Big brother and little brother: The future of privacy

Mark Ryan
University of Birmingham

17th May 2011
4 kB
1 MHz
1981

4 kB
13 MHz
2003
Ihr Abendmenü im April
Täglich ab 18 Uhr

Frühlingssalate mit Wildkräutern und Parmesan im Speckmantel

Vanille-Zander auf Topinambur-Rhabarber mit Lavendel und Kartoffelpüree

Schmandtörtchen mit Holunderragout

dazu pro Person 1/2 Liter Weißwein
The future
Vint Cerf  
co-inventor of TCP/IP  
ACM Turing Award 2004  
Vice president, chief Internet evangelist, Google

Steve Jobs  
chairman and CEO of Apple Inc.

Eric Schmidt  
former CEO of Google

Mark Zuckerberg  
CEO, co-founder of Facebook
1. Wearable computers
2. Cyber-physical systems
Cyber-physical systems integrate the physical world into the electronic world

- They allow us to electronically manage and interact with the physical world. Physical objects are seamlessly integrated into the information network.

**Applications**

**Industry:** aerosp., autom., chemical plants, transp., farming

**Daily life:** healthcare, traffic mgt, finding your wallet, finding your grandmother

**Billions of sensors** (RFID, temp., web cams, Geiger ctrs., seismic);

**Everything is tagged** at manufacture time (clothes, food packets, cups, keys, phones, pets, people, vehicles, tools)

**The Internet of things**
physical
sensors
- cameras, RFID, GPS,
  - seismic, Geiger,
  - temperature, infra-red

actuators
- motors, servos,
  - speakers, controllers,
  - robotics, appliances
digital
3. Cloud computing
What all this enables...
Ben Smyth
facebook.com
- born 26 Oct 1983,
- interested in women.
bham.ac.uk:
- research student
loria.fr: CNRS engineer
bensmyth.com: Worked on Helios voting system.
• Met her at INFOSEC’28.
• Works on public key crypto.

• Student at UoB, 2026-29.
• Did project on image analysis.

• Works for IBM.
• Participates on EU FP14 project “AVANTSSAR”.
“Simply speak a question, or just think it, and an answer will return from a vast, collectively produced data matrix. Google queries will seem quaint.”

David Kirkpatrick, 2006
CNN Fortune senior editor
name: Cynthia Jones
age: 25
status: single
lives: Birmingham, UK
likes: Italian restaurants, cats, romantic films

Back
dailymail.co.uk
Won £20M in lottery 2023.

meganslaw.com
Registered sex offender.

money.com
Hedge fund mgr, earns £15M/year.

telegraph.co.uk
Disqualified from driving 2028-32.
What privacy is

Restrictions on the processing and dissemination of information related to you.

- Privacy of communication
  - e-mail, phone calls, text messages, IMs, Facebook messages

- Privacy of behaviour
  - where you go, what you do, pages you visit

- Privacy of personal records
  - docs, photos, transactions, contributions, archives
  - health records, personnel records, judgements, reviews
<table>
<thead>
<tr>
<th>Threat from</th>
<th>Official</th>
<th>Unofficial</th>
</tr>
</thead>
</table>
| Big brother | Governments that have access to databases  
- transport  
- communications  
- financial | Governments that spy on their people |
| Governments | | |
| Middle brother | Companies that offer services  
- Transp./comms./financial  
- Gmail/Hotmail/Yahoo m.  
- Google docs  
- Facebook  
- Easychair | Companies that spy on your behaviour  
- ISP and phone netw. op.  
- Phorm  
- Facebook “like” button  
- Google analytics |
| Corporations | | |
| Little brother | Neighbours, friends and strangers who  
- point their phones at you  
- watch your facebook page | Neighbours that spy on you  
- Tracking your RFID tags  
- Tracking your phone |
| Individuals | | |
About 440,000 requests by the police, local authorities and other permitted organisations to monitor telephone calls, emails and text messages were requested in a 15 month period in 2005-06 in the UK.

There are 563 such permitted organisations.

The “Intercept Modernisation Programme” is a UK Government initiative to centralise electronic communications traffic data in the UK in a single database.

To combat terrorism, MI5 and MI6 have sought full automated access to Transport for London’s “Oyster” smartcard database.
Chinese Government Ordered Hack on Google Servers: Wikileaks

By: Clint Boulton  
2010-11-29

There are 0 user comments on this IT Security & Network Security News & Reviews story.

Wikileaks gave the New York Times a diplomatic cable that shows the Chinese government was responsible for the hack on Google's Gmail system.

China's government was indeed behind the hack on Google's Gmail system earlier this year according to a cable captured by the controversial Wikileaks organization.

Wikileaks, which butters its bread collecting secret documents and seeding them in media outlets, snagged 250,000 American diplomatic cables dating back three years and released some of them to the New York Times and other media outlets.

The Times cited one of the cables as proof that "China's Politburo directed the intrusion into Google's computer systems in that country, a Chinese contact told
Introduction

Vertigo is the sensation that you or the environment around you is moving or spinning. It is commonly caused by a problem with the balance mechanisms within the inner ear.

If you have vertigo, you may experience the sensation of movement even when you are standing completely still.

**Vertigo is not a fear of heights**

Vertigo is often confused with a fear of heights. However, the dizzy feeling that is often experienced when looking down from a high place is not the same as vertigo, which can occur at any time and may last for many months or even years.

Mild vertigo is very common, and the symptoms are not usually serious. However, vertigo that recurs or persists may be caused by an underlying health condition, such as Ménière's disease (a rare disorder that affects the inner ear).

Therefore, if you have recurrent or persistent vertigo, see your GP. They will be able to confirm or rule out a more serious cause, and recommend appropriate treatment.
Visit
nhs.co.uk/vertigo

Alice's browser
fetch
nhs.co.uk/vertigo
web page with fb button

Alice has visited nhs.co.uk/vertigo

Friends of Alice that like that page

with friends who like it

nhs.co.uk/vertigo
Don’t use Facebook?
Even if you don’t even have a Facebook account, Facebook can still track your activity!
It can serve you a cookie (containing a random identifier), and track your use by linking it to that.
Web searches

- single men in their 60s
- dog that urinates on everything
- several people with surname Arnold
- landscapers in Lilburn, Georgia

Thelma Arnold, 62 from Lilburn, Georgia, who loves her three dogs.
Scott McNealy, CEO Sun Microsystems, 1999

“Consumer privacy issues are a red herring. You have zero privacy anyway. Get over it.”
Larry Ellison, CEO Oracle, 2001

“All you have to give up is your illusions. Right now, you can go onto the Internet and get a credit report about your neighbour, find out where he works and how much he earns.”
Eric Schmidt, CEO Google, 2009
“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”
Mark Zuckerberg, CEO Facebook, 2010

“Privacy is no longer a social norm. People are comfortable sharing more information, and different kinds, and with more people.”
Is that true?
Do people want privacy, and if so, why?
People do want privacy, in order to avoid...

- incorrect conclusions, resulting from deliberate or accidental errors in the data, or misinterpretations, or prejudice
- blackmail or extortion, or other abuse of power
- commercial pestering (spam)

Privacy concerns all aspects of live, including past relationships, political views, financial affairs, past deeds, and also the trivia of everyday life.

Problem: people might abuse privacy to do bad things...

- commit fraud, evade taxes
- trade in child pornography images
- commit terrorism, to kill or injure without being detected
- commandeer a botnet to take down Google
The privacy challenge

- How to balance
  - *privacy* and *accountability*
  - *individual privacy* and *societal security*

- How to build systems that support this balance?
- (Legislation is important too)
Vision

To design, build and evaluate technologies that support appropriate kinds of privacy.

Examples:

- absolute
- relative to interrogator
- verifiable-conditional

Example: your vote.

To ensure free and fair elections, your vote should be completely private to you. It should not be accessible by potentially corrupt election officials, programmers, administrators, or indeed anyone, ever.
Vision

To design, build and evaluate technologies that support appropriate kinds of privacy.

Examples:

- absolute
- relative to interrogator
- verifiable-conditional

Example: e-mail, Facebook, online documents.

Typically, we want data to be confidential from the service provider, while still allowing the provider to route the data to the intended receiver.

Can be very hard to achieve.
To design, build and evaluate technologies that support appropriate kinds of privacy.

Examples:

- absolute
- relative to interrogator
- verifiable-conditional

**Example:** Oyster card usage, mobile phone usage, ISP logs.

Data may be accessed only by authorised agents, and only under certain conditions. The presence/absence of the conditions and of the access are verifiable by the user.
1. The TPM as a privacy-enhancing technology
The trusted platform module

Infineon

TPM1.2
SLB 9635 TT 1.2
Digital rights management

unforgeable configuration report

Secure environment
“With a plan they call trusted computing, large media corporations, together with computer companies such as Microsoft and Intel, are planning to make your computer obey them instead of you.”

He calls it “treacherous computing”.

Richard Stallman
Creator of GNU, Emacs, GCC, GPL, the Free Software Foundation
“TC can support remote censorship. In its simplest form, applications may be designed to delete pirated music under remote control.”

“No 2010 President Clinton may have two red buttons on her desk - one that sends the missiles to China, and another that turns off all the PCs in China.”

He also talks of commercial bullying, economic warfare and political censorship.
Attestation from cloud
What we are doing about the TPM

- Improvements to its specification
- Developing languages for describing its behaviour and verifying its properties
- Developing methods for using it in cloud-based applications
\[\text{and } H = H \land \text{message}(\phi_0, \rho(M), x)\]

\[
\begin{align*}
\left[\text{in}(M, x); Q\right] \rho \mathcal{H} \ell \phi \text{true} & = [Q]((\rho \cup \{x \mapsto x\})(H \land \text{message}(\phi, \rho(M), x))(x :: \ell)\phi \text{true} \\
\left[\text{out}(M, N); Q\right] \rho \mathcal{H} \ell \phi \mu & = \{H \Rightarrow \text{message}(\phi, \rho(M), \rho(N))\} \cup [Q] \rho \mathcal{H} \ell \phi \mu \\
[\text{let } x = g(M_1, \ldots, M_n) \text{ in } Q_1 \text{ else } Q_2]\rho \mathcal{H} \ell \phi \mu & = \bigcup \left\{ \left[Q_1\right]\rho(\sigma \cup \{x \mapsto p'\sigma'\})(H\sigma)(\ell\sigma)(\phi\sigma)\mu \mid \begin{array}{c}
g(p'_1, \ldots, p'_n) \rightarrow p' \in \text{dom}(g) \text{ and } (\sigma, \sigma') \text{ mgus and} \\
M_1\rho\sigma = p'_1\sigma', \ldots, M_n\rho\sigma = p'_n\sigma' \end{array} \right\} \cup \left[Q_2\right] \rho \mathcal{H} \ell \phi \mu \\
\left[\text{if } M = N \text{ then } Q_1 \text{ else } Q_2\right] \rho \mathcal{H} \ell \phi \mu & = [Q_1](\rho\sigma)(H\sigma)(\ell\sigma)(\phi\sigma)\mu \cup [Q_2] \rho \mathcal{H} \ell \phi \mu \quad \text{where } \sigma = \text{mgus}(\rho(M), \rho(N)) \\
[\text{lock}; Q] \rho \mathcal{H} \ell \phi \text{false} & = [Q](\rho \cup \{vs \mapsto vs, \ldots, vs_n \mapsto vs_n\})H\ell\phi_0\text{true} \\
& \quad \text{where } \phi_0 = (vs_1, \ldots, vs_n), \text{ with } vs_1, \ldots, vs_n \text{ fresh} \\
[\text{unlock}; Q] \rho \mathcal{H} \ell \phi \text{true} & = [Q] \rho \mathcal{H} \ell \phi \text{false} \\
[s_i := M; Q] \rho \mathcal{H} \ell \phi \text{false} & = [Q](\rho \cup \{vs_1 \mapsto vs_1, \ldots, vs_n \mapsto vs_n, vc \mapsto vc, vm \mapsto vm\})H\ell\phi_0\text{false} \\
& \quad \cup \{H \land \text{message}(\phi_0, vc, vm) \Rightarrow \text{message}(\phi_1, vc, vm)\} \\
& \quad \cup \{H \land \text{attacker}(\phi_0, vm) \Rightarrow \text{attacker}(\phi_1, vm)\} \\
& \quad \text{where } \phi_0 = (vs_1, \ldots, vs_i-1, vs_i, vs_{i+1}, \ldots, vs_n), \\
& \quad \text{and } \phi_1 = (vs_1, \ldots, vs_i-1, \rho(M), vs_{i+1}, \ldots, vs_n) \\
& \quad \text{with } vs_1, \ldots, vs_n, vc, vm \text{ fresh} \\
[s_i := M; Q] \rho \mathcal{H} \ell \phi \text{true} & = [Q](\rho \cup \{vc \mapsto vc, vm \mapsto vm\})H\ell\phi_0\text{true} \\
& \quad \cup \{H \land \text{message}(\phi, vc, vm) \Rightarrow \text{message}(\phi', vc, vm)\} \\
& \quad \cup \{H \land \text{attacker}(\phi, vm) \Rightarrow \text{attacker}(\phi', vm)\} \\
& \quad \text{where } \phi = (M_1, \ldots, M_{i-1}, M_i, M_{i+1}, \ldots, M_n), \\
& \quad \text{and } \phi' = (M_1, \ldots, M_{i-1}, \rho(M), M_{i+1}, \ldots, M_n), \\
& \quad \text{and } vc, vm \text{ fresh} \\
[\text{read } s_i \text{ as } x; Q] \rho \mathcal{H} \ell \phi \text{false} & = [Q](\rho \cup \{x \mapsto vs_1, vs_1 \mapsto vs, \ldots, vs_i \mapsto vs_i, \ldots, vs_n \mapsto vs_n, \} \\
& \quad vc \mapsto vc, vm \mapsto vm \setminus H \land \text{message}(\phi, vc, vm) \text{ false} \}
\end{align*}
\]
## EasyChair: the little Facebook

<table>
<thead>
<tr>
<th>Year</th>
<th>#confs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>2</td>
</tr>
<tr>
<td>2003</td>
<td>3</td>
</tr>
<tr>
<td>2004</td>
<td>7</td>
</tr>
<tr>
<td>2005</td>
<td>66</td>
</tr>
<tr>
<td>2006</td>
<td>276</td>
</tr>
<tr>
<td>2007</td>
<td>629</td>
</tr>
<tr>
<td>2008</td>
<td>1312</td>
</tr>
<tr>
<td>2009</td>
<td>2183</td>
</tr>
<tr>
<td>2010</td>
<td>3306</td>
</tr>
<tr>
<td>2011</td>
<td>$\geq 3690$</td>
</tr>
<tr>
<td>2012</td>
<td>$\geq 161$</td>
</tr>
<tr>
<td>2013</td>
<td>$\geq 5$</td>
</tr>
</tbody>
</table>
Reviewed papers by A.Gordon (CSF’11), D.Ghica (FCS’11), G.Steel (ESORICS’10), M.Fisher (FM’10), P.Panagaden (LICS’09), and others. Recommended reject for all of them.

Had papers reviewed by S.Kremer (S&P’10), A.Martin (TRUST’09), M.Huth (POPL’08), J.Fiadeiro (CAV’09), etc. They all recommended accept.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of papers submitted</td>
<td>25</td>
</tr>
<tr>
<td>Number of papers accepted</td>
<td>17</td>
</tr>
<tr>
<td>Acceptance rate</td>
<td>0.68</td>
</tr>
<tr>
<td>Number of papers reviewed</td>
<td>107</td>
</tr>
<tr>
<td>Number of times recommended accept</td>
<td>24</td>
</tr>
<tr>
<td>Recommendation agr. w. outcome</td>
<td>28%</td>
</tr>
<tr>
<td>Probability CSF 2012 re-invites him</td>
<td>0.2</td>
</tr>
<tr>
<td>Prob. will win ACM Turing award</td>
<td>$2^{-11.2}$</td>
</tr>
</tbody>
</table>
\[
\begin{align*}
&\{i_1, \ldots, i_k\} \leftarrow \{i \mid (A_i, P_i, R) \in DB\} \\
&DB_R \leftarrow [\{\text{subm}_{i_1}\}^{K_{conf}}; \ldots; \{\text{subm}_{i_k}\}^{K_{conf}}] \\
&\text{pick } s_1, \ldots, s_k \in S \\
&\text{create } r_1, \ldots, r_k \\
&DB'_R \leftarrow [\{\text{subm}_{i_1}, r_1, s_1\}^{K_{conf}}; \ldots; \{\text{subm}_{i_k}, r_k, s_k\}^{K_{conf}}] \\
&DB'_R \leftarrow DB_R @ DB_{rev}
\end{align*}
\]
2. Electronic voting
Electronic voting potentially offers
- efficiency
  - higher voter participation
  - greater accuracy
  - lower costs
- better security
  - vote-privacy even in presence of corrupt election authorities
  - voter verification, i.e. the ability of voters and observers to check the declared outcome against the votes cast.
Desired properties

Verifiability
- Outcome of election is verifiable by voters and observers
- You don’t need to trust election software

Incoercibility
- Your vote is private
  - even if you try to cooperate with a coercer
  - even if the coercer is the election authorities

Usability
- Vote & go
- Verify any time
What we are doing in electronic voting

- Developing solutions that achieve these combinations of properties
- Developing methods for describing its properties, and verifying solutions against them

Incoercibility:

Let $P$ be a process and $C = \text{new } c_1, \text{new } c_2$. If $\neg n \cap fn(C) = \emptyset$ then $\text{new } v \setminus V A \{ ?/v \}$, $c_1, c_2$ $\approx \ell S [C | V A \{ a/v \}]$

Verifiability:

Soundness $\forall i, j. \Phi IV(v_i, r_i, y) \land \Phi IV(v_j, r_j, y) \Rightarrow i = j \quad (1)$

$\Phi UV(\tilde{v}, \tilde{y}, p) \land \Phi UV(\tilde{v}', \tilde{y}, p) \Rightarrow \tilde{v} \approx \tilde{v}' \quad (2)$

Effectiveness $\forall i. \Phi IV(v_i, r_i, y_i) \land \Phi UV(\tilde{v}', \tilde{y}, p) \Rightarrow \tilde{v} \approx \tilde{v}' \quad (3)$
Incoercibility:
VP is coercion resistant if there exists a process $V'$ such that for any $C = \text{new } c_1.\text{new } c_2.(\_ | P)$ satisfying
- $\tilde{n} \cap fn(C) = \emptyset$
- $S[C[V_A{?/\nu}^{c_1,c_2} | V_B{a/\nu}]] \approx_{\ell} S[V_A{c/\nu}^{c_2} | V_B{a/\nu}]$
we have
- $C[V'] \setminus \text{out}(\text{chc},\cdot) \approx_{\ell} V_A{a/\nu}$,
- $S[C[V_A{?/\nu}^{c_1,c_2} | V_B{a/\nu}]] \approx_{\ell} S[C[V'] | V_B{c/\nu}]$.

Verifiability:

Soundness
\[ \forall i, j. \quad \Phi^{IV}(v_i, r_i, y) \land \Phi^{IV}(v_j, r_j, y) \Rightarrow i = j \quad (1) \]
\[ \Phi^{UV}(\tilde{v}, \tilde{y}, p) \land \Phi^{UV}(\tilde{v}', \tilde{y}, p) \Rightarrow \tilde{v} \simeq \tilde{v}' \quad (2) \]
\[ \bigwedge_{1 \leq i \leq n} \Phi^{IV}(v_i, r_i, y_i) \land \Phi^{UV}(\tilde{v}', \tilde{y}, p) \Rightarrow \tilde{v} \simeq \tilde{v}' \quad (3) \]
\[ \Phi^{EV}(\tilde{w}, \tilde{y}, p) \land \Phi^{EV}(\tilde{w}', \tilde{y}, p) \Rightarrow \tilde{w} \simeq \tilde{w}' \quad (4) \]
\[ \bigwedge_{1 \leq i \leq n} \Phi^{IV}(v_i, w_i, r_i, y_i) \land \Phi^{EV}(\tilde{w}', \tilde{y}, p) \Rightarrow \tilde{w} \simeq \tilde{w}' \quad (5) \]

Effectiveness
\[ \bigwedge_{1 \leq i \leq n} \Phi^{IV}(v_i, w_i, r_i, y_i) \land \Phi^{EV}(\tilde{w}, \tilde{y}, p) \land \Phi^{EV}(\tilde{w}, \tilde{y}, p') \Rightarrow \tilde{y} \simeq y' \quad (6) \]
\[ \bigwedge_{1 \leq i \leq n} \Phi^{IV}(v_i, w_i, r_i, y_i) \land \Phi^{UV}(\tilde{v}, \tilde{y}, p) \land \Phi^{EV}(\tilde{w}, \tilde{y}, p) \quad (7) \]
Big brother and little brother
Big, middle and little brother (?)