpoena because both operated differently and have been mentioned in the statute separately. [17, p. 19] Therefore, SCA warrant cannot be operated like a subpoena. [17, p. 21] Microsoft stated that all sections mentioned by the government deal with protection of stored communications whether from hackers or employees §2701, untrusted providers§2702, or government §2703. Therefore, the conduct focus is protection of a user's privacy [17]. The government argued that if the focus conduct is to protect privacy, then, collect a user's information abroad does not considered to be an invasion of privacy because Microsoft choose where to store its data freely and has control and access over the requested information, and the SCA allows service provider to transfer users data. Appellants Brief at 26. Thus, the collection occurs abroad, but the disclosure occurs domestically which will be protected by the fourth amendment [17]. Microsoft disagreed and stated that the "collect" act still an extraterritorial application because the focus of SCA is to protect stored communications regardless of its location and Congress used the term "warrant" to limit searching and seizing on stored communications domestically [17]. Microsoft warned the court to not rule in favor of the government because that will create an intentional conflict of laws and will open the door for foreign countries to seize U.S. citizens' data and will leave European companies between ignoring U.S. laws and held liable or complying with U.S. laws and violate their laws [18]. In the contrast, the government warned the court to not rule in favor of Microsoft because will affect the combat against crimes and society protection against criminal activities. Also, such a judgment could facilitate the way for companies like Microsoft to get around U.S. law by storing their data abroad [18].

4. Conclusion

Congress only has the power to enact statutes that could be applied abroad. However, U.S. privacy online statutes should not be interpreted by courts to apply abroad because that will violate the presumption against extraterritorial and create a contradiction between authorities. Therefore, the final rule in this case must be in favor of Microsoft.

4.1. Presumption against extraterritoriality

In general, federal courts have a presumption that Congress enacted statutes to apply domestically not abroad unless Congress express its intention of extraterritorial application. Put differently, "legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." [19]. Moreover, "Statutory provision must contain a clear indication of an extraterritorial application, otherwise, it has none." [1, p. 198]. Clear or explicit indication it is an important factor to determine whether a statute should apply abroad or not. If Congress made no explicit intention of exterritoriality, then courts are not in need to search into its intent. Congress's role, among others, is to enact statutes and amend them which occurred previously in the same context. In Aramco case, the court held that the title VII does not regulate conducts occurred abroad and thus violated the presumption against exterritoriality. [19, p. 244]. However, Congress within one year of that decision amend title VII to have extraterritoriality affect [20]. Moreover, the Supreme Court rejected to apply securities law abroad on the basis of presumption against extraterritoriality but

after one month of that decision Congress amend the statute and expand its application to overseas. [20]. Thus, courts are not in need to search into Congress's intent whether it meant an exterritorial application or not because it has the power to amend its statutes which is occurred previously or enact new ones. Therefore, U.S. privacy online statutes should not be applied abroad because Congress did not express its intention of exterritorial application and Congress has the power to do so explicitly rather than make courts search into its intention.

4.2. Create a contradiction between authorities

Congress has the constitutional authority to grant statutes that have abroad application effects, and Congress, not courts, take into account rapidly development law areas that requires monitoring and updating the law with having regard to political aspects because it is the responsible branch. [14, pp. 22-23]. Therefore, courts searching into Congress's intention create a contradiction between judicial and legislative authorities. The legislative, executive, and judicial branches are powers derived from the Constitution which is protected by confining each branch to its responsibilities [21]. Each branch exercises its powers and responsibilities and encroach upon other responsibilities is prohibited. This system of separation prevents to accumulate all or some powers in one hand or side [22]. Thus, Congress as a legislative branch has all necessary facilities to draw a policy of exterritorial application in case of international conflicts is so clear [23]. In another hand, the judicial function is to interpret statutes. [24]. Moreover, courts' role is to apply not to amend laws [25]. Therefore, courts cannot amend statutes to apply it abroad with the absence of Congress intention because that will be encroached of Congress's responsibilities. In fact, Congress has the ability and knowledge on how to include extraterritorial application within a statute jurisdiction. [19, p. 258]. Also, the need of clear statement in case of exterritorial application reflecting the awareness of Congress in this regard. [19, p. 258]. Thus, the extraterritorial application is a political not judicial question that Congress needs to address not courts because extraterritoriality issues fall within the Congress's responsibilities and thus arguments that includes foreign policy "should be directed to the Congress rather than to [the court]" [26]. Therefore, courts searching into Congress intention create a contradiction between legislative and judicial authorities because extraterritoriality is a political question that fall within the responsibility of the Congress not the court. and thus U.S. privacy online statutes should not be applied abroad. Finally, the court should rule in favor of Microsoft because applying U.S. privacy online statutes abroad will violate the presumption against extraterritoriality and create a contradiction between legislative and judicial authorities.

References

[1] *Microsoft Corp. v. U.S.,* (2016)..

[2] *Microsoft Corp. v. U.S.,15 F.Supp.3d 466 (S.D.N.Y. 2014),* (2014).

[3] *United States v. Microsoft Corp.,* (2018).

[4] *People v. Diaz,,* (2019).

[5] *Sims v. State*, 2019.

[6] *State v. Cardwell*, 2019.

[7] S. A. Morris, "Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by A Third Party," *42 Fordham Int'l L.J.*, pp. 183-187–188 , 2018.

[8] S. A. Morris, "Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by A Third Party," *42 Fordham Int'l L.J.*, pp. 183-188–189, 2018.

[9] O. S. Kerr, "A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It," *72 Geo. Wash. L. Rev*, pp. 1208-1214, 2004.

[10] S. A. Morris, "Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by A Third Party," *42 Fordham Int'l L.J.*, pp. 183-189–90, 2018.

[11] *WesternGeco LLC v. ION Geophysical Corp.*, 2018.

[12] J. R. O'Sullivan, "The Extraterritorial Application of Federal Criminal Statutes: Analytical Roadmap, Normative Conclusions, and A Plea to Congress for Direction," *106 Geo. L.J.*, pp. 1021-1031, 2018.

[13] *RJR Nabisco, Inc. v. European Cmty.*, 2016.

[14] *Microsoft Corp. v. U.S., Appellants Brief 1*, 2016.

[15] *Microsoft Corp. v. U.S., Appellants Brief 4*, 2016.

[16] *Microsoft Corp. v. U.S., Appellants Brief 26*, 2016.

[17] *Microsoft Corp. v. U.S., Appellants Brief 9*, 2016.

[18] (. Howe). [Online]. Available: https://www.scotusblog.com/2018/02/argument-preview-old-laws-new-technology-national-borders/. .

[19] *EEOC v. Arabian American Oil Co.*, 1991.

[20] Z. D. Clopton, "Replacing the Presumption Against Extraterritoriality," *94 B.U. L. Rev.*, pp. 1-14–15 , 2014.

[21] *United States v. Green*, 2011.

[22] . *Patchak v. Zinke*, 2018.

[23] . *Benz v. Compania Naviera Hidalgo, S.A.*, 1957.

[24] *United States v. Am. Trucking Ass'ns*, 1940.

[25] . *Henson v. Santander Consumer USA, Inc.*, 2017.

[26] *McCulloch v. Sociedad National De Marineros De Hond.*, 1963.