U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

May 5, 2010

MR. SHANE WITNOV
ELECTRONIC FRONTIER FOUNDATION
454 SHOTWELL STREET
SAN FRANCISCO, CA 94110

Subject: INVESTIGATIVE TECHNIQUES FOR
SOCIAL-NETWORKING WEBSITES

FOIPA No. 1139566- 000

Dear Mr. Witnov:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552

☒(b)(1)

☒(b)(2)

□(b)(3)____________________

____

____

____

□(b)(4)

□(b)(5)

☒(b)(6)

□(b)(7)(A)

□(b)(7)(B)

☒(b)(7)(C)

□(b)(7)(D)

☒(b)(7)(E)

□(b)(7)(F)

□(b)(8)

□(b)(9)

Section 552a

□(d)(5)

□(j)(2)

□(k)(1)

□(k)(2)

□(k)(3)

□(k)(4)

□(k)(5)

□(k)(6)

□(k)(7)

17 **page(s)** were reviewed and 12 **page(s)** are being released.

☒ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

☒ referred to the OGA for review and direct response to you.

□ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Number assigned to your request so that it may be easily identified.

□ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

This is an interim release of documents responsive to your request. Enclosed are three items, including FBI Intelligence Information Report (IIR) Handbook, Cyber Intrusions Against Social Networking Sites, and the "Dark Web" e-mail chain and article. A fourth item has been referred to Department of Justice. In the context of your request, the FBI IIR Handbook is a cross-reference. Cross-references are defined as mentions of the subject of your request in documents relating to other individuals, organizations, events or activities. In processing cross-references, the pages considered for possible release included only those pages which mention the subject of your request and any additional pages showing the context in which the subject of your request was mentioned.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/heridentity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 5
Page 1 ~ Referral/Direct - Bates #13
Page 2 ~ Referral/Direct - Bates #14
Page 3 ~ Referral/Direct - Bates #15
Page 4 ~ Referral/Direct - Bates #16
Page 5 ~ Referral/Direct - Bates #17

XXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXX

From: [redacted](CTD) (FBI)
Sent: Wednesday, October 03, 2007 9:46 AM
To: [redacted](DI) (FBI);[redacted](OS) (FBI);
[redacted](OS) (FBI);[redacted](CTD) (FBI);
[redacted](CyD) (FBI);[redacted](CTD) (FBI); b6
[redacted](CTD) (FBI)[redacted](CTD) (FBI); b7C
[redacted](CTD) (FBI)[redacted](CTD) (FBI);
[redacted](CTD) (FBI)
Cc: [redacted](CTD) (FBI)[redacted](CTD) (FBI);[redacted]
[redacted](CTD) (FBI)
Subject: FW: University of Arizona Dark Web Project

Attachments: Scientists Use the _Dark Web_to Snag Extremists and Terrorists Online - US National Science Foundation (NSF).pdf

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

To All,

The article attached in the e-mail thread reflects computer research being conducted by the University of Arizona (U of A) Artificial Intelligence Lab re the use of sophisticated software tools to exploit large amounts of data via spidering to identify authorship, link analysis, content and semantic analysis, social networking patterns, etc. U of A is one of the top academic facilities in the U.S. conducting this type of research. The research project is collectively called "Dark Web".

[redacted]
[redacted]

b2
b7E

I would like to coordinate a meeting in which the U of A briefs the FBI on the Dark Web project to see if any of their analytical tools might be applicable in your respective operational analysis and exploitation of data, including web forums[redacted]
[redacted]

b2
b7E

The list of invitees in not restricted. Please feel free to past the word. Some of you have already contacted me and shown interest in hearing more about possible FBI applications of the Dark Web tools. The U of A and the Dark Web project are receiving national attention via the attached article.

Dr. Chen is the Director of the U of A Artificial Intelligence Lab and in charge of the Dark Web project. He is interested in giving a 2 hour briefing at FBIHQ on Dark Web applications and has advised that he is available on 10/25/2007. If that date is not good, I am sure a later date could be arranged.

Please feel free to contact me for additional information at[redacted]

b6
b7C
b2

I would appreciate any feedback asap so I can advise Dr. Chen re arranging a meeting with the FBI.

Thanks,

[redacted]

-----Original Message-----

b6
b7C

From: [redacted] (CTD) (FBI)
Sent: Thursday, September 13, 2007 4:35 PM
To: [redacted] (OS) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (CTD) (FBI)
Subject: UA in the news

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello,

[redacted] wanted me to pass along the attached document that has made the recent news amongst the academic circle, and in the Bureau as well (CyD and CITT were recently apprised of the article).

Scientists Use the
_Dark Web_t...

b6
b7C
b2

[redacted]
FBIHQ, Ext. [illegible]43
It's great to be a Florida Gator!

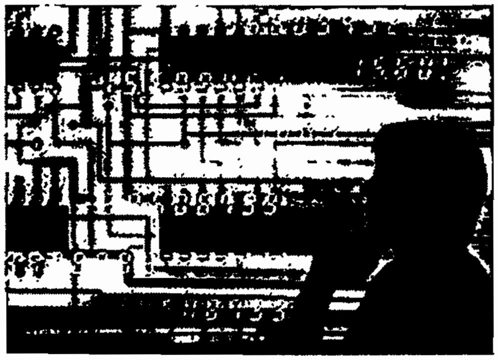
SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Press Release 07-118

Scientists Use the "Dark Web" to Snag Extremists and Terrorists Online

Team from the University of Arizona identifies and tracks terrorists on the Web



The Dark Web project team catalogues and studies places online where terrorists operate.
Credit and Larger Version

September 10, 2007

Terrorists and extremists have set up shop on the Internet, using it to recruit new members, spread propaganda and plan attacks across the world. The size and scope of these dark corners of the Web are vast and disturbing. But in a non-descript building in Tucson, a team of computational scientists are using the cutting-edge technology and novel new approaches to track their moves online, providing an invaluable tool in the global war on terror.

Funded by the National Science Foundation and other federal agencies, Hsinchun Chen and his Artificial Intelligence Lab at the University of Arizona have created the Dark Web project, which aims to systematically collect and analyze *all* terrorist-generated content on the Web.

This is no small undertaking. The speed, ubiquity, and potential anonymity of Internet media--email, web sites, and Internet forums--make them ideal communication channels for militant groups and terrorist organizations. As a result, terrorists groups and their followers have created a vast presence on the Internet. A recent report estimates that there are more than 5,000 Web sites created and maintained by known international terrorist groups, including Al-Qaeda, the Iraqi insurgencies, and many home-grown terrorist cells in Europe. Many of these sites are produced in multiple languages and can be hidden within innocuous-looking Web sites.

Because of its vital role in coordinating terror activities, analyzing Web content has become increasingly important to the intelligence agencies and research communities that monitor these groups, yet the sheer amount of material to be analyzed is so great that it can quickly overwhelm traditional methods of monitoring and surveillance.

This is where the Dark Web project comes in. Using advanced techniques such as Web spidering, link analysis, content analysis, authorship analysis, sentiment analysis and multimedia analysis, Chen and his team can find, catalogue and analyze extremist activities online. According to Chen, scenarios involving vast amounts of information and data points are ideal challenges for computational scientists, who use the power of advanced computers and applications to find patterns and connections where humans can not.

One of the tools developed by Dark Web is a technique called Writeprint, which automatically extracts thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online. Writeprint can look at a posting on an online bulletin board, for example, and compare it with writings found elsewhere on the Internet. By analyzing these certain features, it can determine with more than 95 percent accuracy if the author has produced other content in the past. The system can then alert analysts when the same author produces new content, as well as where on the Internet the content is being copied, linked to or discussed.

Dark Web also uses complex tracking software called Web spiders to search discussion threads and other content to find the corners of the Internet where terrorist activities are taking place. But according to Chen, sometimes the terrorists fight back.

"They can put booby-traps in their Web forums," Chen explains, "and the spider can bring back viruses to our machines." This online cat-and-mouse game means Dark Web must be constantly vigilant against these and other counter-measures deployed by the terrorists.

Despite the risks, Dark Web is producing tangible results in the global war on terror. The project team recently completed a study of online stories and videos designed to help train terrorists in how to build improvised explosive devices (IEDs). Understanding what information is being spread about IED methods and where in the world it is being downloaded can improve countermeasures that are developed to thwart them.

Dark Web is also a major research testbed for understanding the propaganda, ideology, communication, fundraising, command and control, and recruitment and training of terrorist groups. The Dark Web team has used the tools at their disposal to explore the content and impact of materials relating to "virtual imams" on the Internet, as well as terrorist training and weapons manuals.

Dark Web's capabilities are also being used to study the online presence of extremist groups and other social movement organizations. Chen sees applications for this Web mining approach for other academic fields.

"What we are doing is using this to study societal change," Chen says. "Evidence of this change is appearing online, and computational science can help other disciplines better understand this change."

-NSF-

Media Contacts
Dana W. Cruikshank, NSF (703) 292-8070 dcruiksh@nsf.gov

Program Contacts
Maria Zemankova, NSF (703) 292-8930 mzemanko@nsf.gov

Principal Investigators
Hsinchun Chen, Artificial Intelligence Lab, University of Arizona (520) 621-6219 hchen@eller.arizona.edu

Related Websites
Dark Web Project Web Site: http://ai.arizona.edu/research/terror/index.htm
NSF's Division of Information & Intelligent Systems (IIS): http://www.nsf.gov/div/index.jsp?div=IIS

The National Science Foundation (NSF) is an independent federal agency that supports fundamental research and education across all fields of science and engineering, with an annual budget of $5.92 billion. NSF funds reach all 50 states through grants to over 1,700 universities and institutions. Each year, NSF receives about 42,000 competitive requests for funding, and makes over 10,000 new funding awards. The NSF also awards over $400 million in professional and service contracts yearly.

Receive official NSF news electronically through the e-mail delivery and notification system, MyNSF (formerly the Custom News Service). To subscribe, visit www.nsf.gov/mynsf/ *and fill in the information under "new users".*

Useful NSF Web Sites:
NSF Home Page: http://www.nsf.gov
NSF News: http://www.nsf.gov/news/
For the News Media: http://www.nsf.gov/news/newsroom.jsp
Science and Engineering Statistics: http://www.nsf.gov/statistics/
Awards Searches: http://www.nsf.gov/awardsearch/

The National Science Foundation, 4201 Wilson Boulevard, Arlington, Virginia
22230, USA
Tel: (703) 292-5111, FIRS: (800) 877-8339 | TDD: (800) 281-8749

Last Updated: September 10, 2007