The Intersection of Patent Law and Cybersecurity, Privacy, & Data

Laurie Stempler

Key Technologies

- Data
  - Cloud computing
  - Artificial Intelligence
  - Data storage & mining
- Privacy
  - Internet of Things (“IoT”)
  - Ad tracking / user profiling
- Cybersecurity
  - Multifactor authentication
  - Encryption
  - Biometric technologies (ex: facial recognition)
  - Antivirus software / malware detection

Key Players

- IBM
- Microsoft
- Google
- Facebook
- Apple
- Intel
- Samsung
- Cisco
- Finjan
- Symantec/Broadcom
- Qualcomm
- LG
- Ericsson
- Sophos
- Palo Alto Networks
- McAfee
- Trend Micro
- RSA (Symphony Technology Group)
- Fortinet

Why should patent lawyers pay attention?

Practical Relevance

- **Client impact**: Many of the technical advancements in the areas of data, privacy, and cybersecurity are ripe for patent protection and disputes.
- **Protection**: Lawyers take custody of sensitive, confidential data, so technologies that protect our systems and networks are valuable to us and our clients, particularly in an era of huge data breaches (e.g., Yahoo!, Equifax, Facebook).
- **COVID**: Now more than ever we are dependent on secure, reliable data storage and networks, as we work and communicate from remote locations.
- **Compliance**: When collecting client data, we must be cognizant of our obligations under new data privacy and security regulations, such as GDPR. https://gdpr.eu/what-is-gdpr/

Proposed Legislation and Regulation

- **Consumer Online Privacy Rights Act (COPRA)**
  - Introduced by Senator Cantwell
  - Allows for private enforcement of privacy laws
  - Allows individuals to stop transfer of data, access their own portable data, and delete or correct their data
  - Creates GDPR-like obligations for businesses
  - Does not apply to employee data
- **ePR**
  - Was meant to coincide with GDPR; now expected in 2021
  - Regulates electronic communications within the EU
  - Extends to web messaging, VoIP, web-based email, chats
  - Will likely apply to companies who track individuals, process data from electronic communications, and do electronic direct marketing
  - Same fines as GDPR

Legal Relevance: We've Already Seen It

Notable patent cases from the last five years involving data, privacy, or network security technologies:

- VirnetX v. Apple
- SRI v. Cisco
- Finjan v. Blue Coat
- Symantec v. Zscaler
- Akamai v. Limelight

Legal Relevance: Innovation

- There is significant innovation in data, cybersecurity, and privacy technologies, both in the United States and abroad.
  - Over a ten year period: 48,000 granted patents, 220,000 applications, 97,000 patent families in cybersecurity alone
- China is a leader in filing for global patent protection on cybersecurity.
  - China recently passed the U.S. in number of cybersecurity inventions.
  - Top Chinese companies: Tencent, Alibaba, Huawei, Lenovo
  - China leads in subcategory of authentication
- Top U.S. companies: IBM, Microsoft, Intel, Google
  - U.S. leads in subcategories of secure networks, encryption, secure payments, platform integrity, protecting computer data
- Other top countries in this space: South Korea, Japan

Cybersecurity: A Patent Landscape Report, *available at* https://minesoft.com/wp-content/uploads/2020/03/Full-cybersecurity-report.pdf

Legal Relevance: Innovation

- Artificial Intelligence involves machines processing huge amounts of data to generate solutions.
- The more data you feed a computer, the better its "neural networks" perform.
  - Machine learning is the most common technique featured in AI patent applications.
- Approximately 340,000 AI patent families since 1960
  - Half of all AI patents published 2013 or later
- The U.S. and China are the world leaders in AI innovation.
- IBM and Microsoft are at the patenting forefront among U.S. companies.

WIPO Technology Trends 2019: Artificial Intelligence, *available at* https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

Patentability

35 U.S.C. § 101

"Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title."

35 U.S.C. § 101

- Patents that relate to technologies in the cybersecurity, privacy, and data space are vulnerable to Section 101 challenges.
- Over the past 12 months, the Federal Circuit issued nearly three dozen decisions on Section 101 eligibility.
  - Over half of those cases involved patented technology that fell into the category of data, privacy, or cybersecurity.
  - The Federal Circuit found that the claimed subject matter was not ineligible in only three instances.

Ancora Technologies, Inc. v. HTC America, Inc.

Technology: software verification method that stores license verification information in a modifiable, erasable part of the computer BIOS

1. A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:

selecting a program residing in the volatile memory,

using an agent to set up a **verification structure in the erasable, non-volatile memory of the BIOS**, the verification structure accommodating data that includes at least one license record,

verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and

acting on the program according to the verification.

Ancora Technologies, Inc. v. HTC America, Inc.

- Claimed invention passed *Alice* Step One
  - "**Improving security**—here, against a computer's unauthorized uses of a program—can be a non-abstract computer-functionality improvement if done by a **specific technique** that **departs from earlier approaches** to solve a **specific computer problem**."

    908 F.3d 1343, 1348 (Fed. Cir. 2018)

  - Claims covered a **specific** way to improve security in an **unexpected** way: by storing "verification structure" in modifiable portion of BIOS

    Id. at 1348-49

  - Invention reduced vulnerability to hacking

    Id. at 1349

Uniloc USA, Inc. v. LG Electronics USA, Inc.

Technology: communication system that allows fixed device to identify and poll mobile device (e.g., computer mouse) simultaneously

2. A primary station for use in a communications system comprising at least one secondary station, wherein means are provided
for broadcasting a series of inquiry messages, each in the form of a plurality of predetermined data fields arranged according to a first communications protocol, and
for **adding to each inquiry message prior to transmission an additional data field for polling** at least one secondary station.

Uniloc USA, Inc. v. LG Electronics USA, Inc.

- Claimed invention passed *Alice* Step One
  - "[T]he claims at issue are directed to a patent-eligible improvement to computer functionality, namely the reduction of latency experienced by parked secondary stations in communication systems."

    957 F.3d 1303, 1307 (Fed. Cir. 2020)

  - The claimed step of inquiring ***and*** polling parked secondary stations was a "change in the manner of transmitting data [that] results in reduced response time by peripheral devices."

    Id. at 1308

Dropbox, Inc. v. Synchronoss Technologies, Inc.

Technology of the ’505 patent: secure data delivery

1. Apparatus that provides an information resource in response to a request from a user, the request including an identification of the user according to a mode of identification and the apparatus comprising:

access control information including

a sensitivity level associated with the resource and

a trust level associated with the mode of identification; and

an **access checker which permits the apparatus to provide the resource only if the trust level for the mode of identification is sufficient for the sensitivity level of the resource**.

Dropbox, Inc. v. Synchronoss Technologies, Inc.

- The "access checker" is a "functional abstraction" and is a "black box" in the specification.

Nos. 2019-1765, -1767, -1823, 2020 WL 3400682, at *3 (Fed. Cir. June 19, 2020)

- It is not enough to state that the invention solves a technological problem; the patent must describe **how** it solves the problem, and the solution must be in the claims.

Id. at *4

- "[T]he claims recite the application of an abstract idea using conventional and well-understood techniques specified in broad, functional language."

Id.

Dropbox, Inc. v. Synchronoss Technologies, Inc.

Technology of the ’399 patent: synchronized file uploading

1. A method of synchronizing an interactive connection and a non-interactive data transfer connection between a client and a service provider, comprising:

creating an interactive connection;

creating a data transfer connection; and

generating a **single session ID** for the two connections, which ID associates between the two connections.

25. Apparatus for uploading data files, comprising:

a file upload connection server;

an interactive connection server; and

a **synchronizer which synchronizes the operation** of respective connections formed by the file upload connection server and by the interactive connection server.

Dropbox, Inc. v. Synchronoss Technologies, Inc.

- Neither the single session ID nor the synchronizer are non-abstract improvements.

Nos. 2019-1765, -1767, -1823, 2020 WL 3400682, at *6 (Fed. Cir. June 19, 2020)

- The claims are directed to functional results, not specific techniques for synchronized file uploads.

Id.

- The claims do not recite an inventive concept because they "merely apply an abstract idea using conventional and well-understood techniques."

Id.

Dropbox, Inc. v. Synchronoss Technologies, Inc.

Technology of the ’541 patent: data storage for mobile device

1. A method for backing up data stored on a mobile customer premises equipment comprising the steps of:

storing data at the mobile customer premises equipment;

formatting the data stored at the mobile customer premises equipment into fields by determining data fields, identifying which portions of said data correspond to a respective data field, and **tagging said data**[;]

transmitting the data with a user ID from the mobile customer premises equipment across a mobile network to a server for storage;

retrieving said data from said server across a mobile network in response to one of an expiration of time and request from said mobile customer premises equipment by transmitting said data to said mobile customer premises equipment; and

transmitting said data to said mobile customer premises equipment by transmitting the data in more than one information signal and sequentially numbering each of said information signals.

Dropbox, Inc. v. Synchronoss Technologies, Inc.

- Drobox identified the unified tag and data structure and the remote server synchronization for data backup as the claimed advances, but those concepts are abstract.
  - The District Court said this is the same as a person manually transferring data.

Nos. 2019-1765, -1767, -1823, 2020 WL 3400682, at *7 (Fed. Cir. June 19, 2020)

- Formatting, tagging, transmitting, and retrieving data are "generalized steps to be performed on a computer using conventional computer activity."

Id.

- The patent disclosed that the data structure and remote server synchronization were routine and conventional.

Id. at *8

101 Vulnerability in Data, Privacy, and Cybersecurity Patents

- Including only a “black box” disclosure of the allegedly inventive aspect of a claimed computer security functionality
  - In *Dropbox*, having an “access checker” was not enough because the patent did not describe how it worked to clear security for the user to access a protected resource.
- Reciting results of the claimed improvement in security or data management rather than the solution
  - In contrast, reduced latency was achieved in the *Uniloc* invention by the claimed inclusion of a polling step with the inquiry step.
- Omitting specificity from the claimed solution, which raises preemption concern
  - In contrast, *Ancora* included the specific solution of storing a verification structure in a modifiable section of the BIOS.

Inventorship

35 U.S.C. § 115

"An application for patent that is filed under section 111(a) or commences the national stage under section 371 shall include, or be amended to include, **the name of the inventor for any invention claimed in the application**. Except as otherwise provided in this section, **each individual** who is the inventor or a joint inventor of a claimed invention in an application for patent **shall execute an oath or declaration** in connection with the application."

35 U.S.C. § 115 (a)

"An oath or declaration under subsection (a) shall contain statements that (1) the application was made or authorized to be made by the affiant or declarant; and (2) such individual **believes himself or herself** to be the original inventor or an original joint inventor of a claimed invention in the application."

35 U.S.C. § 115 (b)

35 U.S.C. § 100

"The term 'inventor' means the individual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention."

35 U.S.C. § 100(f)

DABUS

- DABUS: Device for the Autonomous Bootstrapping of Unified Sentience
  - Created by Dr. Stephen Thaler of Imagination Engines, Inc.
  - Consists of artificial neural networks, one of which generates ideas and one of which critiques and identifies novel ideas
- DABUS's claimed inventions:
  - Food/Beverage container
  - Light that flashes at a pulse optimized to be noticeable to humans
- Patent applications listed DABUS as the inventor and identified Stephen Thaler as the legal representative and assignee

http://artificialinventor.com/patent-applications/

DABUS's Patent Application

- PTO issued a Notice to File Missing Parts of Nonprovisional Application and refused to vacate the notice
- Artificial Inventor Project, which is committed to establishing inventorship rights for artificial intelligence, petitioned for review of PTO's refusal to vacate the Notice
- Petitioner argued that DABUS had (1) independently created the invention and (2) identified it as novel
- Petitioner also advanced policy arguments in support of naming AI as an inventor:
  - Encourage innovation through AI
  - Reduce incidence of improper naming of inventors
  - Fulfill public notice function by identifying true inventor

U.S.P.T.O. Decision

- PTO disagreed with petitioners
  - The statutory language uses words like “whoever,” “himself,” “herself,” and “person.”
  - The Federal Circuit said an inventor must be a natural person because conception is a “mental act.” *Univ. of Utah v. Max-Planck-Gesellschaft zur Forerung der Wissenschaften e.V.*, 734 F.3d 1315 (Fed. Cir. 2013).
  - The Code of Federal Regulations refers to inventors as “persons.”
  - The MPEP describes conception as a “mental part of the inventive act” and refers to the “mind of the inventor.”

Decision on Petition, Application No. 16/524,530, 4-6 (Feb. 17, 2020).

U.S. patent law does not permit a machine to be named as the inventor in a patent application.

Id. at 6.

EPO Decision

- Legislative history confirms that an inventor is a natural person.
- There is no legislation that would enable AI to be considered a “legal person” (as opposed to a natural person).
- The international standard is that the inventor is a natural person.
- DABUS does not own rights and thus could not transfer ownership rights to the applicant.
- Formal requirements, like naming the inventor, are separate and considered apart from substantive requirements in a patent application.

Grounds for Decision, Application No. 18 275 163.6 (Jan. 27, 2020)

UK IPO Decision

- The IPO accepted that DABUS invented the claimed subject matter in the applications.
- An inventor must be a human and cannot be an AI machine.
- DABUS cannot own the IP, so DABUS could not have assigned the patent to DABUS's owner.
- "[I]nventions created by AI machines are likely to become more prevalent in future and there is a legitimate question as to how or whether the patent system should handle such inventions."

Decision, GB1816909.4, GB1818161.0 (Dec. 4, 2019)

Should We Name AI as an Inventor?

- Arguments for naming AI as inventor
  - Reflect true inventor and combat devaluing inventorship
  - Improve efficiency through AI, which may soon outpace humans in researching and processing ideas
  - Incentivize people to do innovative work using AI
  - Protect innovation of small and large companies alike
- Arguments against naming AI as inventor
  - AI not yet advanced enough; just a tool
  - Complicates analysis of the right level of ordinary skill in the art and whether an invention is obvious under 35 U.S.C. § 103 to "persons" of ordinary skill in the art
  - AI cannot own the claimed invention, making assignment difficult or impossible

What’s next?

For Further Discussion

- Should we have a separate set of patent laws for AI?
- How does Section 101 eligibility impact patent applications for AI-related technologies?
- Relief
  - Should injunctive relief be more difficult to obtain against cybersecurity or data privacy companies?
  - What are the benefits and drawbacks of placing a high value technology that keeps our data networks private and secure?
- What lessons have we learned from the global pandemic about the data, privacy, and cybersecurity space?
  - Where are the greatest vulnerabilities?
  - What are the most valuable ways we can harness technologies in this space for productive, safe, remote work?

Companies and Technologies to Watch

- Winston, by Winston Privacy
  - Plug in between modem and router to block tracking of browsing, block cookies, update firmware, and disguising IP address
- Avast Omni by Avast
  - Plug into home router to monitor data being exchanged with connected devices for unusual or threatening activity
- AT.Wallet by AuthenTrend Technology Inc.
  - "Fingerprint enabled Cryptocurrency Wallet"
- Mudi, by GL Technologies
  - Portable, secure router for travelers
- Keymo, by Bystamp
  - Personal, electronic stamp for authentication that does not require network connection

https://www.ces.tech/search-results.aspx?searchtext=cybersecurity%20and%20privacy&searchmode=anyword