How Your Employer Might be Tracking You
SHARE Anaheim Session 14528

Laura Knapp
WW Business Consultant
Laurak@aesclever.com

Why Do Companies Track Their Employees?

- Monitoring Production
- Security
- Discipline
- Feedback
- Training
- Theft Prevention

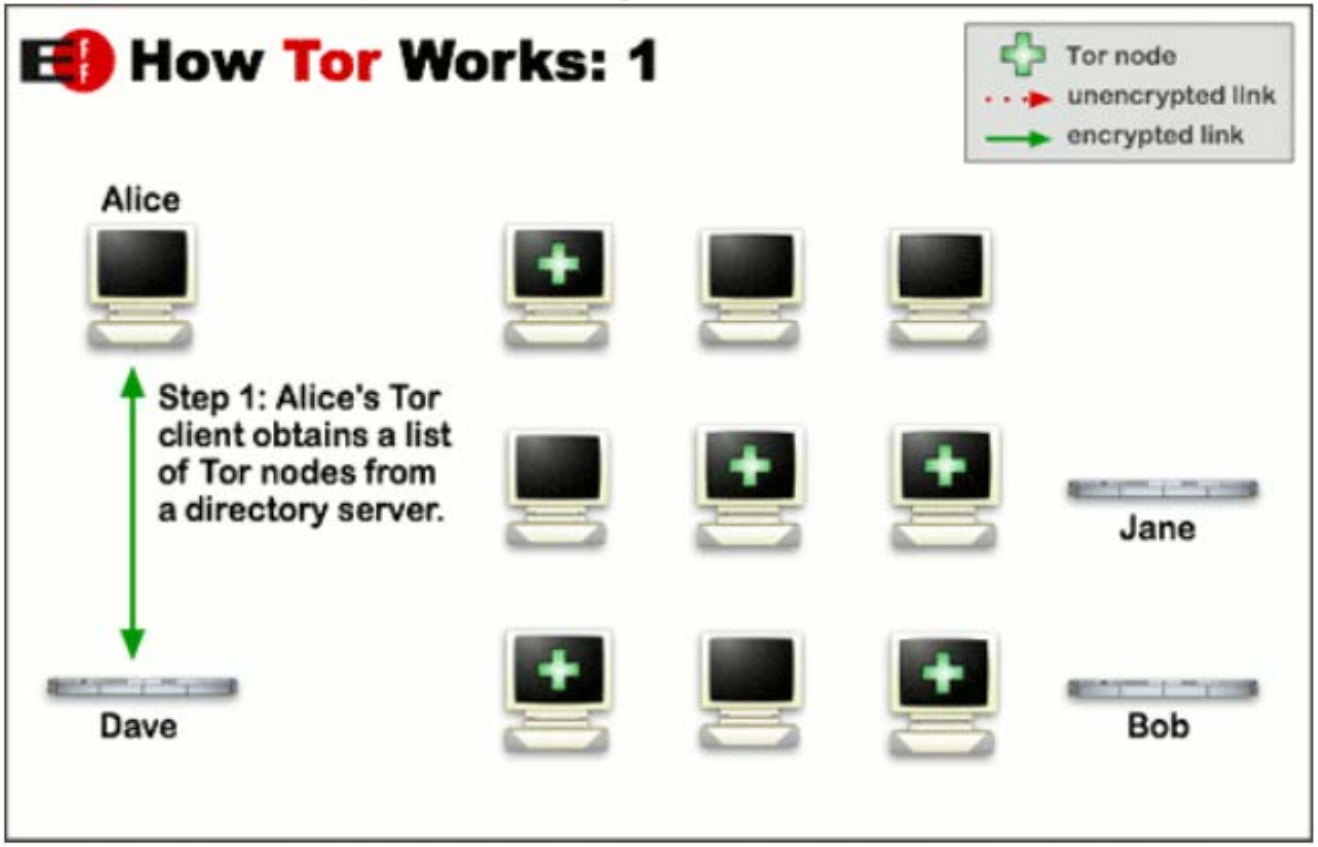
TOR

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

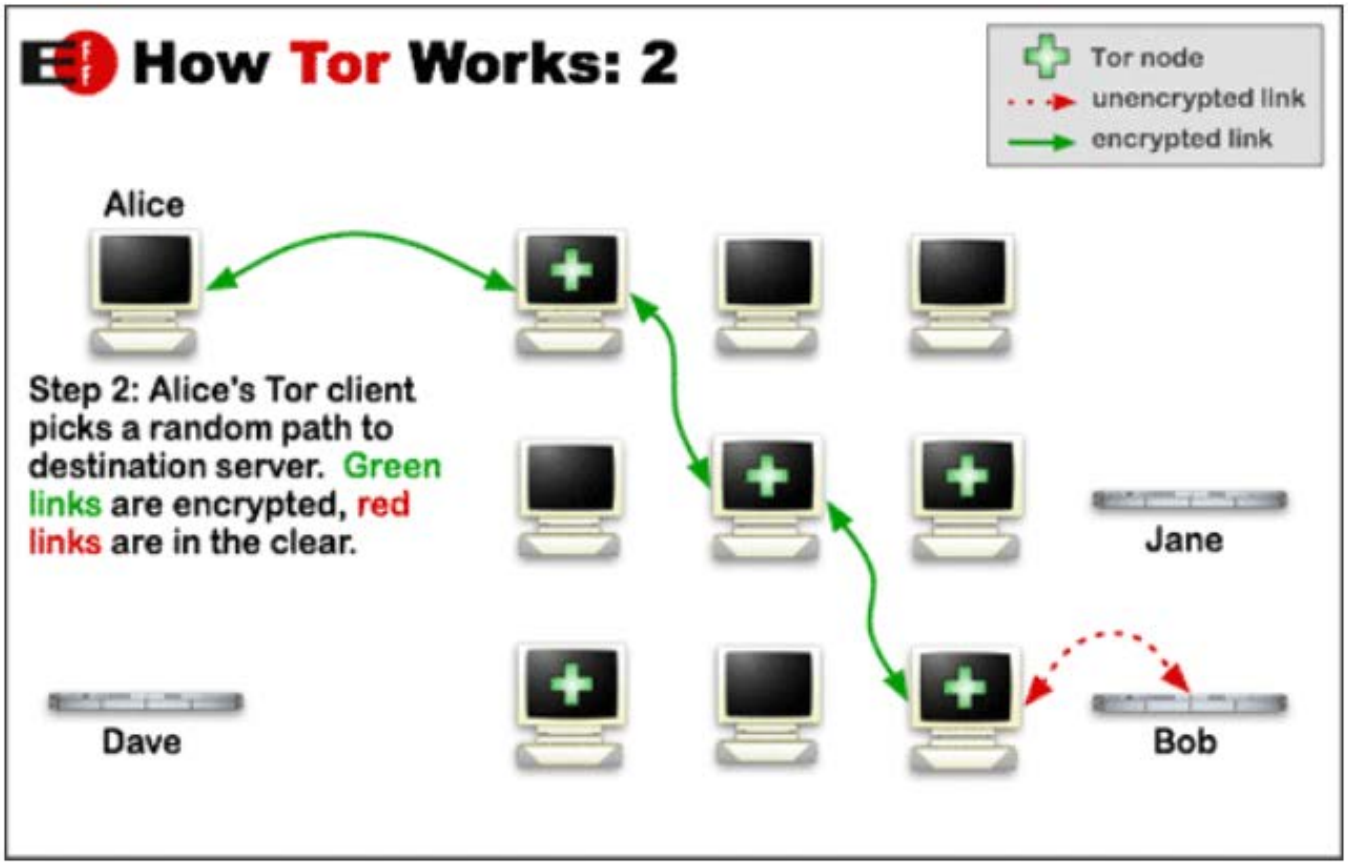
How Tor Works

The solution: a distributed, anonymous network

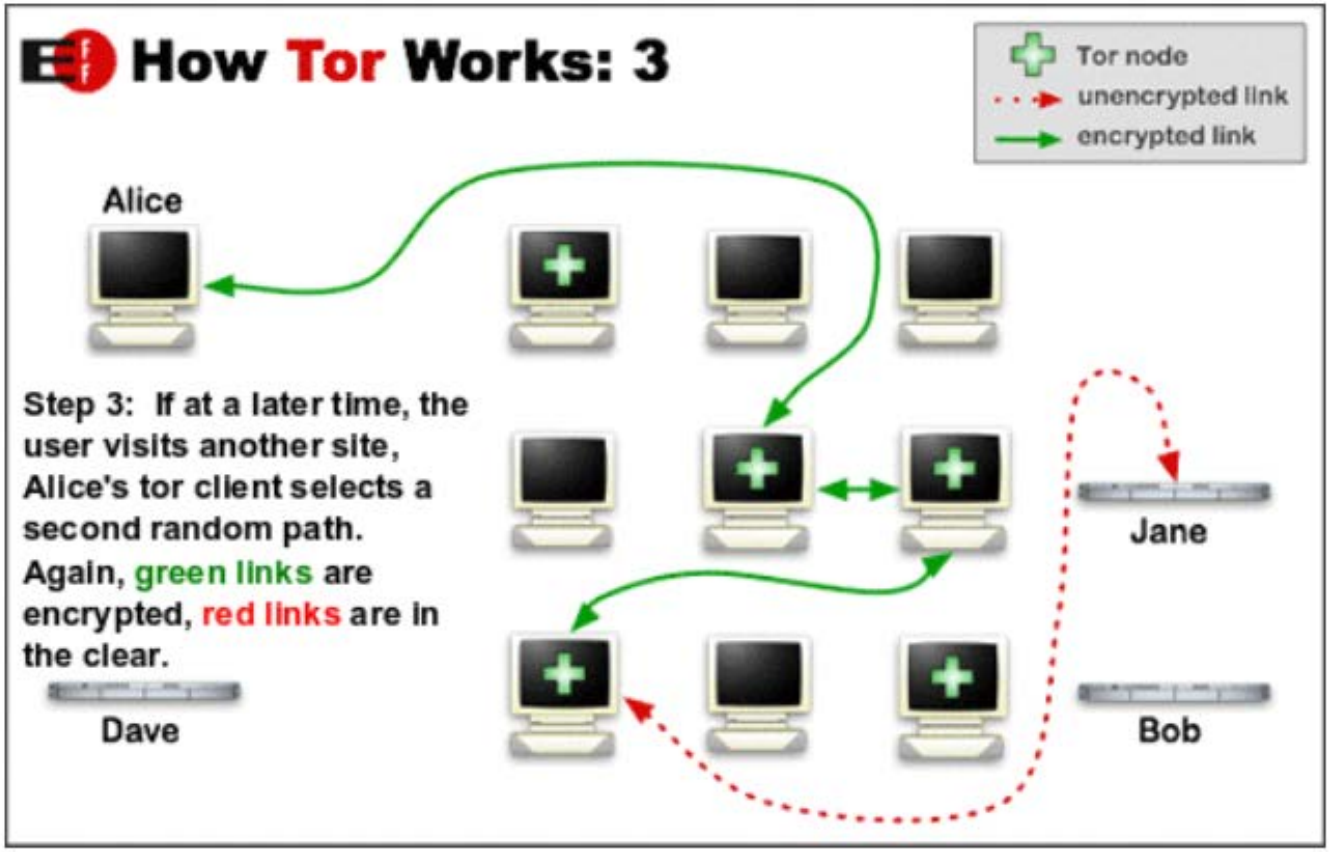


www.torproject.org

How Tor Works



How Tor Works



Tor Hidden Services Protocol

https://www.torproject.org/docs/hidden-services.html.en

Monitoring in Major Cities

- New York City has the largest and oldest system, with more than 7,000 public and private surveillance cameras.

- New Orleans has installed more than 200 wireless digital cameras in locations that include housing projects, cruise terminals and the French Quarter.

- Baltimore is putting in a $2 million network of more than 90 surveillance cameras in the Inner Harbor tourist area and high-crime neighborhoods.

Monitoring in Major Cities

- Chicago is adding 250 cameras in high-crime areas and plans to link the 2,000 that monitor public housing, the transit system and public buildings, so their feeds can all be watched at the city's emergency operations center

- Los Angeles has installed anti-crime video cameras in three neighborhoods, paid for by local businesses and the Motion Picture Association of America, which wants to thwart street sales of bootleg DVDs.

Monitoring in Major Cities

- In San Francisco and Washington, subway stations and platforms are under constant surveillance by closed-circuit television cameras.
- New Jersey Transit uses computer software that automatically alerts the police when an unattended package shows up on video monitors.
- The light-rail system in Houston plans to enable its onboard security cameras to transmit live images, wirelessly, to police cruisers

Monitoring Around the World

Many countries are using CCTV(closed-circuit television)

- Australia
- China
- United Kingdom
- USA
- Russia
- India
- Singapore……

Countries are using surveillance for a number of reasons

- Reduce crimes/deter violence
- Deter driving violations
- Catch terrorists/other wanted individuals

Closer Look at the UK

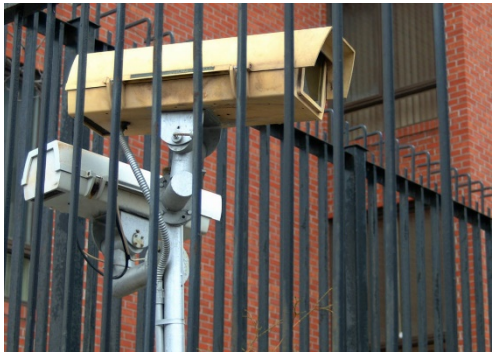
CCTV cameras in Britain is 4.2 million!

One camera for every 14 people

It is estimated that on a single day a person can expect to be filmed 300 times

500 million pounds (944 million dollars) has been spent on the installation of CCTV cameras over the past decade

Three quarters of the crime prevention budget is now spent on CCTV



Monitoring Technologies

- **Integrated IP Surveillance Systems Wi-Fi MESH Wireless**
- **Trailer-mounted Surveillance Point to Point Wireless**
- **Mega-Pixel Network Cameras Point to Multi-Point**
- **Thermal Imaging Cameras Cellular Ethernet**
- **Solar Power Integration GPS Monitoring**
- **Wireless Sensors**
- **Enterprise Network Video Recording Software (NVR)**
- **Radio Frequency Identification (RFID)**

Monitoring is Everywhere in the Workplace

How common is it?

- 1993 20 million Americans were under computer surveillance while at work
- 1997 37.5% of all employers use a surveillance device to spy on workers
- 2000 75% of employers
- 2005 10000 million phone calls are eavesdropped on every year by employers

Workplace Surveillance

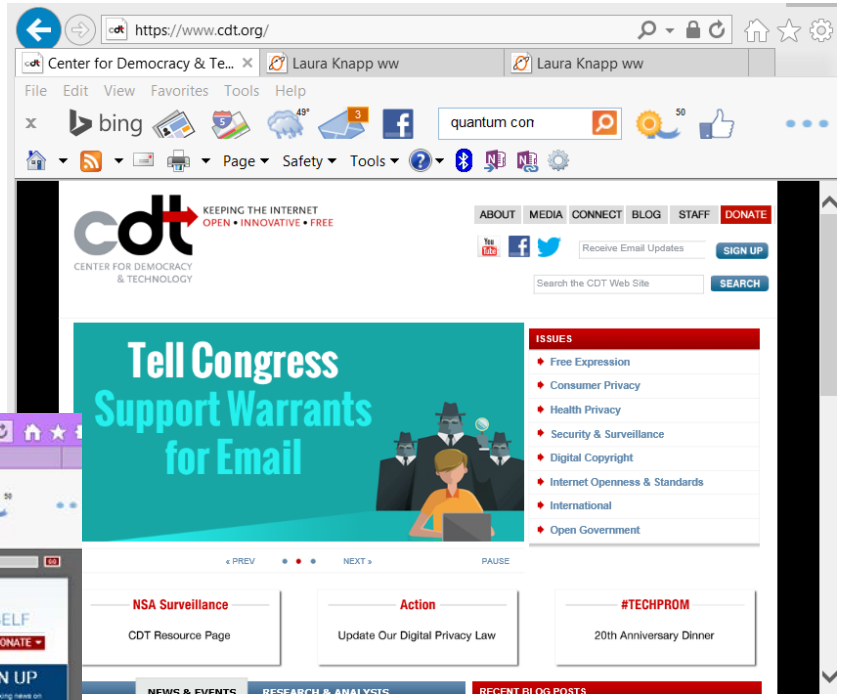
- 99% of all companies with more than 1,000 employees currently use e-mail
- Sixty billion + messages are sent annually
- Employees are under the impression that their messages are private
- Old and deleted messages are archived and easily accessible by management
- In the US there is no comprehensive, uniform legal standard protecting privacy

- http://www.PrivacyExchange.org

What Cyberspace Knows about You

If you go to http://www.cdt.org you will learn how much government and employers can discover about you

Go to http://www.aclu.org/privacy and you will find that a lot of information about you could be available to anyone



Legal Issues

Electronic Communications Privacy Act

- Intended to restrict government power in wire taps and electronic data transmission via computers

USA Patriot Act

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
- Result of 9/11 terrorist attacks
- Weakened power of ECPA

Keylogging Programs

Record every keystroke

Hardware
BIOS, circuit board chip, wireless overlays

Software
Hypervisor, Kernel, API based, form grabbing,
Memory injections, packet analyzers, remote ac
Software.

Acoustic technologies
Analyze the frequency of clicks, electromagnetic emissions

Some Legal Protection?
Stored Communication Act
Federal Wiretap Act

Email/website/application Monitoring

Written policy in companies that they can monitor Email

Even personal emails if sent from company device

Electronics Privacy Law is week in this area

Tools exist for them to scan for words or phrases

Social Media

Be careful who you befriend

Understand the social media policy at work

Employers and potential employers check these sites

Some states have banned the practice

Don’t say you are taking medical leave then post cruise pictures on facebook

Area is still grey on lawsuits

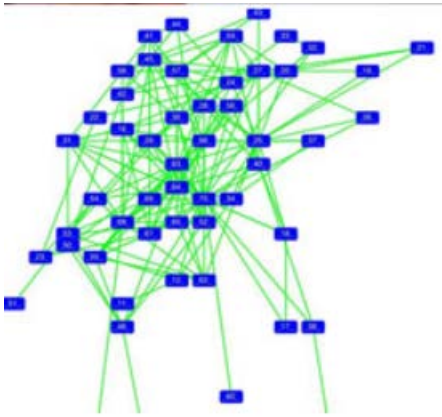
Smart Badges

MIT Technology
- wireless radio
- infrared sensor
- accelerometer
- microphone

Calculate how far apart people are standing

Record conversations

Track Movements



Company Supplied SmartPhones

Bluetooth: On all the time

Track and record encounters wit other Bluetooth devices

iPhones have an accelerometer

Can tell if you are sitting or walking

All have recorders

Tell who you talk to, how you say things, inflections, etc.

Common Ethical Issues for IT Users:
Software Piracy

Software Piracy: a common violation occurs when employees copy software from their work computers for use at home
Inappropriate Use of Computing Resources: some employees use their work computers to surf popular Web sites that have nothing to do with their jobs.

"Half of Fortune 500 companies have dealt with at least one incident related to computer porn in the workplace over the past 12 months, according to a survey released today.
Corporations are taking the problem seriously, and fired the offenders in 44% of the cases and disciplined those responsible in 41% of the instances".

(China Martens, Survey: Computer porn remains issue at U.S. companies, Computer-world, June 21, 2005

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=102664

Common Ethical Issues for IT Users: Inappropriate Sharing of Information

- Organizations stored vast amount of information that can be classified as private or confidential.
- Private data describes individual employees – for example, salary, attendance, performance rating, health record.
- Confidential information describes a company and its operations: sales, promotion plans, research and development.
- Sharing this information with unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors.

National Labor Relations Board – Memo OM-11-74

Non-profit social services organization violated Section 7 of the NLRA when it discharged five employees who engaged in protected concerted activity using Facebook as a discussion forum.

a. Swearing and sarcasm in several of the posts did not cause the activity to lose its protected status.
b. Negative comments about supervisor equals protected activity by exercising her Weingarten rights and by discussing supervisory conduct with her coworkers.
c. Company's internet policy and found the following provisions violated the Act: prohibition against posting any picture of the employees that depict the company in any way, a prohibition against making disparaging comments about supervisors or coworkers, and a broadly worded standards of conduct provision barring "offensive conduct".

National Labor Relations Board – Memo OM-11-74

Complaints on cheap food and poor driving

Photos and comments, although personal, vocalized the sentiments of the coworkers and were, therefore, concerted and that they were protected because they pertained to working conditions.

"Inappropriate Discussions" Prohibition Likely Unlawful
Internet Policy.

a. Employees were advised that they owed additional state income taxes due to employer withholding errors, exchanged posts on Facebook, and made derogatory comments about the employer.
b. The Board found the Facebook postings to be both concerted (multiple postings and comments) and protected (administration of tax withholding was a term or condition of employment).

National Labor Relations Board – Memo OM-11-74

Offensive tweets was not engaged in protected concerted activity.

a. No evidence that he discussed his concerns with his coworkers.
b. Prohibited from airing his grievances or commenting about the newspaper in any public forum. He continued to tweet but not about the company.
c. Posting was protected because it pertained to working conditions, it was not concerted since no coworkers responded to the post or otherwise engaged in conversation about the matter.

5. Bartender upset with the tip-sharing policy took to Facebook to vent and posted cruel comments about the customers

Again, posting was protected (pertaining to work conditions) but not concerted because no co-workers engaged

National Labor Relations Board – Memo OM-11-74

An employee who posted comments of the Facebook wall of her U.S. Senator, including disparaging remarks about how her company failed to assist the situation, was not engaged in concerted activity.

An employee at a shelter was terminated after complaining about her interaction with the clients in mental health facility, but the only persons who commented on the post were Facebook “friends” who were not coworkers.

In one case, clothing store employee took to Facebook to complain about mispriced or misplaced items. Several coworkers responded to the post, but the Board saw no indication in responses that coworkers thought that this employee was initiating group activity on their behalf. (The post was, essentially, a personal grip and therefore not “concerted”).

National Labor Relations Board – Memo OM-11-74 January 2012

Board found social media policies adopted by the companies in several cases violated the Act because they prohibited communication or conduct that was protected by Section 7.

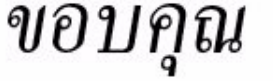
- "An employer violates Section 8(a)(1) through the maintenance of a work rule if that rule 'would reasonably tend to chill employees in the exercise of their Section 7 rights.
- Clearly unlawful if it explicitly restricts Section 7 protected activities.
- Employees would reasonably construe the language to prohibit Section 7 activity.
- The rule was promulgated in response to union activity.
- Applied to restrict the exercise of Section 7 rights."

ありがとうございました

Grazie

Danke

Merci



धन्यवाद
Hindi
Gracias

laurak@aesclever.com

www.aesclever.com

650-617-2400

감사합니다

நன்றி
Tamil

Obrigado

: