CINDY A. COHN (California Bar No. 145997)
cindy@eff.org
JENNIFER STISA GRANICK (California Bar No. 168423)
jennifer@eff.org
MARCIA HOFMANN (California Bar No. 250087)
Marcia@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x134
Fax: (415) 436-9993 (fax)

Attorneys for *Amicus Curiae*
Electronic Frontier Foundation

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FACEBOOK, Plaintiff, v. POWER VENTURES, Defendant.	Case No. 5:08-cv-05780 JW **DECLARATION OF SETH SCHOEN IN SUPPORT OF BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT POWER VENTURES' MOTION FOR SUMMARY JUDGMENT ON CAL. PENAL CODE 502(C)** Date: June 7, 2010 Time: 1:30 p.m. Dep't: Hon. Judge James Ware

I, Seth Schoen, declare as follows:

1. I am Senior Staff Technologist at the Electronic Frontier Foundation (EFF). I make this declaration based on my own personal knowledge from over 16 years of familiarity with Internet protocols. I believe the information presented in this declaration is generally known to computer scientists and to others familiar with the operations of the Internet.

2. An Internet protocol address ("IP address") is a numeric value used to identify a computer or set of computers on the Internet. Internet routers use the IP address to decide where to send communications addressed to a particular computer.[1] The address is normally written as four

[1] Eric A. Hall, *Internet Core Protocols: The Definitive Guide*, 37-40 (O'Reilly and Associates,

numbers separated by periods.[2] For example, one of the web servers operated by *amicus* uses the address 64.147.188.11, while this Court's web server uses 207.41.19.17.

3. IP addresses are allocated to Internet service providers (ISPs) in chunks of consecutive addresses out of a worldwide pool of around four billion possible addresses through geographically-based non-profit organizations known as regional Internet registries.[3] ISPs can further delegate these addresses to smaller entities such as businesses, Internet cafés, or smaller ISPs.[4] ISPs can also assign an IP address directly to an individual computer. This assignment process is frequently automated and the assignment can be short- or relatively long-term.[5]

4. Because IP addresses are allocated in this way, they can convey approximate and general information about a computer's location, how the computer is connected to the Internet or what individual or entity is using that computer to connect.[6] But it is equally true that the IP address used by a particular computer can change over time, that individual users connect through different IP addresses depending on where they are, and that multiple users can connect to the Internet through a single IP address.[7]

5. For instance, a laptop will receive a different IP address when it connects to the

---

2000).

[2] *See* Radia Perlman, *Interconnections Second Edition,* 199 (Addison Wesley Longman, 2000).

[3] *See* American Registry for Internet Numbers, "Internet Number Resource Distribution", available at https://www.arin.net/knowledge/distribution.pdf.

[4] Hall, *supra* note 1, at 40-41.

[5] *See* Wikipedia, "IP Address: Static vs dynamic IP addresses", version of June 17, 2010, available at http://en.wikipedia.org/w/index.php?title=IP_address&oldid=368588938#Static_vs_dynamic_IP_addresses.

[6] *See* Kevin F. King, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies," available at http://ssrn.com/abstract=1622411 (cited here for its clear description of the relationship between IP address and location, but not for its legal conclusions).

[7] *See* Yinglian Xie *et al.*, "How Dynamic Are IP Addresses?", in *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, available at http://*www.sigcomm.org/ccr/drupal/files/fp179-xie.pdf,* and Jeff Tyson, "How Network Address Translation Works", available at http://computer.howstuffworks.com/nat.htm/printable.

Internet from different locations.[8] If a laptop's owner uses the machine from her workplace in the morning, a café in the afternoon, and her home in the evening, she will present at least three different IP addresses over the course of a single day. A traveler who brings a laptop to a different city and goes online there will receive an IP address unrelated to the IP address he used at home. So will an Internet user who chooses to change residential broadband providers – for example, by switching from Comcast to AT&T. Even a home Internet user may encounter an IP address that changes over time, since many ISPs vary the address that they assign to a particular computer on different occasions.[9] America Online, for instance, provides a different, randomly selected IP address to every user with each new telephone modem dial-up session.[10]

6. Some common Internet technologies such as tunnels, virtual private networks ("VPNs"), and proxy servers will also change the apparent IP address that a user appears to be connecting from.[11] Users have many legitimate reasons to use technologies that will change their apparent IP address.[12]

7. Most network routers, firewalls, and Internet server software provide simple, straightforward "IP blocking" features.[13] That is, a computer or network can be configured to

---

[8] *See* University of Illinois Campus Information Technologies and Educational Services, "Network Access While Traveling," available at http://www.cites.illinois.edu/network/access/travel.html.

[9] *See* Whatismyipaddress.com, "Dynamic IP Addressing," available at http://whatismyipaddress.com/dynamic-static, and Xie *et al.*, note 7, *supra*.

[10] *See* Wikimedia Foundation, "Why are AOL users often blocked?," available at https://en.wikipedia.org/wiki/Wikipedia:AOL#Why_are_AOL_users_often_blocked.3F, and AOL, "AOL Outbound Mail Server Hostnames and IPv4 Addresses," available at http://postmaster.aol.com/Postmaster.OMRs.html.

[11] *See* eHow.com, "How to Change Your IP Address," available at http://www.ehow.com/how_2352631_change-ip-address-multiple-methods.html; University of California at Los Angeles, "Bruin OnLine Proxy Server," available at http://www.bol.ucla.edu/services/proxy/; Stanford University Information Technology Services, "VPN Virtual Private Network," available at http://itservices.stanford.edu/service/vpn.

[12] *See generally* Testimony of Seth Schoen before the United States Sentencing Commission (March 17, 2009), available at http://www.ussc.gov/AGENDAS/20090317/Schoen_testimony.pdf (describing use of proxy servers and virtual private networks for computer security and privacy reasons, and as a means of proving entitlement to access subscription-based resources).

[13] *See* Wikipedia, "Blacklist (computing)," version of June 13, 2010, available at

discard or ignore all communications from a particular IP address. A server operator could use this as a way to reduce unwanted Internet traffic based on her belief that particular IP addresses are associated with a greater likelihood of undesired activity, such as spam email.[14] The operator could choose to use this ability to refuse communications with a particular computer, with a particular ISP, or with an entire geographic area, such as a country.[15] If a computer has been configured to "block" an IP address or addresses, it will either return an error in response to communications from those addresses (for instance, stating that a web site is unavailable), or simply ignore those communications entirely, making no reply to them.[16]

8. Because it is so easy for a user to change her IP address, system administrators know that this kind of blocking is a rather rough and easily ignored tool for limiting Internet connections.[17] Requiring a username and password, for example, as Facebook does, is a far more robust and direct way of distinguishing between authorized and unauthorized users.

9. Internet users who find their computers blocked from accessing a particular service might have many reasons to try to circumvent the restriction – which could often mean doing something as simple as trying again from a different place. For instance, an employer might have a policy that a certain service may be accessed only from certain recognized locations. This policy could be implemented by blocking all unknown IP addresses; an employee traveling to a new location could use a proxy or VPN service to change the apparent IP address from which the service was accessed. Or an American bank's anti-fraud measures could categorically forbid

---

http://en.wikipedia.org/w/index.php?title=Blacklist_(computing).

[14] *See* dnsbl.info, "What is a DNSBL?," available at <http://www.dnsbl.info/ (describing publicly-available blacklist databases of IP addresses alleged to have been the origin of large numbers of unwanted spam messages).

[15] *See* Wikipedia, "IP blocking," version of June 10, 2010, available at http://en.wikipedia.org/w/index.php?title=IP_blocking&oldid=367115237.

[16] *See*, e.g., "Yahoo Help, IP Address Blocking," available at http://help.yahoo.com/l/us/yahoo/smallbusiness/store/risk/risk-17.html.

[17] *See* Simson Garfinkel and Gene Spafford, *Practical Unix and Internet Security*, 484 (O'Reilly and Associates, 1996) ("Restricting a service by IP address or hostname is a fundamentally unsecure way to control access to a server."). *See also* Yahoo, *supra,* note 16 (describing possibility of evading IP address blocks and possibility that IP address blocks will be ineffective due to dynamic allocation of addresses by ISPs).

access to online banking services from certain foreign countries with no known customers and a high incidence of fraud; this blocking could be implemented by blocking all IP addresses associated with those countries.[18] A legitimate customer of the bank, frustrated at the inability to log on to the bank's web site during a trip, could use a proxy or VPN service to bypass the restriction by appearing to connect from a U.S.-based IP address.

10. More trivially, an email service might refuse to accept any messages from IP addresses associated with a particular hotel, because guests staying in that hotel had previously sent large amounts of unwanted spam email. An innocent guest could be prevented from sending legitimate email to the service as a result, but could readily avoid this restriction by using a proxy or a VPN.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct to the best of my knowledge, and that this document was executed in San Francisco, California.

DATED: June 21, 2010

Respectfully submitted,

/s/ Seth Schoen

Seth Schoen

[18] *See* Wikipedia, "IP blocking," version of June 19, 2010, http://en.wikipedia.org/w/index.php?title=IP_blocking&oldid=368931563 (suggesting that some services may forbid all access to Nigerian IP addresses because of high rates of fraud associated with Nigeria); Yahoo, *supra,* note 16 (mentioning prospect of blocking "a high-risk country or organization" by IP address, with associated risks of excluding legitimate users who share an IP address or address range).