

# **JURISDICTION IN CYBERSPACE: A QUESTION OF CONFLICT OF LAWS?**

**Peter Stephenson, PhD, CISSP (ret)**

The Cyber Crime Research Lab  
PhD Research – University of Leicester, School of Law  
<https://DrPeterStephenson.org>

# AGENDA

- **Laying the Groundwork – Definitions and Issues**
  - **Cyber-definitions applicable to law in cyber space**
  - **Jurisdiction generally**
  - **The problem of jurisdiction in cyberspace**
  - **Choice of law and conflict of laws**

## Break

- **Addressing the Issues and cases**

# DEFINITIONS

- **Cyberspace**

- **Cyberspace is a complex global information infrastructure that facilitates communication between technology such as computers, networks and other digital systems, both independently and on behalf of people using it. Cyberspace is distinct from physical space and the constraints imposed by it such as geographic boundaries.**

- **Cyber Science**

- **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.**

- **Cyber Law**

- **Cyber law is the set of obligations and duties applied to events related directly to cyber science.**

- **Cyber Crime**

- **A cyber crime is crime or misdemeanor occurring in the space defined by cyber science and comprising an act committed or omitted, in violation of public law either forbidding or commanding it.**

- **Cyber Tort**

- **A cyber tort is a breach of duties fixed and imposed upon the parties by the law itself in the space defined by cyber science without regard to their consent to assume them, or their efforts to evade them that causes harm and for which courts will impose civil liability.**

- **Cyber Jurisprudence**

- **Cyber jurisprudence is the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law.**

# JURISDICTION GENERALLY

- **Authority of the court to hear and determine a cause**
- **Jurisdiction over the person, jurisdiction over the subject-matter, and jurisdiction to render the particular judgment**
  - **A court has subject matter jurisdiction if it has the authority to adjudicate a particular type of legal controversy. Such jurisdiction relates to the court's competency to exercise power, and not to the regularity of the court's exercise of that power.**
    - **Ungerland v. Morgan Stanley and Co., Inc.**
  - **Personal jurisdiction precedents call for a two-part analysis. The contacts prong asks whether the defendant has sufficient contacts [“minimum contacts”] with the forum State to support personal jurisdiction; the reasonableness prong asks whether the exercise of jurisdiction would be unreasonable under the circumstance**
    - **Daimler AG v. Bauman**
  - **Territorial jurisdiction is the concept that only when an offense is committed within the boundaries of the court's jurisdictional geographic territory, which generally is within the boundaries of the respective states, may the case be tried in that state – roots are in the Sixth Amendment**
    - **State v. Butler – MD Court of Appeals**

# THE PROBLEM OF JURISDICTION IN CYBERSPACE

## ▪ Territorial Jurisdiction

- Cyberspace does not reflect any territory or it reflects all territories
- ID of the source and destination locations
- Territoriality is the basis of all jurisdictional matters (Svantesson: Solving the Internet Jurisdiction Puzzle)

## ▪ Subject matter jurisdiction

- US Constitution – Article III, Section 2, Clause 1
  - *The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority ... between Citizens of different States ... and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.*
  - This does not present a problem (usually) in cyberspace and generally either would survive an attack or permit a change of territory – BUT... see Territorial Jurisdiction

## ▪ Personal jurisdiction

- Lots of issues
  - ID of individuals
  - Are the individuals subject to the jurisdiction of the forum state?
  - Personal jurisdiction is under attack in the courts
  - The “minimum contacts” yardstick, but note “... peripheral arrangements between parties that involve little communication and minimal obligations are insufficient for personal jurisdiction” (Old Republic Insurance Co. v. Continental Motors 2017)
    - Courts becoming more non-resident defendant-friendly

## ▪ Comity

- A local sovereign is called upon to defer to the self-regulatory judgments of a population partly, but not wholly, composed of its own subjects
  - David Post & David R. Johnson, “Law and Borders – The Rise of Law in Cyberspace”



# CHOICE OF LAW/CONFLICT OF LAW

- **17<sup>th</sup> Century approach to solving conflicts of laws**
  - **All subjects of a government, whether citizens, residents or visitors are subject to that government's laws**  
sovereigns will observe comity as long as it does not cause prejudice to its own government or citizens.
- **First Restatement Approach (First Restatement of Conflicts of Law, § 377 – The Place of the Wrong)**
  - **The place of wrong is in the state where the last event necessary to make an actor liable for an alleged tort takes place (the place where the harmful force takes effect upon the body)**
    - *Rule 4. When a person sustains a loss by fraud, the place of wrong is where the loss is sustained, not where the fraudulent representations are made.*
    - *Rule 5. Where harm is done to the reputation of a person, the place of wrong is where the defamatory statement is communicated. [NB – but consider republication]*

# **SECOND RESTATEMENT APPROACH (RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6)**

- **The most significant relationship**
  - **(1) A court, subject to constitutional restrictions, will follow a statutory directive of its own state on choice of law.**
  - **(2) When there is no such directive, the factors relevant to the choice of the applicable rule of law include**
    - **(a) the needs of the interstate and international systems,**
    - **(b) the relevant policies of the forum,**
    - **(c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue,**
    - **(d) the protection of justified expectations,**
    - **(e) the basic policies underlying the particular field of law,**
    - **(f) certainty, predictability and uniformity of result, and**
    - **(g) ease in the determination and application of the law to be applied.**

# MINIMUM CONTACTS APPROACH

- **Level of contact needed to exercise specific jurisdiction over a defendant – Int’l Shoe Co v. Washington 326 US 310, 316 1945**
  - The burden on the defendant
  - The forum State's interest in adjudicating the dispute
  - The plaintiff's interest in obtaining convenient and effective relief
  - The interstate judicial system's interest in obtaining the most efficient resolution of controversies
  - The shared interest of the several States in furthering fundamental substantive social policies
- **Express-aiming Requirement**
  - Alleged wrongful conduct aimed at a particular forum
  - Targeting, which suggests an intentional selection of a particular plaintiff
  - Knowledge of the plaintiff's location in the forum
- **Notions of territory are not completely irrelevant in cyberspace**
  - Concentrate on the content, not the connection
  - Kleven (116 Mich. L. Rev. 785) suggests assessing minimum virtual contacts by considering a defendant's sophistication and the frequency with which a defendant engages in tortious conduct.

# SVANTESSON'S "NEW FRAMEWORK"

- **Moving from proxy principles to core principles**
  - **The territoriality principle is a proxy principle for core principles**
    - Proxy derived from “The Harvard Draft Convention on Jurisdiction with Respect to Crime” – 1935
- **New Framework**
  - **In the absence of an obligation under international law to exercise jurisdiction, a state may only exercise jurisdiction where:**
    - **There is a substantial connection between the matter and the state seeking to exercise jurisdiction**
    - **The state seeking to exercise jurisdiction has a legitimate interest in the matter, and**
    - **The exercise of jurisdiction is reasonable given the balance between the state's legitimate interests and other interests**

**BREAK**

**Solutions and case examples  
when we return**

# PARTIAL BASIS FOR A SOLUTION

- **Enough similarity and overlap between the physical and the cyberspace that we can apply many physical, or traditional (such as the Common Law) concepts in cyberspace with equal efficacy**
  - Existing or contemplated physical space law is sufficient without modification to address cyberspace
  - Existing or contemplated physical space law may be updated/modified to address cyberspace
  - There is no existing law and new law addressing cyberspace directly must be developed
- **Definition of cyberspace (complex global information infrastructure) that allows us to consider content as well as the “wires”**
- **Express-aiming considerations**
- **Minimum virtual contacts**
- **1<sup>st</sup> Restatement rules 4 and 5**
- **Place of commencement of a wrong and place of its impact**
- **Significant relationship test of the 2<sup>nd</sup> Restatement**

# **MICROSOFT V IO JOHN DOES USING IP ADDRESSES 73.28.34.136 AND 73.156.69.83 – 2017**

- **Action for copyright and trademark infringements**
- **True identities of defendants not known**
- **MS claims:**
  - **The Court has personal jurisdiction over Defendants because they purposefully directed their unlawful activities at Washington**
  - **Defendants activated and attempted to activate at least several thousand copies of Microsoft software, much of which was pirated and unlicensed. During the software activation process, Defendants contacted Microsoft activation servers in Washington over 14,000 times from 2015 to August 2017, and transmitted detailed information to those servers in order to activate the software.**
  - **Defendants' contact with Microsoft's activation servers was voluntary, intentional and comprised a routine part of Defendants' installation of software.**
  - **Defendants expressly aimed their conduct at Washington**

# **TECHNICAL ISSUES — LAW VS TECHNOLOGY**

- **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?**
  - **The “butt-in-the-seat” problem**
- **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”?**

# THE COMPLAINT

- **Seeks relief from the John Does**
- **Second filing (granted) seeks limited expedited discovery against Comcast to identify the Does**
  - **Service cannot be made against unknown defendants**
  - **Plaintiff has demonstrated that:**
    - **(1) the John Doe Defendants are real people and/or entities that may be sued in federal court;**
    - **(2) it has unsuccessfully attempted to identify the John Doe Defendants prior to filing this motion;**
    - **(3) its claims against the John Doe Defendants would likely survive a motion to dismiss; and**
    - **(4) there is a reasonable likelihood that service of the proposed subpoena on Comcast will lead to information identifying the John Doe Defendants.**

# **MICROSOFT CORPORATION V. GLOBAL MEDIA, INC. AND JOHN DOES 1-20 - 2003**

- **Action based upon using Microsoft mail servers to deliver spam**
- **True identities of individual spammers not known but spam provider is alleged to be Global Media, Inc. formerly known as Fluxxx, Inc., a Florida corporation.**
- **Microsoft claims**
  - **Trespass to chattels**
  - **Conversion**
  - **Violations of**
    - **Washington Commercial Electronic Mail Act (RCW Ch. 19.190)**
    - **Washington Consumer Protection Act**
    - **Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030)**

# THE COMPLAINT

- **Trespass to chattels**
  - The servers belong to Microsoft
  - Defendants intentionally trespassed upon Microsoft's property
- **Conversion**
  - Willfully interfered with and converted Microsoft's personal property, as a result of which Microsoft has been deprived of possession and use of its property
- **Violation of the Washington Commercial Electronic Mail Act and the Washington Consumer Protection Act**
  - Defendants initiated the transmission, conspired with one another to initiate the transmission, or assisted in the transmission of commercial e-mail messages from a computer located in Washington and/or to an e-mail address that they knew, or had reason to know, is held by a Washington resident.
    - a) used Microsoft's or another third party's internet domain names without permission;
    - b) misrepresented or obscured information identifying the point of origin or the transmission path of a commercial electronic e-mail message; or
    - c) contained false or misleading information in the subject
- **Violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4)**
  - Knowingly and with intent to defraud, accessed Microsoft's protected computer system, without authorization and/or in excess of authorized access
- **Violation of the federal Computer Fraud and Abuse Act – 18 U.S.C. § 1030(a)(5), (g)**
  - Intentionally and knowingly accessed Microsoft's protected computer system, and knowingly caused the transmission of a program, information, code, or command, without authorization and/or in excess of authorized access

# TAKEAWAYS

- **We need a set of settled, universally-accepted definitions so that we all mean the same thing when we talk about cyberspace.**
- **There is no need to throw out old law and start over — “rip and replace” — but it is counterproductive to “force-fit” old laws to new circumstances in cyberspace just as it is in the physical space**
- **A basic cyber jurisprudence is necessary to establish a basis for discussing law in the cyber space**
- **We can develop an approach to jurisdiction in cyberspace by applying settled principles of law as applicable and updating existing or developing new law where necessary to address our cyber science-related definitions.**

# Questions?

---

# THANK YOU!!