



Managing Data & Databases

Session 22
Data Ownership and Privacy

Who owns your digital footprint?

- Why aren't you paying for your email service? Wouldn't it be great if you could get free phone plans as well, by letting phone companies mine your phone calls?
- Why isn't there any good paid email / social networking service for those who want to pay?
- Why isn't the data on your phone and your personal computer encrypted by default?
- How does Facebook decide which posts to show you, and why is their choice necessarily right?
- Is it fine that Google makes billions by selling 'targeted ads' enabled by your data, while it doesn't pay you a cent? They mine your data, but also that of your friend's data who doesn't have a Google account. Is that fine?
- Which one of you knows how to encrypt his/her sensitive data?
- What is cryptography?

Whose is your data?

- Data you (or someone else) shares with public
 - Data you share with a company, or a company acquires on you
 - Data the government(s) acquire(s) on you
-
- What are the modalities of access and ownership?

Some basics of property rights

- Three types of rights
 - Usus
 - Notion of use and control
 - Fructus
 - Notion of profit
 - Abusus
 - Notion of destroy or transfer

Your data and the firms

A brief history of user data exploitation

- Online advertising ([doubleclick.net](#), etc.)
- Targeted marketing (Office Depot, Google, etc.)
- Behavioral targeting (gameloft, Facebook, etc.)
- Social engineering?

Facebook reveals news feed experiment to control emotions

Protests over secret study involving 689,000 users in which friends' postings were moved to influence moods

[Poll: Facebook's secret mood experiment: have you lost trust in the social network?](#)





Current Issue >

vol. 111 no. 24 > Adam D. I. Kramer, 8788–8790, doi: 10.1073/pnas.1320040111



CrossMark

[click for updates](#)

Experimental evidence of massive-scale emotional contagion through social networks

Adam D. I. Kramer^{a,1}, Jamie E. Guillory^{b,2}, and Jeffrey T. Hancock^{b,c}

Author Affiliations

Edited by Susan T. Fiske, Princeton University, Princeton, NJ, and approved March 25, 2014 (received for review October 23, 2013)

A correction has been published

A correction has been published

[Abstract](#)[Full Text](#)[Authors & Info](#)[Figures](#)[Metrics](#)[Related Content](#)[PDF](#)

Significance

We show, via a massive ($N = 689,003$) experiment on Facebook, that emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness. We provide experimental evidence that emotional contagion occurs without direct interaction between people (exposure to a friend expressing an emotion is sufficient), and in the complete absence of nonverbal cues.

What happens to your data
when it becomes public?

What if Audrie Pott hadn't killed herself?

EU court backs 'right to be forgotten': Google must amend results on request

Individuals have right to control their data and can ask search engines to remove results, says European court



Your data and the government



13

Surveillance

Nation & World

Ubiquitous TV cameras aid London bomb probe

You're being watched: there's one CCTV camera for every 32 people in UK

Research shows 1.85m machines across Britain, most of them indoors and privately operated



Surveillance

Caught on Camera: You are Filmed on CCTV 300 Times a Day in London

By **Geetha Pillai**

March 11, 2012 08:37 GMT



16



A Metropolitan police officer monitors CCTV screens in the new Special Operations Room in London.

A Londoner is caught on a close circuit surveillance camera over 300 times a day, thanks to the 51,600 CCTV cameras installed across Britain controlled by local authorities, almost 20 per cent of the world's CCTV population.

According to a report released recently by NGO Big Brother Watch, £515 million spent on CCTVs for the past four years would be sufficient to put an extra 4,121 police constables on the streets, equivalent of Northumbria police's entire force.

<http://www.ibtimes.co.uk/>

Surveillance

Surveillance



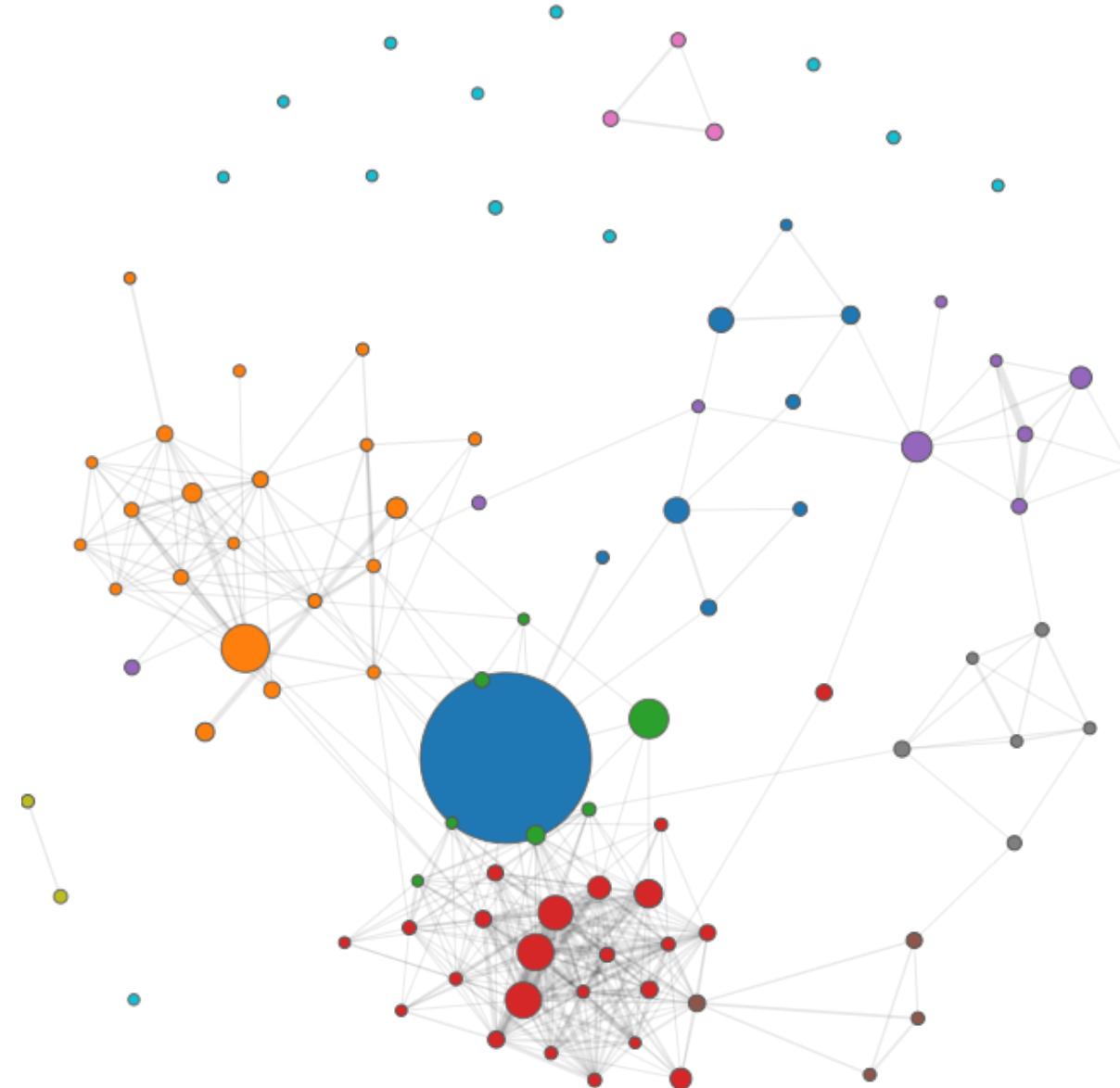
Surveillance:

Catch-all, white-lists, black-lists, or case-based?

What about metadata? What is metadata?

Data about data
But is that sensitive material?!

Metadata



An aerial photograph of a massive industrial complex, likely a data center, situated in a valley. The facility consists of numerous large, white, rectangular buildings arranged in a grid-like pattern. In the foreground, there are several smaller buildings and parking lots. A major highway cuts through the valley floor, with traffic visible. The surrounding terrain is a mix of dry, brown fields and green pastures. In the background, a range of mountains is visible under a sky filled with scattered clouds.

Surface

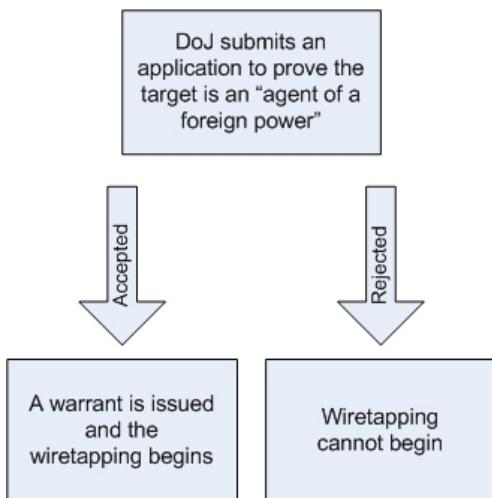
Lower-bound capacity estimates:

3 exabytes to 5 zettabytes (3 million to 5 billion terabytes)

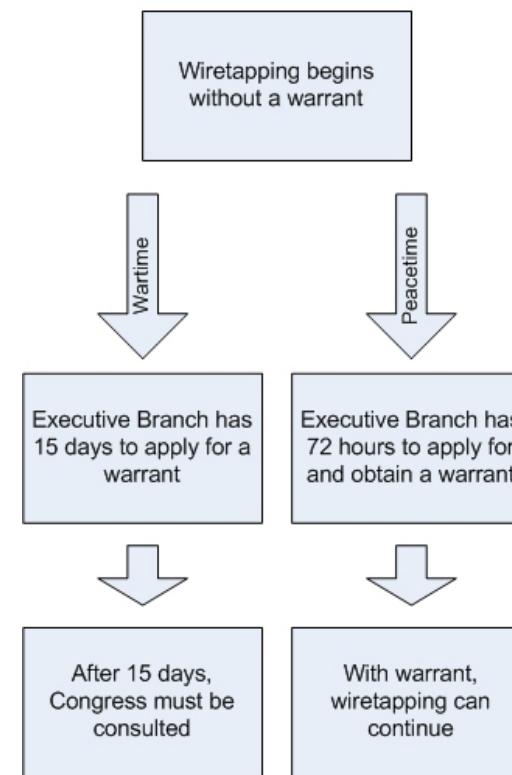


Search warrants

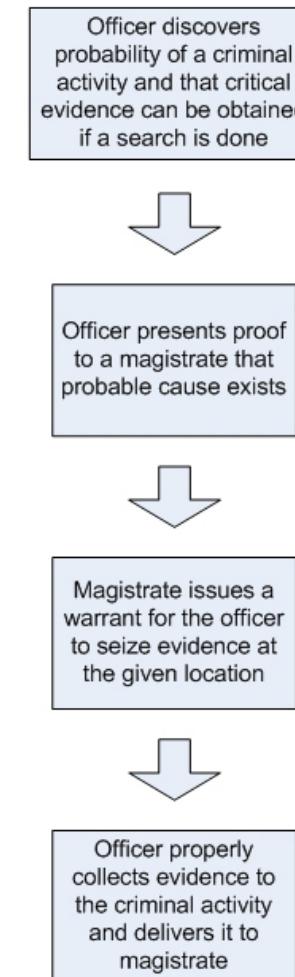
Obtaining a FISA Wiretap Warrant Under Non-urgent Circumstances



Obtaining a FISA Wiretap Warrant Under Urgent Circumstances



Obtaining a Normal, non-Wiretapping Search Warrant





24

A non-anarchist solution to the surveillance dilemma

- Lawrence Lessig's solution
 - All data must be encrypted
 - The keys to decryption must be in the hands of justice
 - Courts may decide to reveal keys on a case-by-case basis
 - No master key

Encryption

- Hashing
 - Irreversible
 - MD5/SHA: Authenticity verification
- Symmetric Methods
 - The key must remain secret (encoding/decoding using the same key)
 - AES: Your wifi
- Asymmetric Methods
 - There is a public key and a private key
 - RSA/PGP: SSL, hard disk encryption, etc...