

epic.org

July 10, 2012

VIA CERTIFIED MAIL

Mary Ellen Callahan
Chief Privacy Officer/Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
245 Murray Drive SW, Building 410
STOP-0655
Washington, D.C. 20528-0655

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

Re: Freedom of Information Act Request

To Whom it May Concern:

This letter constitutes a request under the Freedom of Information Act.¹ This request is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the Department of Homeland Security (“DHS”).

Background

On March 9, 2006, the National Communications System (“NCS”) approved Standard Operating Procedure (“SOP”) 303, however it was never released to the public.² This secret document codifies a “shutdown and restoration process for use by commercial and private wireless networks during national crisis.”³ In a 2006-2007 Report, the President’s National Security Telecommunications Advisory Committee (“NSTAC”) indicated that SOP 303 would be implemented under the coordination of the National Coordinating Center (“NCC”) of the NSTAC, while the decision to shut down service would be made by state Homeland Security Advisors or individuals at DHS.⁴ The report indicates that NCC will determine if a shutdown is necessary based on a “series of questions”.⁵

On July 3, 2011, a Bay Area Rapid Transit (“BART”) officer in San Francisco shot and killed a homeless man, Charles Hill.⁶ The officer alleged later that Hill had

¹ 5 U.S.C. § 552 (2011).

² National Security Telecommunications Advisory Committee, NSTAC Issue Review 2006-2007 (2007), available at <http://www.ncs.gov/nstac/reports/2007/2006-2007%20NSTAC%20Issue%20Review.pdf>, at 139.

³ *Id.* at 139.

⁴ *Id.* at 139-40.

⁵ *Id.* at 139.

⁶ *BART Protests: San Francisco Transit Cuts Cellphones to Thwart Demonstrators; First Amendment Debate*, Ned Potter, ABC News, Aug. 16, 2011 <http://abcnews.go.com/Technology/bart-protest-san-francisco-transit-cut-cellphones-prevent/story?id=14311444#.T9jZlvF2m5Y>.

attacked him with a knife and that he had acted in self-defense.⁷ The death sparked a major protest against BART on July 11, 2011.⁸ Though the protests disrupted service at several transit stations, no one was injured.⁹ A second protest was planned one month later, but was cut short after BART officials cut off all cellular service inside four transit stations for a period of three hours.¹⁰ This act prevented any individual on the station platform from sending or receiving phone calls, messages, or other data.¹¹

The incident with BART has set off a renewed interest in the government's power to shut down access to the Internet and other communications services.¹² A 2011 Report from the White House asserted that the National Security Council and the Office of Science and Technology Policy have the legal authority to control private communications systems in the United States during times of war or other national emergencies. The Federal Communications Commission plans to implement policies governing the shutdown of communications traffic for the "purpose of ensuring public safety". Also, on July 6, 2012, the White House approved an Executive Order seeking to ensure the continuity of government communications during a national crisis.¹³ As part of the Executive Order, DHS was granted the authority to seize private facilities, when necessary, effectively shutting down or limiting civilian communications.¹⁴

It is impossible to have an informed debate on the need for additional shutdown procedures without public information on the provisions of SOP 303. The complete shutdown of wireless communications for any period of time may be used to prevent the detonation of a bomb through a remote device.¹⁵ However, it can also be leveraged to quell political dissent, prevent protests, and stop the free flow of information and communications. For example, in 2011, the Egyptian government shut down all access to Internet and cellular services for the sole purpose of quieting large-scale anti-government

⁷ *Id.*

⁸ *BART protest causes major delays in service*, Kelly Zito, SFGate, July 11, 2011 <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/07/11/BA9G1K9905.DTL>.

⁹ *Id.*

¹⁰ Potter, *supra* note 6.

¹¹ *Id.*

¹² On April 30, 2012, the Federal Communications Commission ("FCC") requested public comment on proposed procedures to guide "intentional interruption of wireless service by government actors for the purpose of ensuring public safety." (http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0301/DA-12-311A1.pdf). Among other things, the FCC sought feedback on when, if ever, it is appropriate to disrupt wireless services. The comment period closed on May 30, 2012. A final document has not yet been released. However, any final procedures would only apply in circumstances involving public safety, and SOP 303 would remain the governing document for times of national emergency.

¹³ White House, Executive Order: Assignment of National Security and Emergency Preparedness Communications Functions (July 6, 2012), *available at* <http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.

¹⁴ *Id.* at Sec. 5.2(e).

¹⁵ *Government asks: when can we shut down wireless service?*, Matthew Lasar, Ars Technica, May 7, 2012 <http://arstechnica.com/tech-policy/2012/05/government-asks-when-can-we-shut-down-wireless-service/>.

protests.¹⁶ Early reports indicated, “The shutdown caused a 90 percent drop in data traffic to and from Egypt, crippling an important communications tool.”¹⁷

Documents Requested

In accordance with the facts presented above, EPIC requests the following three (3) categories of records from DHS:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined “series of questions” that determines if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information...” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.”¹⁸

EPIC is “primarily engaged in disseminating information.”¹⁹

There is a particular urgency for the public to obtain information about DHS’ authority to approve the shutdown of wireless networks in the United States. As previously discussed, President Obama signed a new Executive Order on July 6, 2012, which will grant DHS expanded authority to seize control of private communications facilities during times of national crisis.²⁰ This Executive Order has been the focus of a large number of recent news stories.²¹ In addition, numerous cybersecurity bills are currently under consideration, any of which may further extend DHS’ cyber authority.²²

¹⁶ *Egypt Cuts Off Most Internet and Cell Service*, Matt Richtel, New York Times, Jan. 28, 2011, <http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html>.

¹⁷ *Id.*

¹⁸ 5 U.S.C. § 552(a)(6)(E)(v)(II) (2012); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

¹⁹ *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

²⁰ White House, *supra* note 13.

²¹ *See, e.g., White House order on emergency communication riles privacy group*, Jaikumar Vijayan, Computerworld, July 10, 2012

http://www.computerworld.com/s/article/9228950/White_House_order_on_emergency_communications_riles_privacy_group; *White House creates new critical comms management committee*, Mark Rockwell, Gov’t Sec. News, July 9, 2012 <http://www.gsnmagazine.com/node/26716?c=communications>; *CNN Newsroom: Govt. re-prioritizing U.S. communications* (CNN television broadcast July 9, 2012, 2:40 PM), available at <http://newsroom.blogs.cnn.com/2012/07/09/govt-re-prioritizing-u-s-communications/>.

²² *See, e.g., Cybersecurity Act of 2012*, S. 2015, 112th Cong. (2012); *SECURE IT Act of 2012*, H.R. 4263, 112th Cong. (2012).

In order for the public to comment meaningfully on these actions, or subsequent measures, the public must be aware of DHS' current policies and procedures. Neither DHS nor the White House have provided substantive information on the development or implementation of SOP 303. The public must be informed about the government's powers to shut down wireless communications within the United States.

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for FOIA purposes.²³ Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed.²⁴ Further, consistent with the Department of Homeland Security regulations, any duplication fees should be waived because disclosure of the records requested herein "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Government," and "disclosure of the information 'is not primarily in the commercial interest of [EPIC]'".²⁵

This FOIA request involves information on DHS cybersecurity procedures. Responsive documents will hold a great informative value regarding activities of the Department that will have a significant public impact.

EPIC routinely and systematically disseminates information to the public. EPIC maintains several heavily visited websites that highlight breaking news concerning privacy and civil liberties. Two of EPIC's websites, EPIC.org and PRIVACY.org, consistently appear at the top of search engine rankings for searches on "privacy." EPIC also publishes a bi-weekly electronic newsletter, the EPIC Alert, which is distributed to around 20,000 readers, many who report on technology and privacy issues for major news outlets.²⁶

In addition, EPIC's FOIA documents have routinely been the subject of national news coverage. On a related matter, EPIC submitted a FOIA request to DHS for documents concerning the Department's surveillance of social networks and news organizations.²⁷ The documents detailed the Department's implementation of a program to gather information from public social communities on the Internet.²⁸ EPIC was able to disseminate those documents to the public at large, which resulted in numerous news stories.²⁹

²³ *EPIC v. Department of Defense*, 241 F.Supp.2d 5 (D.D.C. 2003).

²⁴ 6 C.F.R. § 5.11(c)(1)(i) (2011).

²⁵ *Id.* at (k)(1).

²⁶ See EPIC: EPIC Alert, <http://epic.org/alert/> (last visited Mar. 14, 2012).

²⁷ Letter from EPIC to Dept. of Homeland Sec. (Apr. 12, 2011) (on file at <http://epic.org/privacy/socialnet/EPIC-FOIA-DHS-Social-Media-Monitoring-04-12-11.pdf>).

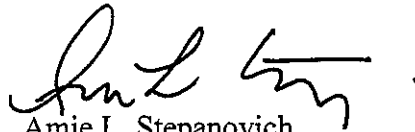
²⁸ See EPIC: EPIC v. Department of Homeland Security: Media Monitoring, <http://epic.org/foia/epic-v-dhs-media-monitoring/> (last visited July 9, 2012).

²⁹ See, e.g., *DHS list of words you should never ever blog or tweet. Ever.*, Kevin Fogarty, IT World, May 31, 2012 <http://www.itworld.com/security/279429/dhs-list-words-you-should-never-ever-blog-or-tweet->

EPIC is a non-profit, public interest research center that was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.³⁰ EPIC's work is distributed freely through our website and through the bi-weekly EPIC Alert newsletter. EPIC has no clients, no customers, and no shareholders. Therefore, EPIC has no commercial interest that would be furthered by disclosing the requested records.

Thank you for your consideration of this request. As provided in 6 C.F.R. § 5.5(d)(4), I will anticipate your determination on this request for expedited processing within ten (10) business days. For questions regarding this request, I can be contacted at (202)-483-1140 ext. 104 or FOIA@epic.org.

Respectfully Submitted,



Amie L. Stepanovich
Associate Litigation Counsel
Electronic Privacy Information Center

John J. Sadlik
IPIOP Clerk
Electronic Privacy Information Center

ever; *DHS monitoring of social media concerns civil liberties advocates*, Ellen Nakashima, The Washington Post, Jan. 13, 2012 http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIQANPO7wP_story.html; *Federal Contractor Monitored Social Network Sites*, Charlie Savage, New York Times, Jan. 13, 2012 <http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html>.

³⁰ EPIC: About EPIC, <http://epic.org/epic/about.html> (last visited Mar. 20, 2012).