



April 12, 2011

VIA CERTIFIED MAIL
 FOIA/PA
 The Privacy Office
 U.S. Department of Homeland Security
 245 Murray Drive SW
 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

Dear FOIA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks agency records in the possession of the Department of Homeland Security ("DHS") concerning private sector contracts, internal government trainings, inter-governmental communications and agreements, technical specifications, and security measures related to the agency's social media monitoring initiatives.

Background

On February 6, 2011, emails between employees of technology and security firm HB Gary Federal leaked to the press.¹ The emails revealed the company was planning to monitor, sabotage, and discredit the online expressive activities of American citizens.² HB Gary Federal had worked with data analysis companies Palantir Technologies and Berico Technologies to design a tactical program for mapping and tracking networks of labor union activists.³

HB Gary Federal planned to target their collection practices to specific individuals and match information from social media sites (e.g., Facebook, LinkedIn) to existing systems of records. The program involved multiple, "fake insider personas" (i.e., fraudulent social media accounts) designed to "generate communications" with union officials.⁴ CEO Aaron Barr spearheaded a mock up investigation as a proof of concept, scraping social media accounts for personally identifiable information, and compiling a

¹ Eric Lipton and Charlie Savage, *Hackers Reveal Offers to Spy on Corporate Rivals*, N.Y. Times, Feb. 11, 2011, <http://www.nytimes.com/2011/02/12/us/politics/12hackers.html>.

² HB Gary Email about US Chamber and Change to Win, FIREDOGLAKE, <http://firedoglake.com/documents/hb-gary-email-about-us-chamber-and-change-to-win/>

³ See E-mail from Sam Kremin of Berico Technologies to Ryan Castle of Palantir Technologies (Nov. 17, 2010, 1:29), http://thinkprogress.org/wp-content/uploads/2011/02/kremin_scraped_facebook_email.png.

⁴ See US Chamber Watch Information Operations Recommendation (Nov. 29, 2010), <http://images2.americanprogress.org/ThinkProgress/ProposalForTheChamber.pdf>

report that included pictures of his target's spouse and children, high school address and home address information, and political donations.⁵

On March 1, 2011, twenty lawmakers from the House of Representatives sent a public letter to the Chairs of the House Oversight and Government Reform, Judiciary, Permanent Select Intelligence, and Armed Services Committees.⁶ They demanded an investigation into these companies and their "subversive techniques."⁷ The letter recommended measures to obtain "any correspondence and documents from the parties concerning the planned campaign and any other similar activities, including the government contracts, under which the contractors in question have been paid millions of dollars."⁸ One of the signatories, Representative Hank Johnson (D-Ga) sent another letter on March 28, 2011, calling upon the Department of Justice to review its federal contracts with the three firms.⁹ Representative Johnson specifically cited the possibility that the three companies "may have violated the law and/or their federal contracts by conspiring to use technologies developed for U.S. intelligence and counterterrorism purposes against American citizens and organizations on behalf of private actors."¹⁰

One of the leaked emails revealed that HB Gary Federal President Penny C. Leavy was planning a special training with DHS in 2010.¹¹ Leavy sent the email on May 28, 2010, in the middle of DHS's efforts to scale up the agency's Publicly Available Social Media Monitoring and Situational Awareness Initiatives. DHS has stated these initiatives were designed to gather information from "online forums, blogs, public websites, and message boards," to store and analyze the information gathered, and then to "disseminate relevant and appropriate de-identified information to federal, state, local, and foreign governments and private sector partners."¹² Previously, DHS had tailored individual initiatives to individual events, gathering intelligence pertaining to the January 2010 earthquake in Haiti, the 2010 Winter Olympics in Canada, or to the April 2010 BP Oil Spill Response.¹³ In June of 2010, however, DHS signaled its intention to introduce

⁵ Scott Keyes, *CHAMBERLEAKS: US Chamber's Lobbyists Solicited Firm to Investigate Opponents' Families, Children*, THINKPROGRESS (Feb. 10, 2011 8:05 PM), <http://thinkprogress.org/2011/02/10/chamberleaks-target-families/>.

⁶ Letter from Rep. Hank Johnson et al., to Rep. Darrell Issa, Chairman of H. Comm. on Oversight and Government Reform, et al. (Mar. 1, 2011), http://hankjohnson.house.gov/johnson_letter.pdf.

⁷ *Id.*

⁸ *Id.*

⁹ Letter from Rep. Hank Johnson to James Clapper, Dir. Of National Intelligence (Mar. 28, 2011), http://hankjohnson.house.gov/2011_03_28_rep_hank_johnson_requests_themis_contracts_dod_doj_dni.pdf

¹⁰ *Id.*

¹¹ Justin Elliott, *Firm in WikiLeaks Plot Has Deep Ties to Feds*, SALON, (Feb. 16, 2011 11:01 AM), http://www.salon.com/news/politics/war_room/2011/02/16/hbgary_federal. See E-mail from Penny C. Leavy, President of HB Gary to Tim Vera and Jim Richards of HB Gary (May 28, 2011, 08:36 AM), <https://uoadr.com/u/E3.txt>.

¹² Privacy Act of 1974; Department of Homeland Security Office Operations Coordination and Planning-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records, 76 Fed. Reg. 5603 (Feb. 1, 2011).

¹³ See Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Haiti Social Media Disaster Monitoring Initiative, January 21, 2010, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_haiti.pdf; Department of Homeland

permanent social media monitoring, and officially announced a new permanent program on February 1, 2011 in the Federal Register.¹⁴

As laid out in the Federal Register and Privacy Impact Assessments, an ongoing DHS social media monitoring initiative would authorize the agency to "establish usernames and passwords," to form social media profiles that will follow other accounts, deploy search tools, and record the results of an array of potentially sensitive search terms (stated examples of search terms include "illegal immigrants," "drill," "infection," "strain," "outbreak," "virus," "recovery," "deaths," "collapse," "human to animal," and "trojan").¹⁵ DHS proposed targeting search terms likely to retrieve embarrassing information, which the agency would then store for up to five years and package for dissemination through transnational and international networks.¹⁶

The proposed social media monitoring initiative is designed to gather personally identifiable information (PII), including full names, affiliations, positions or titles, and account usernames.¹⁷ The agency plans to collect PII "when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners."¹⁸ Social media users could provide any range of sensitive information in their online communications if they have no reason to believe that the Department of Homeland Security is tracking their every post. The agency anticipates retrieving such information in the normal course of performing social media searches.¹⁹ DHS states that it will redact PII before "dissemination," presumably to other agencies as well as state, local, tribal, and foreign governments, and authorized private sector entities.²⁰ The agency plans regularly to relay the records it produces through this program to "federal, state, local, tribal, territorial, foreign, or international government partners."²¹ The DHS Chief Privacy Officer (CPO) has stated that the records will be

Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning 2010 Winter Olympics Social Media Event Monitoring Initiative, February 10, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_2010winterolympics.pdf; Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative, April 29, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_bpoilspill.pdf.

¹⁴ Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, June 22, 2010; Privacy Act of 1974; System of Records Notice, *supra* note 12.

¹⁵ *Id.*

¹⁶ Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 7, Jan. 6, 2011, *available at*

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf.

¹⁷ System of Records Notice, *supra* note 12, at 5604.

¹⁸ *Id.* at 5603-4.

¹⁹ *Id.* at 5603.

²⁰ *Id.* ("The NOC will . . . disseminate relevant and appropriate de-identified information to federal, state, local, and foreign governments, and private sector partners authorized to receive situational awareness and a common operating picture.")

²¹ *Id.* at 5604.

shared both by "email and telephone" to contacts inside and outside of the agency.²² The CPO further stated that "[n]o procedures are in place" to determine which users may access this system of records.²³ Even Department contractors have full access to the system.²⁴

Documents Requested

EPIC requests the following agency records (including but not limited to electronic records):

1. All contracts, proposals, and communications between the federal government and third parties, including, but not limited to, H.B. Gary Federal, Palantir Technologies, and/or Berico Technologies, and/or parent or subsidiary companies, that include provisions concerning the capability of social media monitoring technology to capture, store, aggregate, analyze, and/or match personally-identifiable information.
2. All contracts, proposals, and communications between DHS and any states, localities, tribes, territories, and foreign governments, and/or their agencies or subsidiaries, and/or any corporate entities, including but not limited to H.B. Gary Federal, Palantir Technologies, and/or Berico Technologies, regarding the implementation of any social media monitoring initiative.
3. All documents used by DHS for internal training of staff and personnel regarding social media monitoring, including any correspondence and communications between DHS, internal staff and personnel, and/or privacy officers, regarding the receipt, use, and/or implementation of training and evaluation documents.
4. All documents detailing the technical specifications of social media monitoring software and analytic tools, including any security measures to protect records of collected information and analysis.
5. All documents concerning data breaches of records generated by social media monitoring technology.

Request for Expedited Processing

This request warrants expedited processing because it has been filed 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." 5 U.S.C. §552(a)(6)(E)(v)(II)(2009); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C.

²² Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 8, Jan. 6, 2011.

²³ Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 10, June 22, 2010.

²⁴ *Id.*

Cir. 2001). The Electronic Privacy Information Center is "primarily engaged in disseminating information." *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about the privacy implications of social media monitoring because government surveillance has a direct impact on the civil rights and civil liberties of American citizens. This request will serve to fill in gaps in publicly available information, and clarify the federal government's relationship to individuals and entities using advanced surveillance techniques for political purposes. Prominent lawmakers have already lodged multiple requests for additional public scrutiny into the implications of HB Gary's conduct. EPIC's request will serve to inform this process with timely, accurate, and significant information.

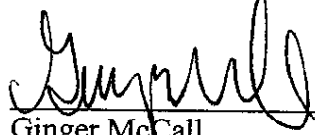
Request for "News Media" Fee Status

EPIC is a "representative of the news media" for fee waiver purposes. *Electronic Privacy Information Center v. Department of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003). EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC maintains a heavily visited Web site (<http://www.epic.org>) that highlights the "latest news" concerning privacy and civil liberties issues. The site also features documents EPIC obtains under the FOIA. EPIC also publishes a biweekly electronic newsletter that is distributed to over 15,000 readers, many of whom report on technology issues for major news outlets. The newsletter reports on relevant policy developments of a timely nature (hence the bi-weekly publication schedule). The newsletter has been published continuously since 1996, and an archive of past issues is available at EPIC's web site. Finally, EPIC publishes and distributes printed books that address a broad range of privacy, civil liberties, and technology issues. A list of EPIC publications is available on its website. Based on its status as a "news media" requester, EPIC is entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operation or activities of the government," any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 5 U.S.C. §552(a)(6)(E)(ii), EPIC anticipates your determination on its request for expedited processing within ten (10) calendar days.



Conor Kennedy
EPIC Appellate Advocacy Fellow
Electronic Privacy Information Center
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
202.483.1140 x 123



Ginger McCall
EPIC Associate Director of Open
Government Project
Electronic Privacy Information Center
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
202.483.1140 x 102