A Justisdictional Analysis of Microsoft v. 10 John Does Using IP Address 73.21.204.220

Peter R. Stephenson
University of Leicester School of Law
Leicester, UK
prs33@leicester.ac.uk

Abstract — On 22 December 2017 Microsoft Corporation (MS) filed a lawsuit[1] (the "complaint") in the United States District Court for the Western District of Washington at Seattle. The suit alleges large-scale copyright infringement through software piracy and trademark infringement relative to Microsoft registered trademarks. What was unusual about this filing is that MS, at the time of filing, had nothing more on which to base its lawsuit than an IP address that had communicated over 2,8000 times with its registration servers in Seattle. This paper analyzes the jurisdictional issues raised by MS in the suit and questionable designation of an IP address as the definitive source of identities of the Does.

Keywords— cyber, tort, jurisdiction, software piracy, copyright infringement, trademark infringement, Internet crime

I. Introduction

The filing of "John Doe" lawsuits is not uncommon. It is used frequently in cyber-related cases where actual defendants are, at the time of the complaint, unknown as in this case.

However, the usual purpose for filing such a lawsuit is to facilitate discovery. Should the suit continue without discovering the true identities of the Doe(s) it must be dismissed without prejudice since service against an unknown party cannot be made[2]. Further, no injunction can be made against an unknown party.

Since discovery must be made relative to a case pending – i.e., a complaint and summons issued to the defendant[3] – the John Doe suit is useful only for obtaining defendant identity.

The current case states in relevant part (Section II paragraph 3 at line 25):

> *The true identities of Defendants are not presently known to Microsoft. On information and belief, Defendants are in possession or control of the Internet Protocol ("IP") address 73.21.204.220 ("the subject IP Address") and have used it to further the unlawful conduct alleged herein.*

This poses intertwined technical and jurisdictional challenges. This research paper will explore those challenges.

II. Jurisdiction and Venue

MS claims personal jurisdiction over the Does based upon several theories. The complaint says, in relevant part,

> *Civil actions, suits, or proceedings arising under any Act of Congress relating to copyrights or exclusive*

[1] Microsoft Corporation v. John Does 1-10 using IP address73.21.204.220, (United States District Court, Western Disctrict of Washington at Seattle).
[2] See Jon BEUTLER, v. John DOE (In re <rat.com>), (Circuit Court of Virginia. Nineteenth Judicial Circuit, Fairfax County).
[3] See "Federal Rules of Civil Procedure (USA), Title II, Rule 4. Summons.

rights in mask works or designs may be instituted in the district in which the defendant or his agent resides or may be found[4].

MS also claims personal jurisdiction based upon Brayton Purcell LLP v. Recordon & Recordon[5]:

This circuit interprets this provision to allow venue in any judicial district where, if treated as a separate state, the defendant would be subject to personal jurisdiction.

Finally, MS states, again, in relevant part,

Venue is also proper in this district pursuant to 28 U.S.C. 1391(b) because a substantial part of the events giving rise to the claims occurred in the Western District of Washington.

28 U.S.C. 1391(b) reads:

(b) Venue in general. *-- A civil action may be brought in—*

(1) *a judicial district in which any defendant resides, if all defendants are residents of the State in which the district is located;*

(2) *a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated; or*

(3) *if there is no district in which an action may otherwise be brought as provided in this section, any judicial district in which any defendant is subject to the court's personal jurisdiction with respect to such action.*

On the surface it would appear that MS has a valid point regarding personal jurisdiction. However, a careful reading of the citations in the complaint tells a somewhat different story. The reasons are technical and based upon the basics of cyber science and demonstrate an instance where knowledge of these basics would be helpful.

We define cyber science as:

Cyber science is the study of phenomena caused or generated within the cyber space, which may or may not interact with phenomena caused or generated within the physical space[6].

In MS we see a combination of phenomena caused or generated within the cyber space and phenomena caused or generated within the physical space. It is clear that the physical space phenomina comprise the theft of intellectual property belonging to MS and the unauthorized registration of that intellectual property on an MS server located in Seattle.

What is not clear is where the Does reside. There is no guarantee that, simply because the IP address alleged by MS is, in fact, being used by Does who reside in the United States, complicating the jurisdictional issues as presented by MS. In fact, it is quite conceivable that the Does reside in some other part of the world and have hijacked the server at the IP address in the complaint. This is an action generated within the cyberspace. It demands a more thorough analysis of the address itself.

Because the complaint is filed largely with the intent of facilitating discovery, we may assume that (1) MS was not able to find out who the Does are through the owner of the address (Comcast) or, (2), that Comcast does not know who the Does are and deeper investigation is required. It is most likely that Comcast has not provided user information to MS and will not do so without a subpoena to prevent violations of its customers' privacy based upon a fishing expedition by MS[7].

[4] See 28 U.S.C. § 1400(a)

[5] See Brayton Purcell LLP v. Recordon & Recordon, 606 F.3d 1124 (9th Cir. 2010)

[6] Peter R. Stephenson, Defining a Cyber Jurisprudence (2017). *(See Definition I)*

[7] See State v. Reid, 194 N.J. 386, 945 A.2d 26 (2008) – this is one of the most-often cited cases on the topic of ISP subscriber policy. It

That the court has subject matter jurisdiction is clear from the citations by MS in the complaint[8].

III. Technical Considerations

The technical consideration in MS are part and parcel of the jurisdictional issues because there is no guarantee that the does are residents of any jurisdiction in which the court would have personal jurisdiction. Some of the considerations are:

- Are the Does direct users (subscribers) of the IP address?
- Have the Does hijacked the IP address which, in fact, is assigned to a legitimate user?
- Is the IP address static or dynamic? If dynamic, was it the only address allegedly used for the alleged infringements?
- Is the IP address in use by a home user or a business? Who has access to the computer(s) connected to the address?
- Is the IP address the Internet-facing element of a back-end computer network?
- If the IP address is connected to a back-end computer network, of what does the network consist? Are firewalls and other security measures in place?
- Is the IP address the actual IP address or has it been "spoofed"?

Recognizing that the complaint is for facilitating discovery and issuing a subpoena to which Comcast will need to respond, a detailed analysis of the computer(s) related to the IP address is necessary. The complaint reads in relevant part:

> *The true identities of Defendants are not presently known to Microsoft. On information and belief, Defendants are in possession or control of the Internet Protocol ("IP") address 73.21.204.220 ("the subject IP Address") and have used it to further the unlawful conduct alleged herein.*

Further, it may not be reasonable for the technical reasons to assert personal jurisdiction over all ten Does. There is no evidence that all ten Does participated in the same events that triggered the complaint and thus the joinder of the defendants would be improper[9].

The presence of the technical considerations suggested by the MS complaint tend to make the complaint too broad.

> *A plaintiff may sue a defendant using a fictitious name when she knows the defendant's general identity but cannot, without further discovery, determine the defendant's true name. In this situation: ... The plaintiff must provide a description that is sufficient to permit the defendant to be served with process[10].*

This specificity in the naming of John Doe defendants is well-settled. See, for example, Keno v. Doe which reads in relevant part[11],

> *This ruling in no way involves the long-known and well established practice of naming parties by fictitious names, such as "John Doe", when the real name of the party is not known. See, for example, Bivens v. Six Unknown Agents, 403 U.S. 388, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971). In such cases, however, the complaint should state that the name is fictitious and provide an adequate description of some kind which is sufficient to identify the person involved so that process can be served.*

---

requires, based upon the New Jersey Constitution, a subpoena prior to the surrender of subscriber information by the ISP.

[8] See 15 U.S.C. § 1121, 17 U.S.C. § 501, and 28 U.S.C. §§ 1331 and 1338(a)

[9] See Hard Drive Prods., Inc. v. Does 1-188, 809 F. Supp. 2d 1150 (N.D. Cal. 2011)

[10] *Complaint (Federal) RESOURCE ID 9-507-9951*, THompson, Reuters(2017), *available at* https://intl-westlaw-com.ezproxy3.lib.le.ac.uk/Document/I0f9fc042ef0811e28578f7ccc38dcbee/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=(sc.Search)#co_anchor_a514141.

[11] Keno v. Doe, 74 F.R.D. 587 (D.N.J. 1977), aff'd, 578 F.2d 1374 (3d Cir. 1978)

Given the vague description of the Doe defendants in the complaint (…*On information and belief, Defendants are in possession or control of the Internet Protocol ("IP") address 73.21.204.220*), make it difficult or impossible to, with certainty, identify the ten Doe defendants.

IV. Conclusions

While we do not argue with the need to address software piracy and copyright/trademark infringement, especially where the Internet is involved, we think that this complaint is likely not to lead to a successful conclusion. We find the identification of the Doe defendants to broad and vague to be useful, especially when the defendants must be named explicitly.

The technical considerations implicit and explicit in the facts of the case as presented by MS in the complaint are complicated and ambiguous. While we accept that the purpose of the complaint may be to permit discovery that can lead to the identification of the defendants, its overbroad nature will make the resulting investigation little more than a fishing expedition.

We suspect that, given the resources available to MS, there could be considerable more data available. For example, the complaint refers to MS use of cyberforensics[12]:

> *In order to combat the global threat of software piracy of its software, Microsoft relies on state-of-the-art technology to detect software piracy called "cyberforensics."*

The complaint goes on[13]:

> *Through cyberforensics, Microsoft analyzes activation data voluntarily provided*
>
> *by users when they activate Microsoft software, including the IP address from which a given product is activated. An IP address is a numerical identifier used to uniquely identify an internet-capable device when the device is connected to the Internet. An IP address is ordinarily assigned to an internet user (whether an individual or an entity) by the user's Internet Service Provider ("ISP").*

This is misleading because under certain circumstances IP addresses are assigned automatically based upon connection to the ISP server and are rotated periodically. While it is true that logs are kept of these rotations IP address use is by no means consistent, especially if an unauthorized user takes pains to obfuscate his or her actual use.

Given the level of cyberforensics and the breadth of MS's reach across the global Internet it should not be difficult to provide more information, perhaps making it more difficult for the Doe defendants ultimately to prevail.

[12] Complaint at E 29

[13] Complaint at E 30

Bibliography

Complaint (Federal) RESOURCE ID 9-507-9951, Thompson, Reuters (2017), *available at* https://intl-westlaw-com.ezproxy3.lib.le.ac.uk/Document/I0f9fc042ef0811e28578f7ccc38dcbee/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=(sc.Search)#co_anchor_a514141

Jon BEUTLER, v. John DOE (In re <rat.com>), (Circuit Court of Virginia. Nineteenth Judicial Circuit, Fairfax County).

Microsoft Corporation v. John Does 1-10 using IP address73.21.204.220, (United States District Court, Western Disctrict of Washington at Seattle).

Peter R. Stephenson, Defining a Cyber Jurisprudence (2017).