Jennifer Lynch (SBN 240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Jason M. Schultz (SBN 212600)
jschultz@law.berkeley.edu
Lila I. Bailey (SBN 238918)
lbailey@law.berkeley.edu
Aaron Mackey (Application for Student Practice Pending)
Jose de Wit (Application for Student Practice Pending)
SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
U.C. Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-1957
Facsimile: (510) 643-4625

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ELECTRONIC FRONTIER FOUNDATION,

Plaintiff,

v.

DEPARTMENT OF DEFENSE, *et al.*,

Defendants.

Case No. 09-cv-05640-SI

DECLARATION OF JENNIFER LYNCH IN SUPPORT OF PLAINTIFF'S CROSS MOTION FOR SUMMARY JUDGMENT AND OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Date: Friday, Jan. 13, 2012
Time: 9:00 a.m.
Place: Courtroom 10, 19th Floor
Judge: Hon. Susan Illston

DECLARATION OF JENNIFER LYNCH

1. I am an attorney of record for Plaintiff Electronic Frontier Foundation ("EFF") in this matter. I am a member in good standing of the California State Bar, and am admitted to practice before this Court. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

2. EFF is a nonprofit corporation established under the laws of the Commonwealth of Massachusetts with offices in San Francisco, California and Washington, D.C. EFF is a donor-supported membership organization that works to inform policymakers and the general public about civil liberties issues related to technology, and to act as a defender of those liberties. In support of its mission, EFF uses the Freedom of Information Act ("FOIA") to obtain and disseminate information concerning the activities of federal agencies.

3. Plaintiff EFF filed this lawsuit in order to bring greater transparency to law enforcement's use of online social networking.

4. Plaintiff's FOIA request for records at issue in this case was prompted by a number of media reports discussing law enforcement's use of online social networks, such as Facebook and MySpace, in the course of their investigations.

5. On October 7 and 8, 2009, EFF sent FOIA requests to the defendant federal agencies, including the Department of Homeland Security ("DHS") and two of its components, the Secret Service and Immigration and Customs Enforcement ("ICE"), as well as two Department of Justice components, the Criminal Division ("DOJ") and the Federal Bureau of Investigation ("FBI").

6. EFF requested eight categories of records related to "federal guidelines on the use of social-networking websites (including but not limited to Facebook, MySpace, Twitter, Flickr and other online social media sites) for investigative or data gathering purposes created since January 2003." Attached as Exhibit 1 are true and correct copies of EFF's FOIA requests. After exhausting its administrative remedies, EFF sued.

7. Attached hereto as Exhibit 2 are true and correct copies of several news articles that supported Plaintiff's FOIA requests: Gene Johnson, *Fraud Fugitive Busted After Unwise Friend*

Request, Associated Press, Oct. 13, 2009; Ryan Singel, *FBI Investigated Coder for Liberating Paywalled Court Records,* Wired, Oct. 5, 2009, available at http://www.wired.comlthreatlevel/2009110/swartz-fbi/; *Wanted by the FBI*, Raw Thought, http://www.aaronsw.comlweblog/ (Oct. 5, 2009); Colin Moynihan, *Arrest Puts Focus on Protesters' Texting,* N.Y. Times, Oct. 5, 2009, at A19; Alexandra Topping, *International: Facebook habit proves fugitive's undoing*, The Guardian (London), Oct. 15, 2009.

8. Attached hereto as Exhibit 3 is a screen capture of Facebook's website that discusses the site's user statistics. The page can be found at http://www.facebook.com/press/info.php?statistics.

9. The Department of Defense; Central Intelligence Agency; Department of the Treasury; Office of the Director of National Intelligence; Bureau of Alcohol, Tobacco, Firearms and Explosives; and Executive Office for United States Attorneys were later dismissed from this action. *See* Dkt. Nos. 15 at 3; 42; 49.

10. In preparation for the government's Motion for Summary Judgment, EFF agreed to waive challenges to information withheld under Exemptions 1, 6, 7(C) (in conjunction with 6) or low 2. *See* Email from Jennifer Lynch to Defense Counsel Kimberly Herb dated Oct. 17, 2011 and attached as Exhibit 4. EFF has also waived challenges to documents withheld under Exemption 7(D).

11. Attached hereto as Exhibit 5 is a true and correct copy of the document *How to Effectively Search MySpace.com: A Guide for Investigators*, available at http://cryptocomb.org/MySpace-How%20to%20Search.pdf (last visited on Oct. 29, 2011). Students at the Samuelson Clinic assisting me in this case found the document after performing a Google search. The DOJ has withheld it in full.

12. Attached hereto as Exhibit 6 is a true and correct copy of a record DHS released in this case entitled "Social Networking Monitoring Center (SNMC) Concept of Operations for the Presidential Inauguration Operational Phase Friday, 1/16/2009 through Wednesday, 1/21/2009."

13. Attached hereto as Exhibit 7 are true and correct copies of several media reports

outlining law enforcement's efforts to monitor social networking sites for criminal activity: Chris Morran, *NYPD Forms New Unit to Monitor Facebook and Twitter For Signs of Criminal Activity*, The Consumerist (August 10, 2011), available at http://consumerist.com/2011/08/nypd-forms-new-unit-to-monitor-facebook-and-twitter-for-signs-of-criminal-activity.html; Michael Miller, *Facebook posts help police track down suspects in Ocean City skate-park theft*, Press of Atlantic City (Oct. 28, 2011), available at http://www.pressofatlanticcity.com/news/facebook-posts-help-police-track-down-suspects-in-ocean-city/article_2e4f81cc-01c3-11e1-bdb3-001cc4c03286.html; *Use of Social Networking Sites in Investigations*, Wikipedia, available at http://en.wikipedia.org/wiki/ Use_of_social_network_websites_in_investigations (last visited Oct. 29, 2011); *Police use Flickr to identify London riot suspects*, available at http://thenextweb.com/uk/2011/08/09/police-use-flickr-to-identify-london-riot-suspects/ (last visited Nov. 11, 2011).

14. Attached hereto as Exhibit 8 is a true and correct copy of a screen capture of the online video *CIA's 'Facebook' Program Dramatically Cuts Agency's Costs*, which is available for viewing at http://www.theonion.com/video/cias-facebook-program-dramatically-cut-agencys-cos,19753/.

15. Attached hereto as Exhibit 9 is a true and correct copy of an article discussing how individuals lie when they are online: danah boyd, *et al*., *Why Parents Help Their Children Lie to Facebook About Their Age: Unintended Consequences of the 'Children's Online Privacy Protection Act,'* First Monday, Vol. 6, No. 11-7 (November 2011), available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075.

16. Attached hereto as Exhibit 10 is a true and correct copy of a news story detailing law enforcement's use of pretext in investigations: Simma Aujla, *Police Officers Set Up Facebook Account to Catch Underage Drinkers*, The Chronicle of Higher Education (Dec. 8, 2009), available at http://chronicle.com/blogs/wiredcampus/police-officers-set-up-facebook-account-to-catch-underage-drinkers/9103.

17. Attached hereto as Exhibit 11 are true and correct copies of news articles describing pretextual techniques used by law enforcement agents to investigate crime: Laura Sanders, *Is 'Friending' in Your Future? Better Pay Your Taxes First*, The Wall Street Journal, available at http://online.wsj.com/article/SB125132627009861985.html (Aug. 27, 2009); Julie Masis, *Is This Lawman Your Facebook Friend?*, The Boston Globe (Jan. 11, 2009), available at http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend/?s_campaign=8315; Cyndy Aleo-Carreira, *Police Use Social Networks, Fake Profiles in Investigations*, PC World (Jan. 12, 2009), available at http://www.pcworld.com/businesscenter/article/156999/police_use_social_networks_fake_profiles_in_investigations.html.

18. Attached hereto as Exhibit 12 is a true and correct copy of a record released by the IRS in response to EFF's FOIA request that discusses online techniques for monitoring delinquent taxpayers, including using social networking sites to determine a target's occupation. *IRT – WBT Content 2009*, available at https://www.eff.org/files/filenode/social_network/training_course.pdf.

19. Attached hereto as Exhibit 13 is a true and correct copy of a record released by the U.S. Citizenship and Immigration Services in response to EFF's FOIA request that describes efforts by the agency to verify a person's marital status by "friending" the individual on Facebook. *Social Networking Sites and Their Importance to FDNS*, available at https://www.eff.org/files/filenode/social_network/DHS_CustomsImmigration_SocialNetworking.pdf.

20. Attached hereto as Exhibit 14 is a true and correct copy of the transcript of an episode of the MSNBC television show *To Catch a Predator*, available at http://www.msnbc.msn.com/id/22423433/ns/dateline_nbc-to_catch_a_predator/#.TsVSZ8Mk6so.

21. Attached hereto as Exhibit 15 is a true and correct copy of a news article describing law enforcement's general use of social networks to monitor criminals online, including using location information to track down a suspect: Alice Lipowicz, *For law enforcement, social media can cut both ways*, Government Computing News (April 8, 2011), available at http://gcn.com/articles/2011/04/05/law-enforcement-agencies-usiing-social-media-to-bust-gangs.aspx.

22. Attached hereto as Exhibit 16 are true and correct copies of news articles describing how location information published on social networking sites can be used by law enforcement: Annie Blanco, *Italian Police use Facebook to Catch Mafia Thug*, Home Security Store, available at http://www.homesecuritystore.com/blog/2010/03/17/italian-police-use-facebook-to-catch-mafia-thug/; Dan Fletcher, *Please Rob Me: The Risks of Online Oversharing*, Time (Feb. 18, 2010) available at http://www.time.com/time/business/article/0,8599, 1964873,00.html.

23. Attached hereto as Exhibit 17 is a true and correct copy of a screen capture of the website GitHub, which describes and makes publicly available for download a geolocation aggregator known as "Creepy." The program is available at http://ilektrojohn.github.com/creepy/.

24. Attached hereto as Exhibit 18 is a true and correct copy of a recent news article that reports on how the CIA compiles information from social networking websites such as Twitter to gain intelligence and predict future behavior. Kimberly Dozier, *AP Exclusive: CIA Tracks revolt by Tweet, Facebook*, Associated Press (Nov. 4, 2011), available at http://hosted.ap.org/dynamic/stories/U/US_CIA_SOCIAL_MEDIA?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT.

25. Attached hereto as Exhibit 19 is a true and correct copy of a record that the CIA released in response to EFF's FOIA request that details its efforts to mine social networking websites for information on individuals and criminal activity.

26. Attached hereto as Exhibit 20 is a true and correct copy of FBI Bates Nos. 1-4, released in response to EFF's FOIA request that describes the agency's interest in a University of Arizona program that purports to predict future terrorist behavior.

27. Attached hereto as Exhibit 21 are true and correct copies of articles discussing a process called "doxing," which is used to compile personal information on individuals via social media. *Doxing — Hackers Information Gathering Technique*, Hacker's Lodge (July 31, 2011), available at http://lodge4hacker.blogspot.com/2011/07/doxing-hackers-information-gathering.html; Peter Bright, *Dox everywhere: LulzSec under attack from hackers, law enforcement*, available at http://arstechnica.com/security/news/2011/06/dox-everywhere-lulzsec-under-attack-from-hackers-law-enforcement.ars.

28. Attached hereto as Exhibit 22 is a true and correct copy of an article that describes the investigative technique known as "sniffing," where technology is used to monitor the electronic communications and activities of individuals on a particular computer or network: Matthew Tanase, *Sniffers: What They Are and How to Protect Yourself*, Symantec (Feb. 26, 2002), available at http://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself.

29. Attached hereto as Exhibit 23 is a true and correct copy of an article about the history of email, describing how email first became commercially available in 1988 and became widespread after 1993. Dave Crocker, *Email History*, The World's First Web Published Book (last visited Nov. 16, 2011), available at http://www.livinginternet.com/e/ei.htm.

30. Attached hereto as Exhibit 24 is a true and correct copy of a blog post describing an Oakland Police Department Officer's alleged infiltration of the Occupy Oakland Movement: Robert Mackey, *Police Officer Accused of Infiltrating Occupy Oakland Says He Supports the Movement*, The New York Times "The Lede" blog (Nov. 14, 2011), available at http://thelede.blogs.nytimes.com/2011/11/14/police-officer-accused-of-infiltrating-occupy-oakland-says-he-supports-the-movement/.

31. Attached hereto as Exhibit 25 are true and correct copies of the following publicly available search warrants and supporting applications and affidavits, which describe in detail federal investigations into users of the social networking websites Facebook and MySpace: Application and Affidavit for Search Warrant, *U.S. v. FaceBook User ID 1562893877*, No. 4:09-mj-00036-RKS (D. Mont. Aug. 3, 2009), ECF No. 1; Application & Affidavit for Search Warrant, *U.S. v. MySpace Account:www.MySpace.com/NCSVA, ID 60577378*, No. 7:09-mj-00306-mfu (W.D. Va. July 24, 2009), ECF No. 1; Application and Affidavit for Warrant, *U.S. v. Facebook User ID 100000606062410 (Eric Kemper)*, No. 3:11-mj-00535-AJB (S.D. Cal. Feb. 11, 2011), ECF No. 1; Search Warrant Application, *U.S. v. MySpace account "Timberlinebombinfo,"* No. 3:07-mj-05114-JPD (W.D. Wash. June 12, 2007), ECF No. 1; Application & Affidavit for Search Warrant, *U.S. v. MySpace Account of Jeffrey Scott Easley*, No. 7:10-mj-00409-mfu (W.D. Va. Jan. 14, 2011), ECF No. 5. Students at the Samuelson Clinic assisting me in this case found these

affidavits through PACER searches.

32. Attached hereto as Exhibit 26 is a true and correct copy of a sample DOJ search warrant affidavit template that is publicly available on the agency's website. Appendix F, *Sample Premises Computer Search Warrant Affidavit*, of the document *Searching and Seizing Computers and Obtaining Electronic Evidence Manual*, available at http://www.cybercrime.gov /ssmanual/06ssma.html. This document is publicly available on the DOJ's cybercrime information website, www.cybercrime.gov.

33. Attached hereto as Exhibit 27 is a true and correct copy of a screen capture of ICE's Homeland Security Investigations website (noting that the agency has 6,700 special agents), which is publicly available at http://www.ice.gov/about/offices/homeland-security-investigations/.

34. Attached hereto as Exhibit 28 is a true and correct copy of a news article describing ICE's use of social networking website Multiply.com to investigate an online child pornography ring: Rich Lord, *Dozens sent to prison for trading child porn online*, Pittsburgh Post-Gazette (May 13, 2011), which is available at http://www.post-gazette.com/pg/11133/1146192-53-0.stm?cmpid=nationworld.xml.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Signed this 17th day of November, 2011.

/s/ Jennifer Lynch
Jennifer Lynch, Esq.