U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

CRM-200900732F

MAR 3 2010

Mr. James Tucker
Mr. Shane Witnov
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Dear Messrs Tucker and Witnov:

This is an interim response to your request dated October 6, 2009 for access to records concerning "use of social networking websites (including, but not limited to Facebook, MySpace, Twitter, Flickr and other online social media) for investigative (criminal or otherwise) or data gathering purposes created since January 2003, including, but not limited to:

1) documents that contain information on the use of "fake identities" to "trick" users "into accepting a [government] official as friend" or otherwise provide information to he government as described in the Boston Globe article quoted above;

2) guides, manuals, policy statements, memoranda, presentations, or other materials explaining how government agents should collect information on social networking websites:

3) guides, manuals, policy statements, memoranda, presentations, or other materials, detailing how or when government agents may collect information through social networking websites;

4) guides, manuals, policy statements, memoranda, presentations and other materials detailing what procedures government agents must follow to collect information through social-networking websites;

5) guides, manuals, policy statements, memorandum, presentations, agreements (both formal and informal) with social-networking companies, or other materials relating to privileged user access by the Criminal Division to the social networking websites;

6) guides, manuals, memoranda, presentations or other materials for using any visualization programs, data analysis programs or tools used to analyze data gathered from social networks;

7) contracts, requests for proposals, or purchase orders for any visualization programs, data analysis programs or tools used to analyze data gathered from social networks.

8) guides, manuals, policy statements, memoranda, presentations, or other materials describing how information collected from social-networking websites is retained in government databases or shared with other government agencies."

While processing your request, we located one record totaling 33 pages. After careful review of this document we determined to release this item in part. We are withholding portions of the record pursuant to the exemption in 5 U.S.C. 552(b)(6)which permits the withholding of personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. The withheld material consists of work telephone numbers and e-mail addresses of DOJ attorneys.

We will continue to search for any additional documents that may be responsive to your request. We estimate that it make take approximately fourteen days to complete the processing of your request.

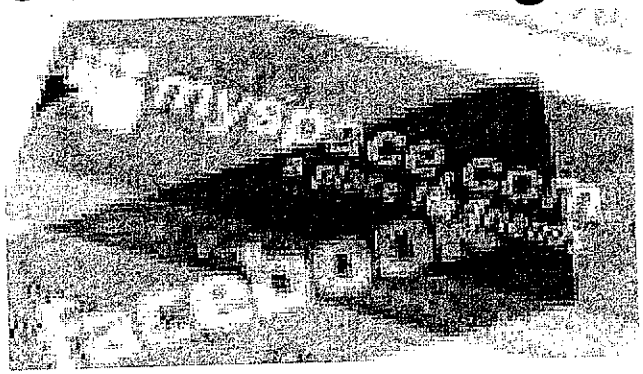
Although your FOIA request is the subject of litigation, I am nonetheless required by regulation to inform you that you that you have a right to an to an administrative appeal of this partial denial of your request. Your appeal should be addressed to: The Office of Information Policy, United States Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, DC 20530-0001. Both the envelope and the letter should be clearly marked with the legend "FOIA Appeal." Department regulations provide that such appeals must be received by the Office of Information Policy within sixty days of the date of this letter.

Sincerely,

Catherine Gonzalez Gallego for

Rena Y. Kim, Chief
Freedom of Information/Privacy Act Unit
Office of Enforcement Operations
Criminal Division

Obtaining and Using Evidence from Social Networking Sites



Facebook, MySpace, LinkedIn, and More

John Lynch
Deputy Chief, Computer Crime
Computer Crime & Intellectual Property Section

Jenny Ellickson
Trial Attorney
Computer Crime & Intellectual Property Section

AGENDA

Introduction to Social Networking Sites

Overview of Key Social Networking Sites

Additional Legal and Practical Issues

AGENDA

[redacted]

Overview of Key Social Networking Sites

Additional Legal and Practical Issues

Introduction to Social Networking

THE RISE OF ONLINE SOCIAL NETWORKS

1997	SixDegrees.com
2003	Friendster, LinkedIn
2004	MySpace
2005	Facebook
2008	Twitter

Introduction to Social Networking

POPULAR SOCIAL NETWORKS

Worldwide: **Facebook**

U.S. and Canada: **MySpace, LinkedIn, Twitter**

Europe: **MySpace, Twitter, Hi5, V Kontakte**

Latin America: **Hi5, Orkut, Tagged**

Asia: **QQ, Friendster, Xiaonei, Orkut, Mixi, Hi5**

Middle East and Africa: **Maktoob, Hi5**

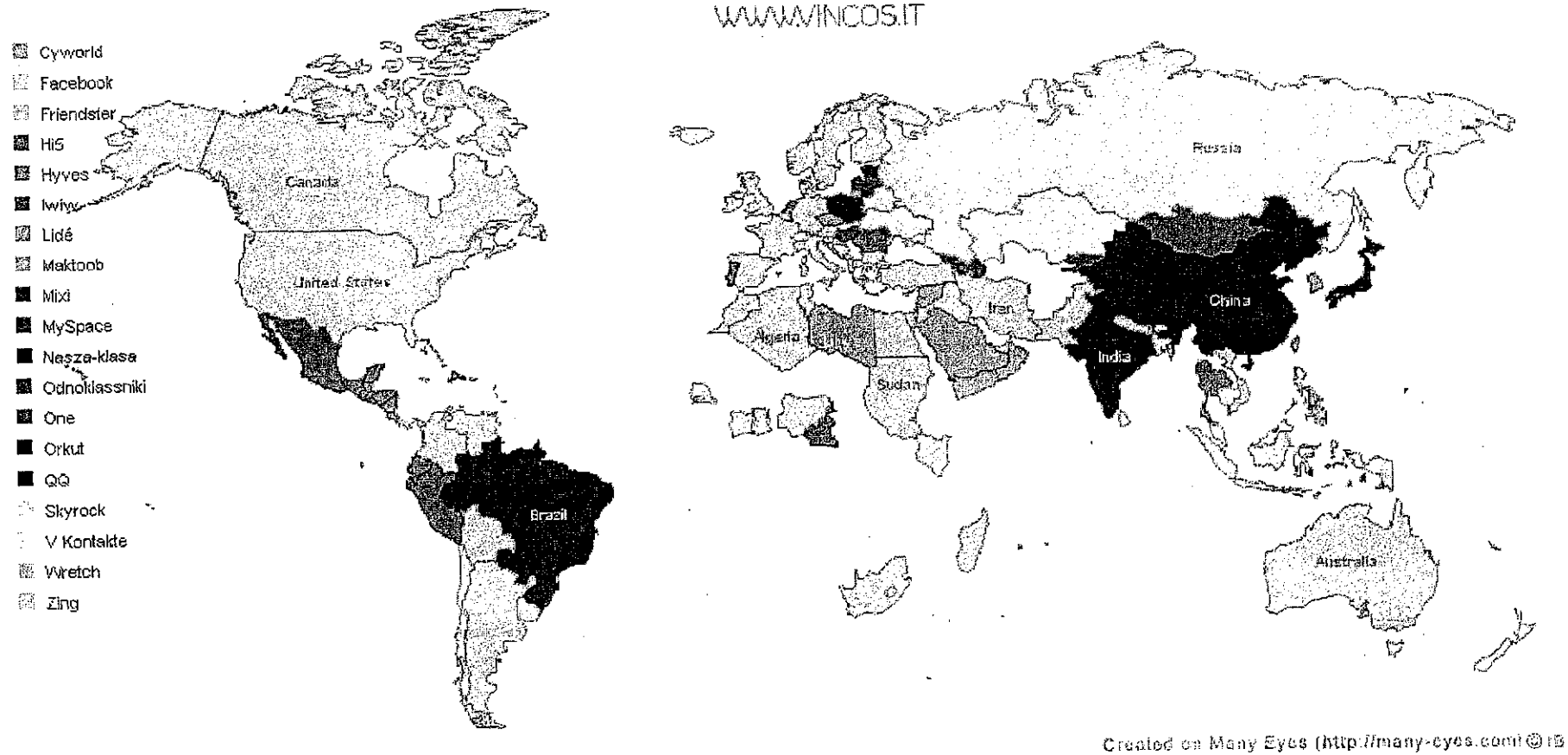


Image courtesy Vincenzo Cosenza (www.vincos.it), data based on Alexa and Google Trends

Introduction to Social Networking

POPULARITY IN THE UNITED STATES

Most-visited websites in the U.S. (August 2009)

1. Google
2. Yahoo
3. Facebook
4. YouTube
5. MySpace

. . .

13. Twitter

. . .

27. LinkedIn

Source: Alexa.com – August 12, 2009 list of Top 100 websites in United States.

Introduction to Social Networking

THE BASICS

Most social-networking sites allow users to:

- Create personal profiles
- Write status updates or blog entries
- Post photographs, videos, and audio clips
- Send and receive private messages
- Link to the pages of others (i.e., "friends")

How can LE obtain data from these sites?

- Some info may be public
- Use ECPA to get info from providers
- Undercover operations?

Introduction to Social Networking

UTILITY IN CRIMINAL CASES

Evidence from social-networking sites can

- **Reveal personal communications**
- **Establish motives and personal relationships**
- **Provide location information**
- **Prove and disprove alibis**
- **Establish crime or criminal enterprise**

Also: instrumentalities or fruits of crime.

AGENDA

Introduction to Social Networking

[redacted]

Additional Legal and Practical Issues

Overview of Key Social Networking Sites

FACEBOOK

Founded in 2004, primarily catering to students

Now over 250m active members worldwide

Over 10b photos in Oct 2008; adds over 1b monthly

Applications run on Facebook platform

True names encouraged but not guaranteed

Privacy model is highly granular; present different information to different groups or individual users

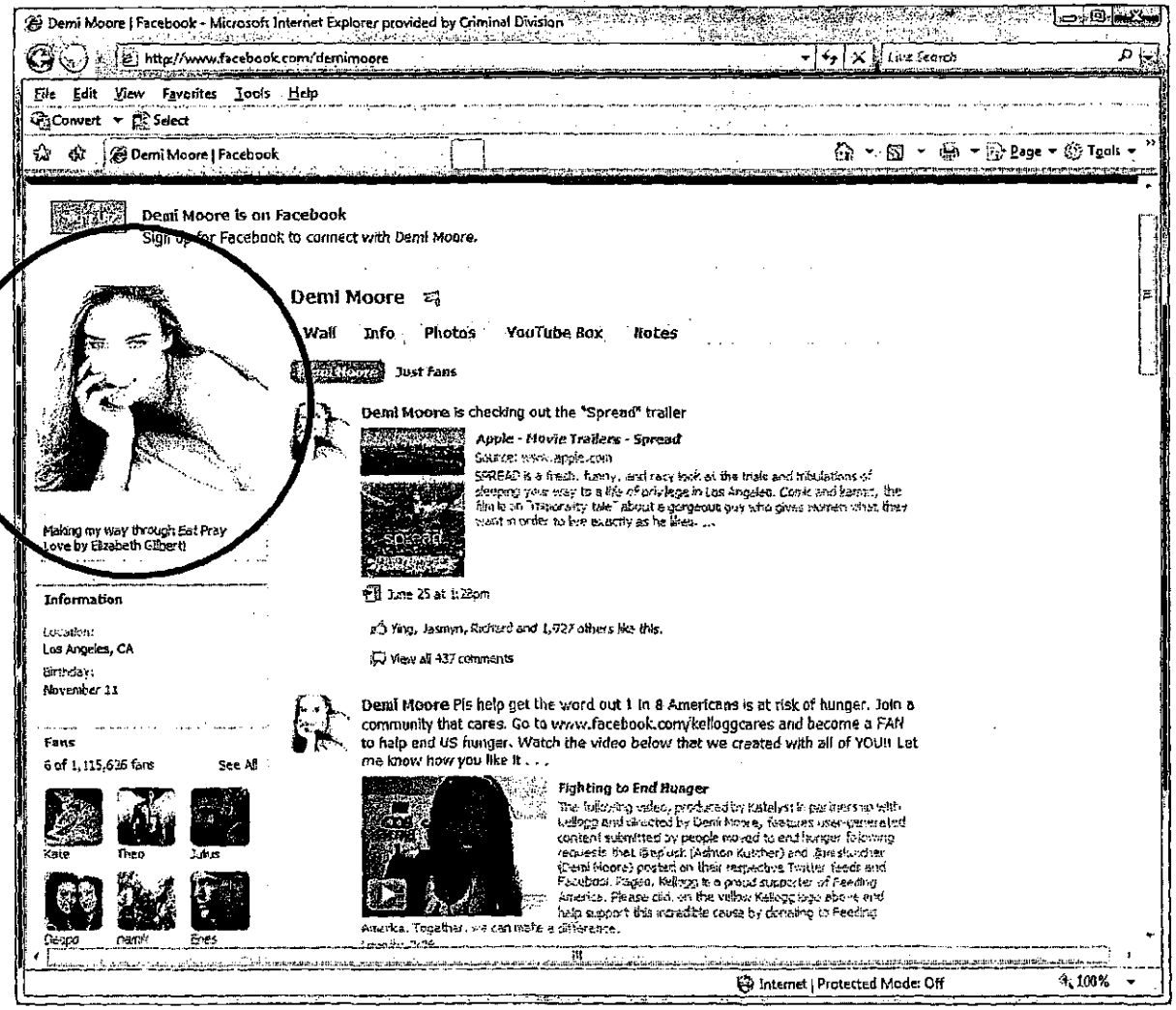
Messaging includes mail, real-time chat, "wall"

Now used in private background checks

Koobface – virus/worm vector

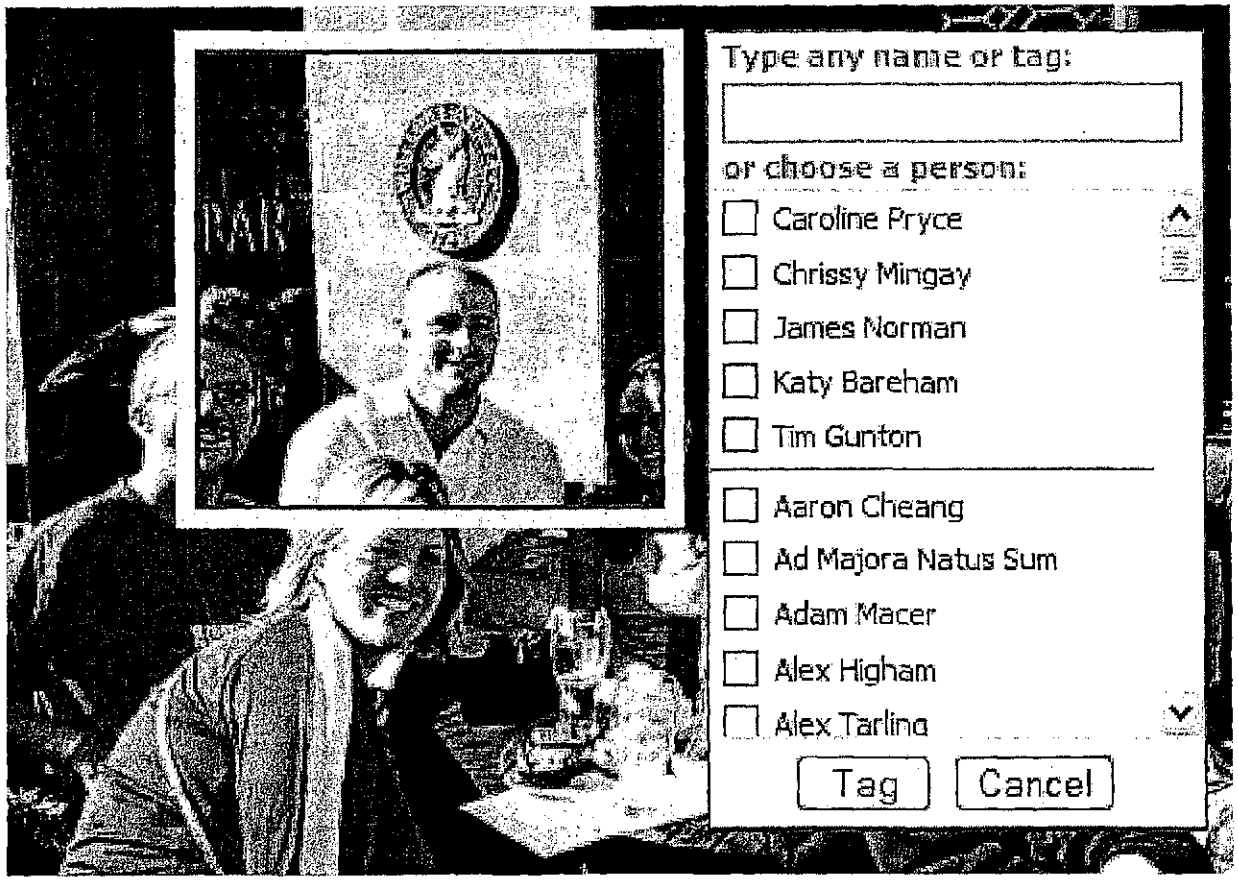
Overview of Key Social Networking Sites

FACEBOOK



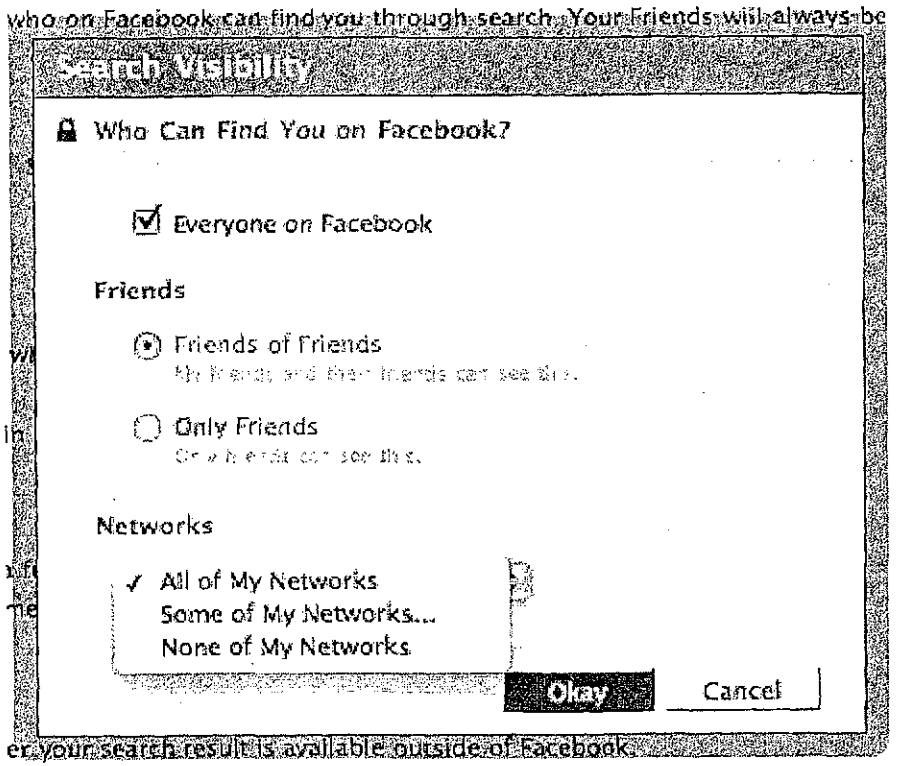
Overview of Key Social Networking Sites

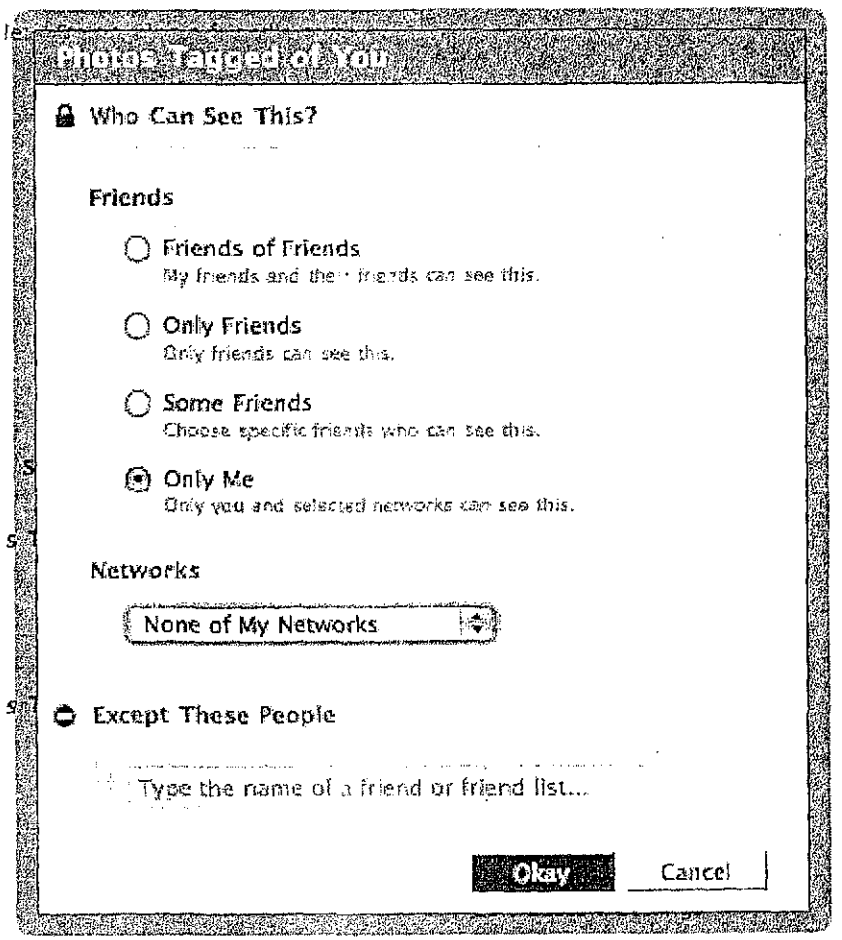
FACEBOOK



Overview of Key Social Networking Sites

FACEBOOK





Overview of Key Social Networking Sites

GETTING INFO FROM FACEBOOK

Data is organized by user ID or group ID

Standard data productions (per LE guide):

Neoprint, Photoprint, User Contact Info, Group Contact Info, IP Logs

HOWEVER, Facebook has other data available.

Often cooperative with emergency requests.

Overview of Key Social Networking Sites

MYSPACE

Founded 2003, now owned by Fox Interactive Media

2006: Most popular SN; passed by Facebook in 2008

Currently tens of millions of active users monthly

True names less encouraged than Facebook

Messaging through messages, chat, friend updates

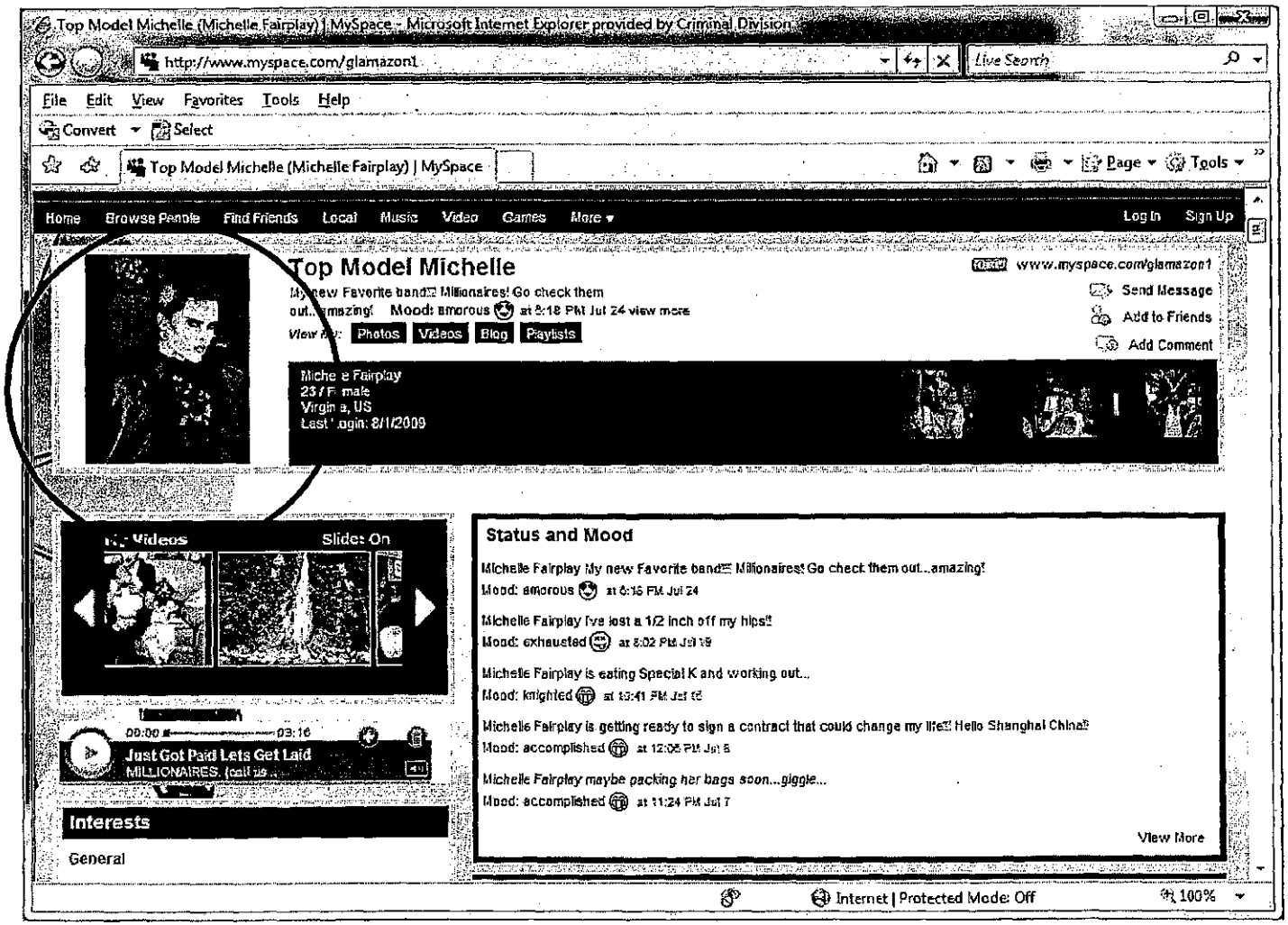
Application platform rolled out early 2008

Young user base, history of child safety concerns

Privacy is currently less granular than Facebook

Overview of Key Social Networking Sites

MYSPACE

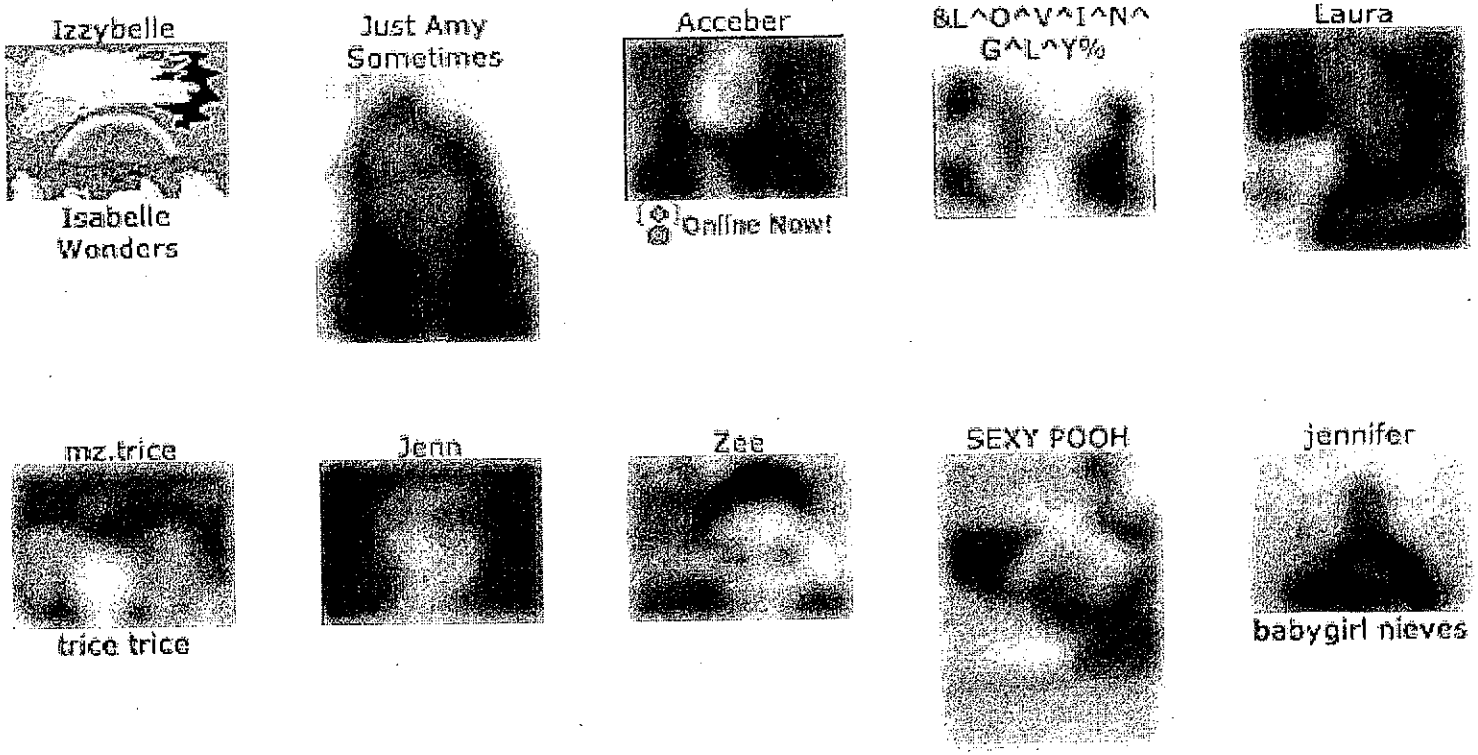


Overview of Key Social Networking Sites

MYSPACE

Overview of Key Social Networking Sites

MYSPACE



Overview of Key Social Networking Sites

GETTING INFO FROM MYSPACE

Many profiles have public content.

Data is organized by FriendID – see LE guide.

MySpace requires a search warrant for private messages/bulletins less than 181 days old

- **Also considers friend lists to be stored content**

Data retention times

User info and stored files – indefinitely

IP logs, info for deleted accounts – 1 year

Overview of Key Social Networking Sites

TWITTER

Market leader in "micro-blogging"

Began in mid-2006 as "status message" service

Ubiquity and ease of updating, but limited space

Breaking news, real-time updates: USAir, Iran

Most multimedia handled by 3d party links

Simplified privacy model: updates public or private

Direct messages are private; sender can delete

Short URLs used to serve malicious links and code

Overview of Key Social Networking Sites

TWITTER

Overview of Key Social Networking Sites

GETTING INFO FROM TWITTER

The good news

- Most Twitter content is public
- Private messages kept until user deletes them

The bad news

- No contact phone number
- Only retain last login IP
- Will not preserve data without legal process
- Stated policy of producing data only in response to legal process (i.e., no 2702)
- No Law Enforcement Guide

Overview of Key Social Networking Sites

LINKEDIN

Business-focused with enforced limits to interaction

Profiles focused on education and work experience

Use for criminal communications appears limited

But can be used to identify experts

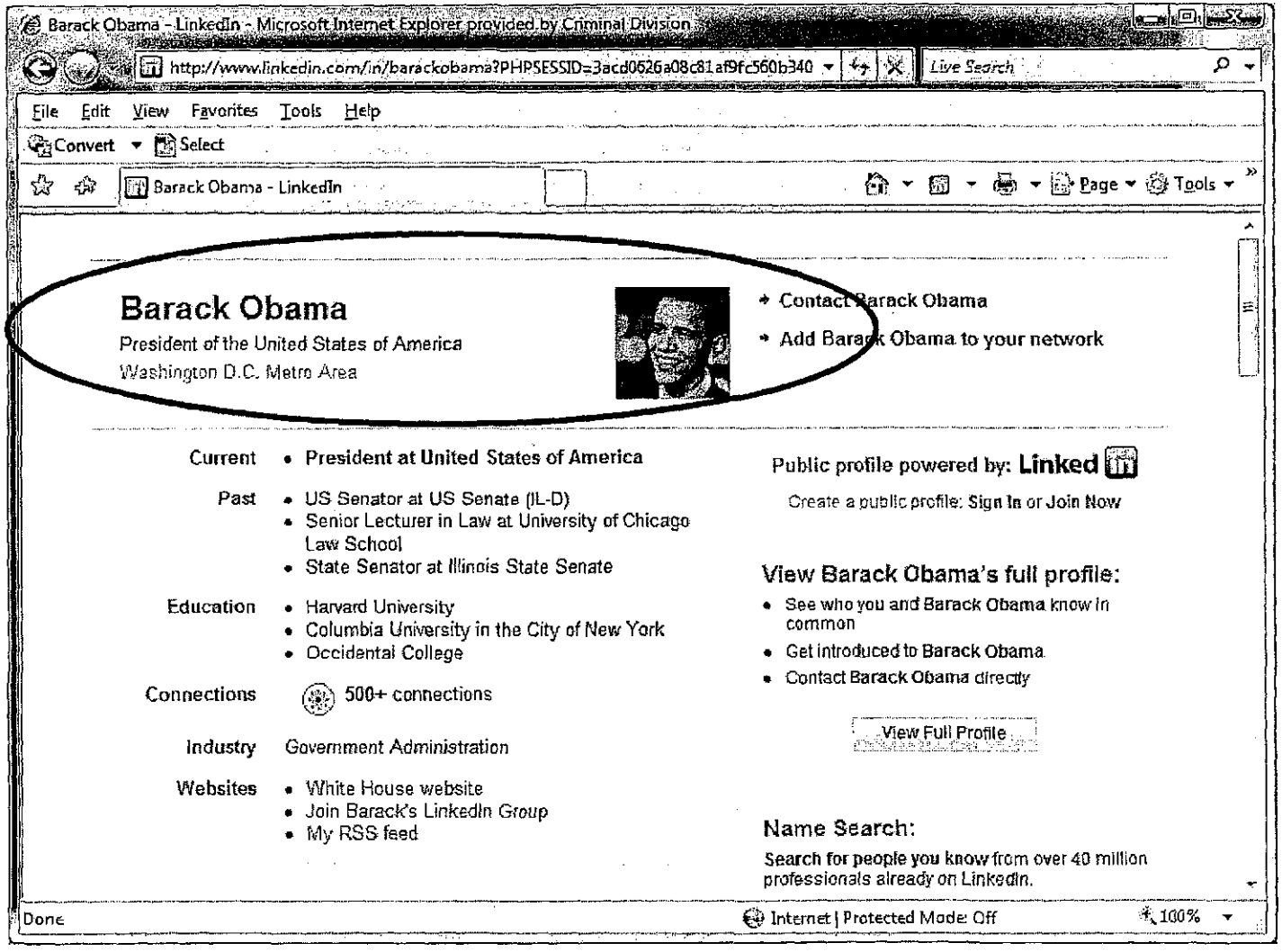
Can check background of defense experts

Privacy model similar to Facebook

Profile information is not checked for reliability

Overview of Key Social Networking Sites

LINKEDIN



AGENDA

Introduction to Social Networking

Overview of Key Social Networking Sites

[redacted]

Legal and Practical Issues

FEDERATED IDENTITY ISSUES

- Social networking sites increasingly adopting federated identity schemes
  - OpenID, Facebook Connect
- Facebook, MySpace, Yahoo!, and Google act as identity authenticators – "Single Sign-In" model
- *Example:* A user can log in to a Facebook account using Google credentials
  - After a link is established between two accounts, Google will check and vouch for identity of its user
  - Authentication information split from activity information
  - In turn, a Facebook login may be used to authenticate to sites using "Facebook Connect"
- If attribution is necessary, must determine identity provider – not simply the domain.

Introduction to Social Networking

TERMS OF SERVICE / PRIVACY POLICIES

- **Social networks have extensive terms of service and privacy policies**
  - **Most permit emergency disclosures to LE**
  - **All specify exceptions to respond to legal process and protect service against fraud/damage**
- ***U.S. v. Drew* – can failure to follow TOS render access unauthorized under 1030?**
  - **Employment policy cases tend to say yes**
  - **But concerns that transforms TOS into private criminal code for site misconduct**

Legal and Practical Issues

DOES THE PPA APPLY?

- **Growth of social networks raises questions of breadth of PPA**
  - **Is Facebook/Twitter a "similar form of communication" to a newspaper, book, broadcast? (Ashton Kutcher? CNNbrk? Iran?)**
  - **No easy answers, but look to intent to communicate news to sizable audience**
  - **In many cases, *Guest v. Leis* rule will be sufficient; CCIPS can help with analysis**
- **Congress continues to examine media shield**

Legal and Practical Issues

UNDERCOVER OPERATIONS

Why go undercover on Facebook, MySpace, etc?

- **Communicate with suspects/targets**
- **Gain access to non-public info**
- **Map social relationships/networks**

Undercover operations after *U.S. v. Drew*

- **If agents violate terms of service, is that "otherwise illegal activity"?**

Legal and Practical Issues

WITNESSES & SOCIAL NETWORKS

Many witnesses have social-networking pages

- Valuable source of info on defense witnesses
- Potential pitfalls for government witnesses

Knowledge is power

- Research all witnesses on social-networking sites
- Discovery obligations?

Advise your witnesses:

- Not to discuss cases on social-networking sites
- To think carefully about what they post

Legal and Practical Issues

OTHER COURTROOM ISSUES

Social networking and the courtroom can be a dangerous combination

- Use caution in "friending" judges, defense counsel
- Warn jurors about social-networking sites

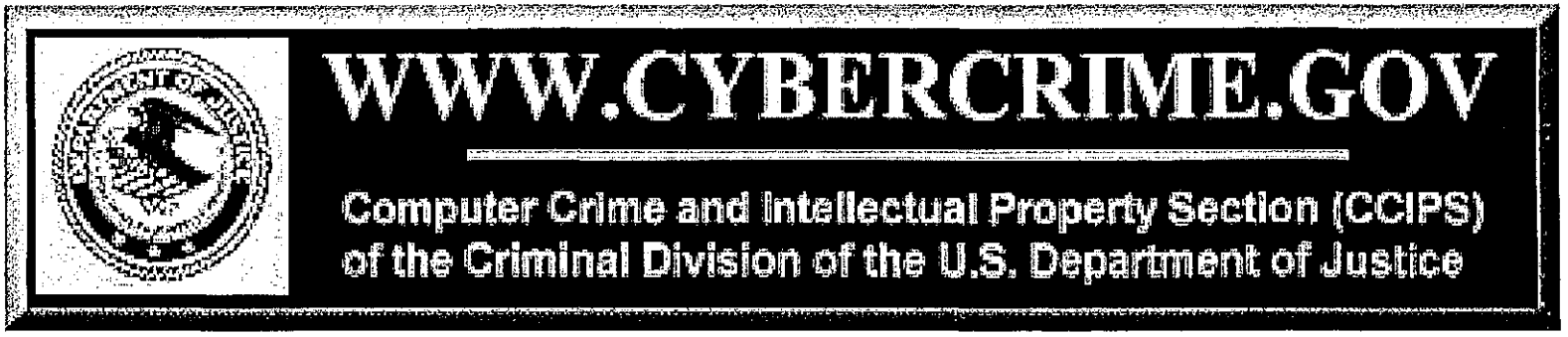
Social networking + mobile devices = real-time updates on courtroom events

Computer Crime & Intellectual Property Section

CCIPS Duty Line: 202-514-1026

John Lynch

B6

Jenny Ellickson

B6