Big brother and little brother: The future of privacy

Mark Ryan
University of Birmingham

17th May 2011

1977

1981


VIEW
System free 25086
Editing No File
Screen mode 7
=>
40T SS 100K

1981


Windows 7
SAMSUNG


Windows 7
SAMSUNG


DELL

2003

4 kB
1 MHz
1981

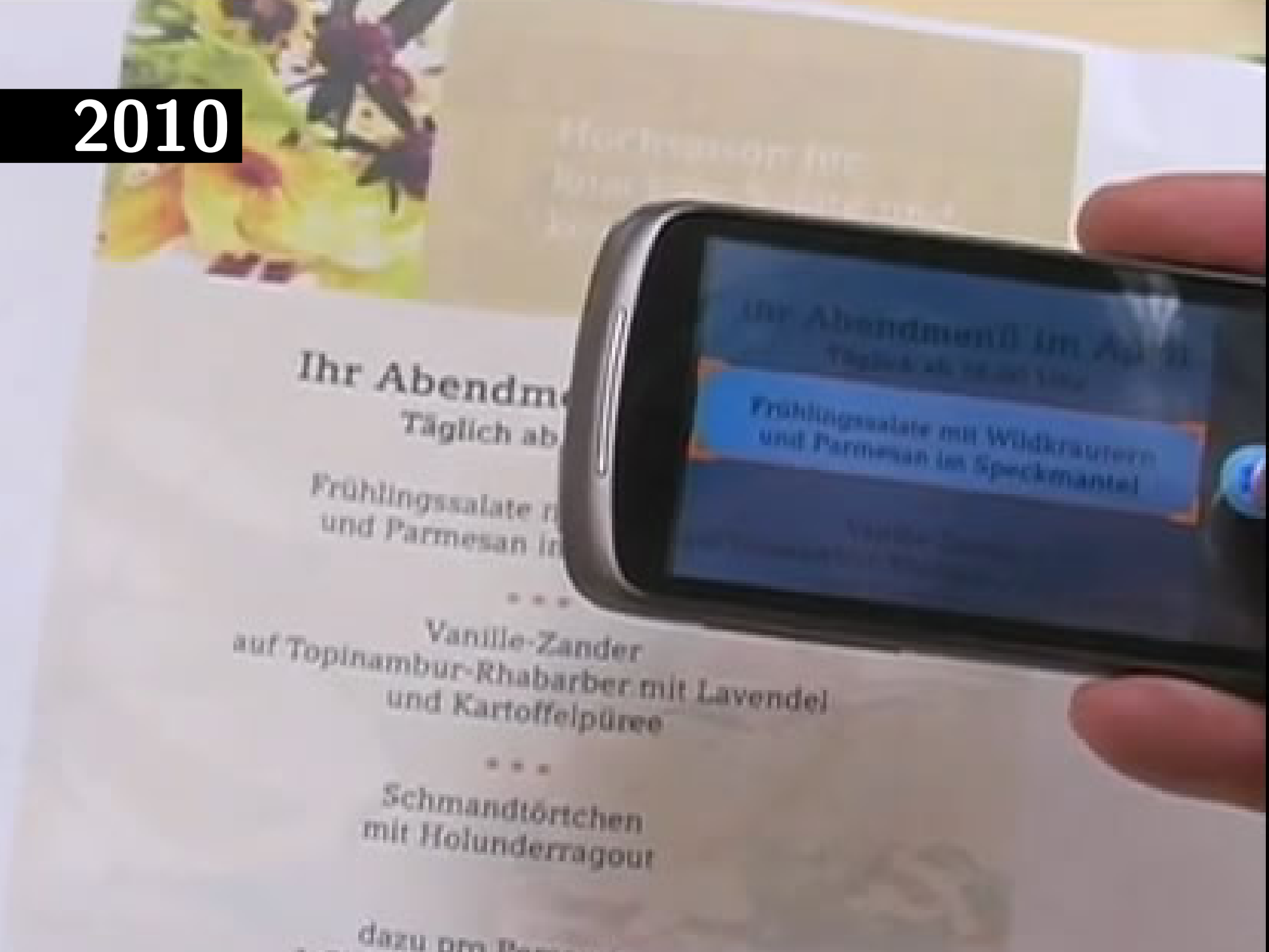
4 kB
13 MHz
2003

2007

2010

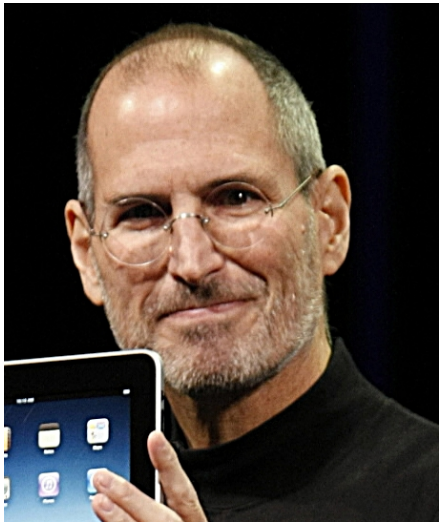

Google goggles labs
Landmark
Golden Gate Bridge
www.panora...
Golden Gate Bridge
Web Results
Golden Gate Bridge - Wikipedia, the free encyclopedia
The Golden Gate Bridge by night, with part of downtown San Francisco ... Golden Gate Bridge is the most popular place to commit suicide in the United States ...
http://en.wikipedia.org/wiki/Golden_Gate_Bridge
Seacliff Webcam - Weather Seacliff, Golden

2010


Ihr Abendm
Täglich ab
Frühlingssalate r
und Parmesan in
* * *
Vanille-Zander
auf Topinambur-Rhabarber mit Lavendel
und Kartoffelpüree
* * *
Schmandtörtchen
mit Holunderragout
dazu pro
Ihr Abendmenü im A
Frühlingssalate mit Wildkräutern
und Parmesan im Speckmantel

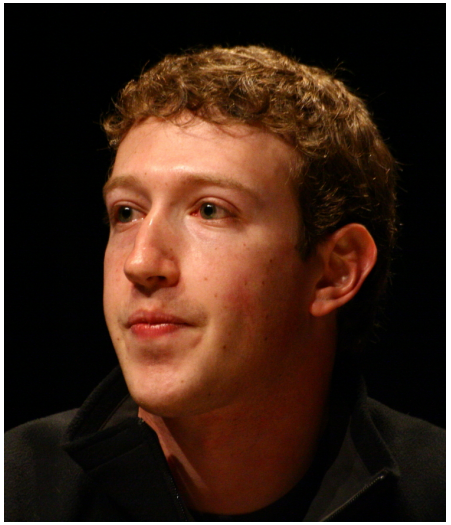
The future

Vint Cerf
co-inventor of TCP/IP
ACM Turing Award 2004
Vice president, chief Internet evangelist, Google



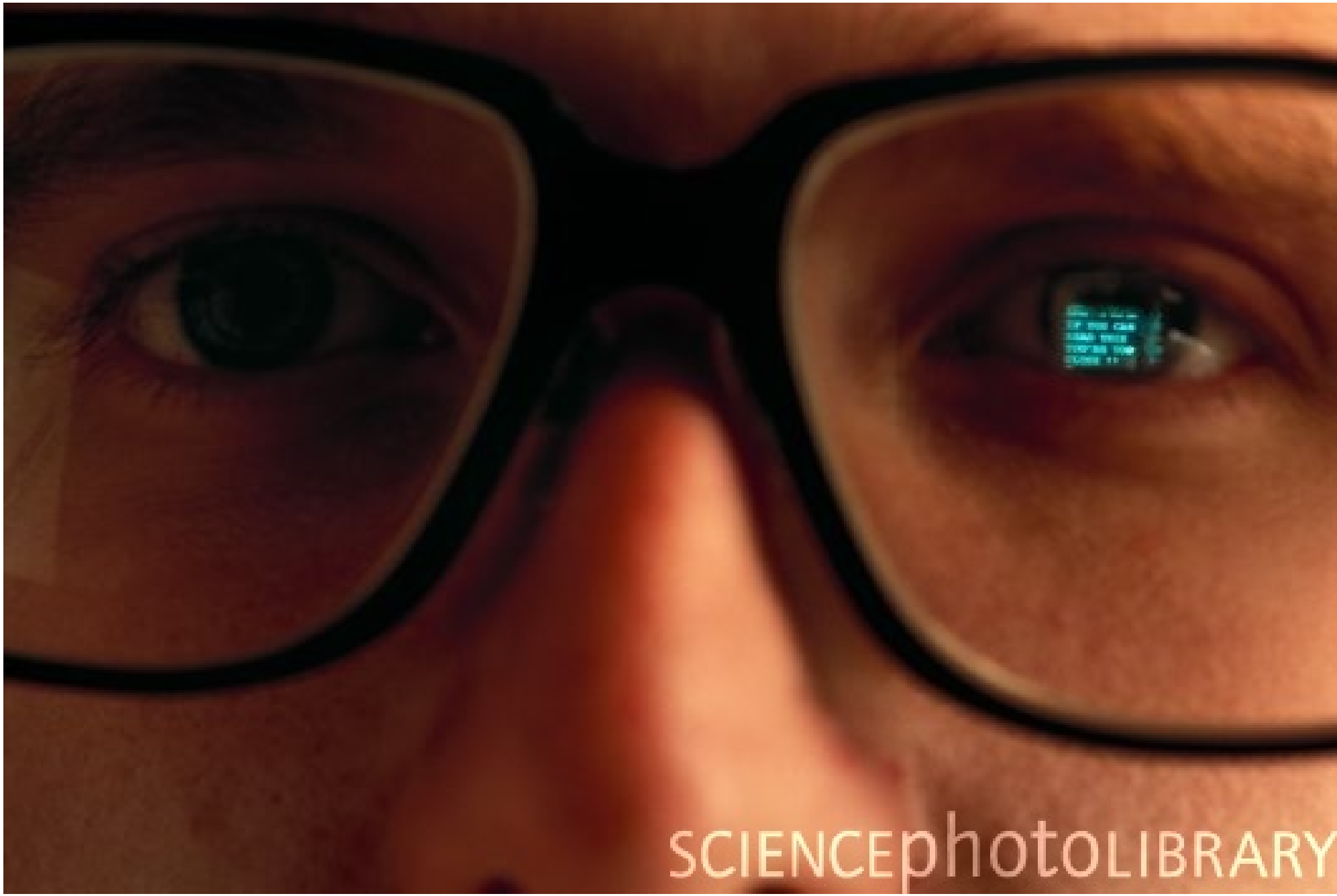
Steve Jobs
chairman and CEO of Apple Inc.

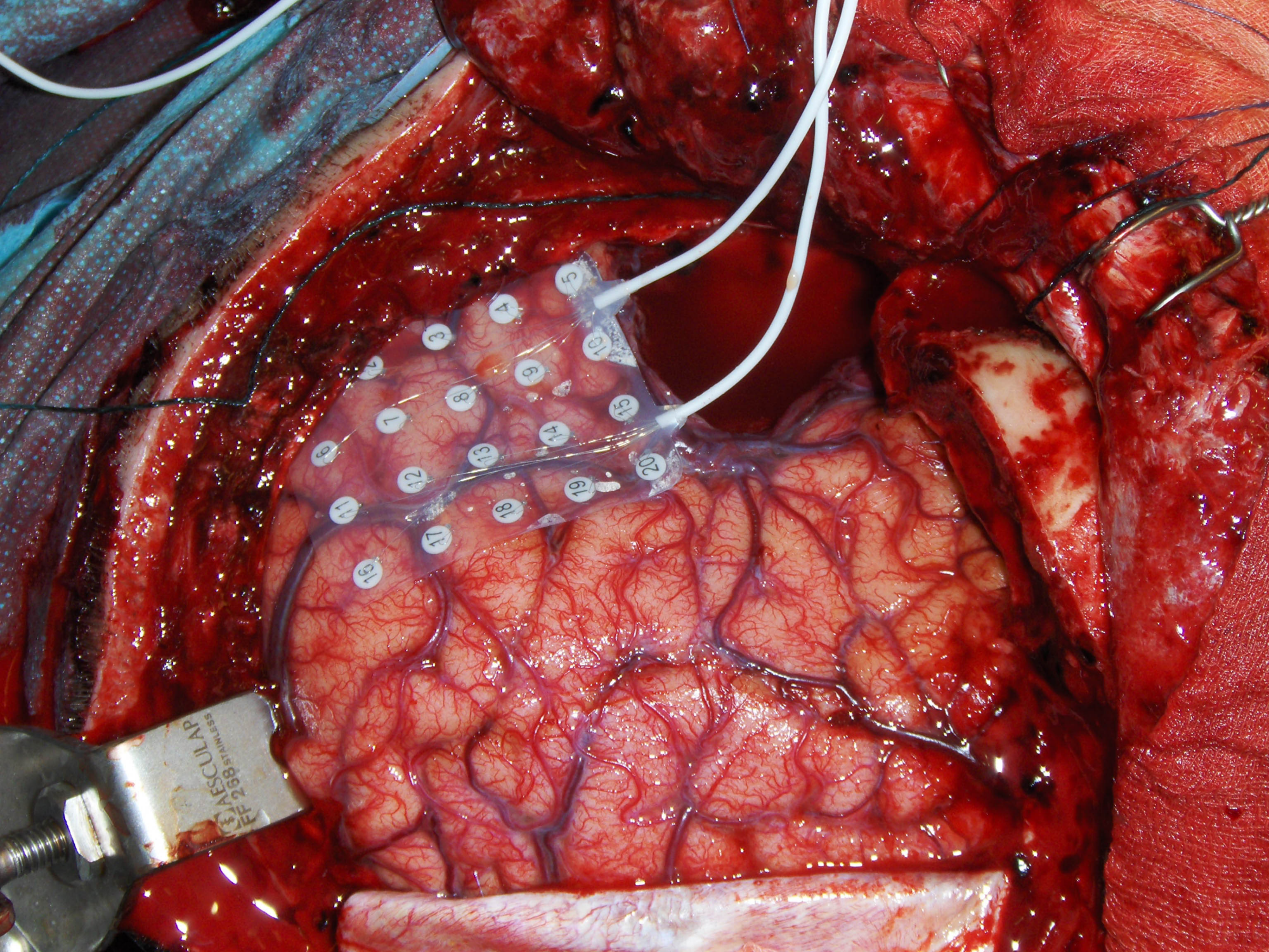
Eric Schmidt
former CEO of Google



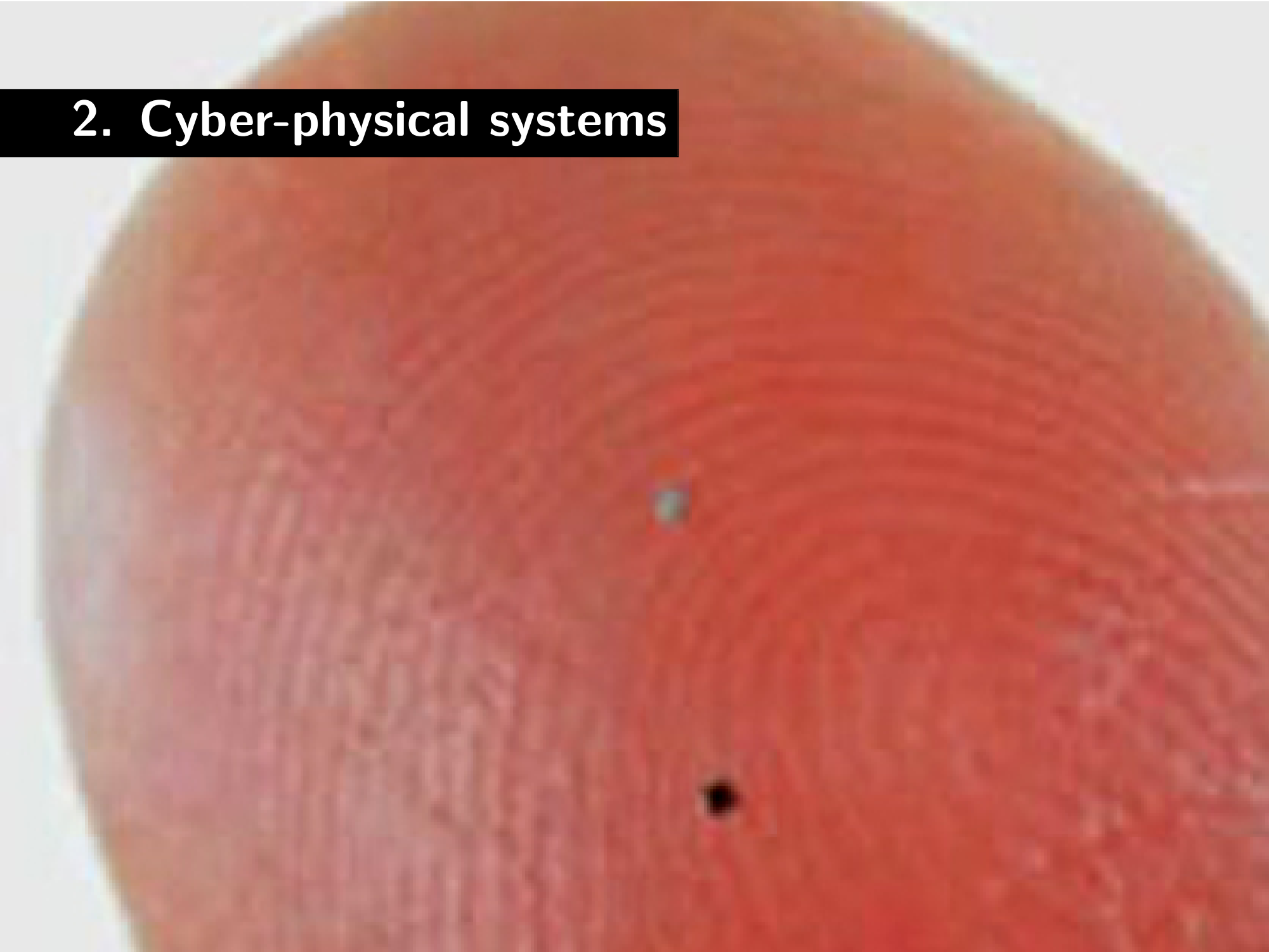
Mark Zuckerberg
CEO, co-founder of Facebook

1. Wearable computers


SCIENCEphotoLIBRARY


AESCULAP
FF 288 STAINLESS

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, verhicles, tools)

The Internet of things

Cyber-physical systems integrate the physical world into the electronic world

- T the p d into t

Applic

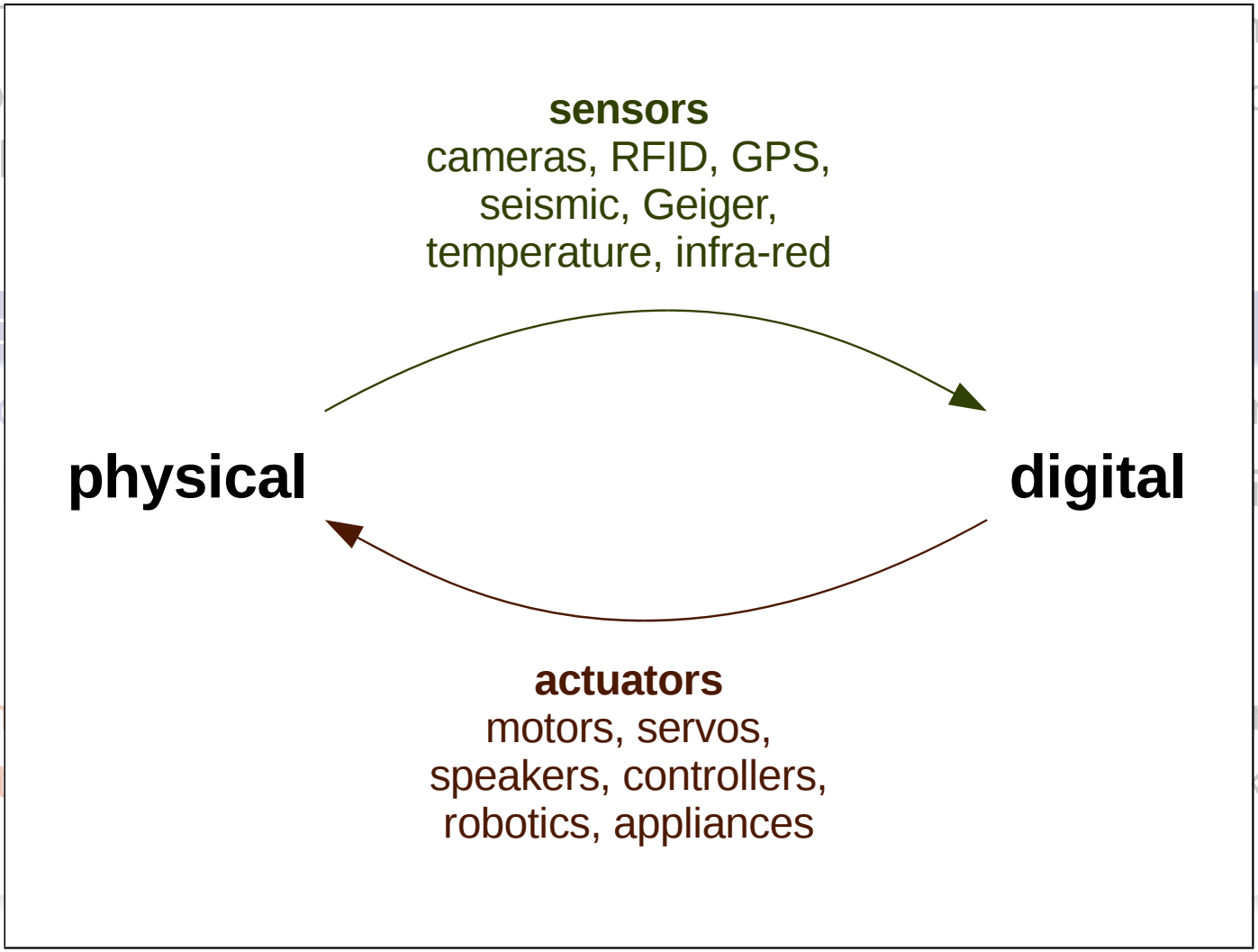
In ng

Da ing

Billion mic);

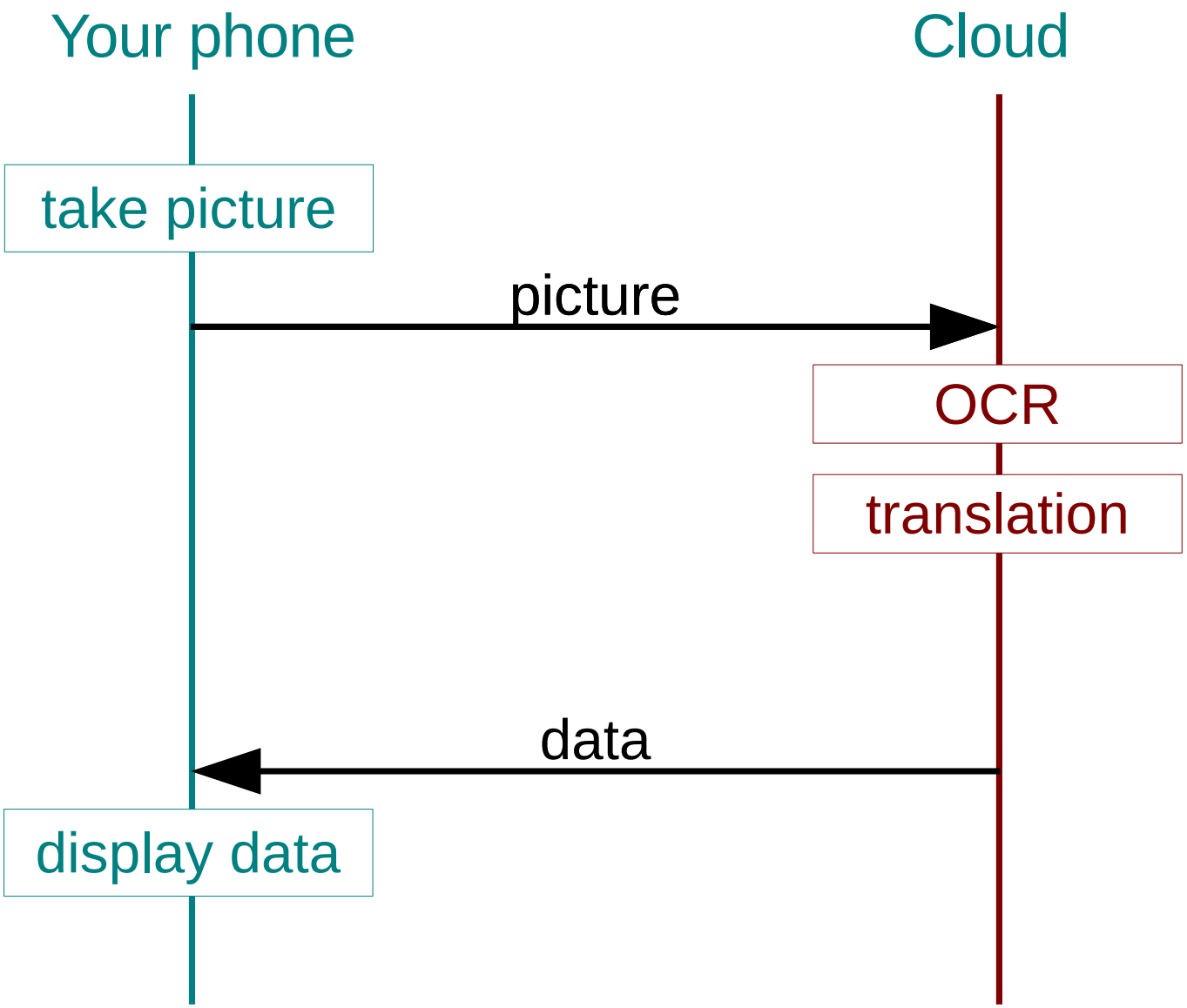
Everyt kets,

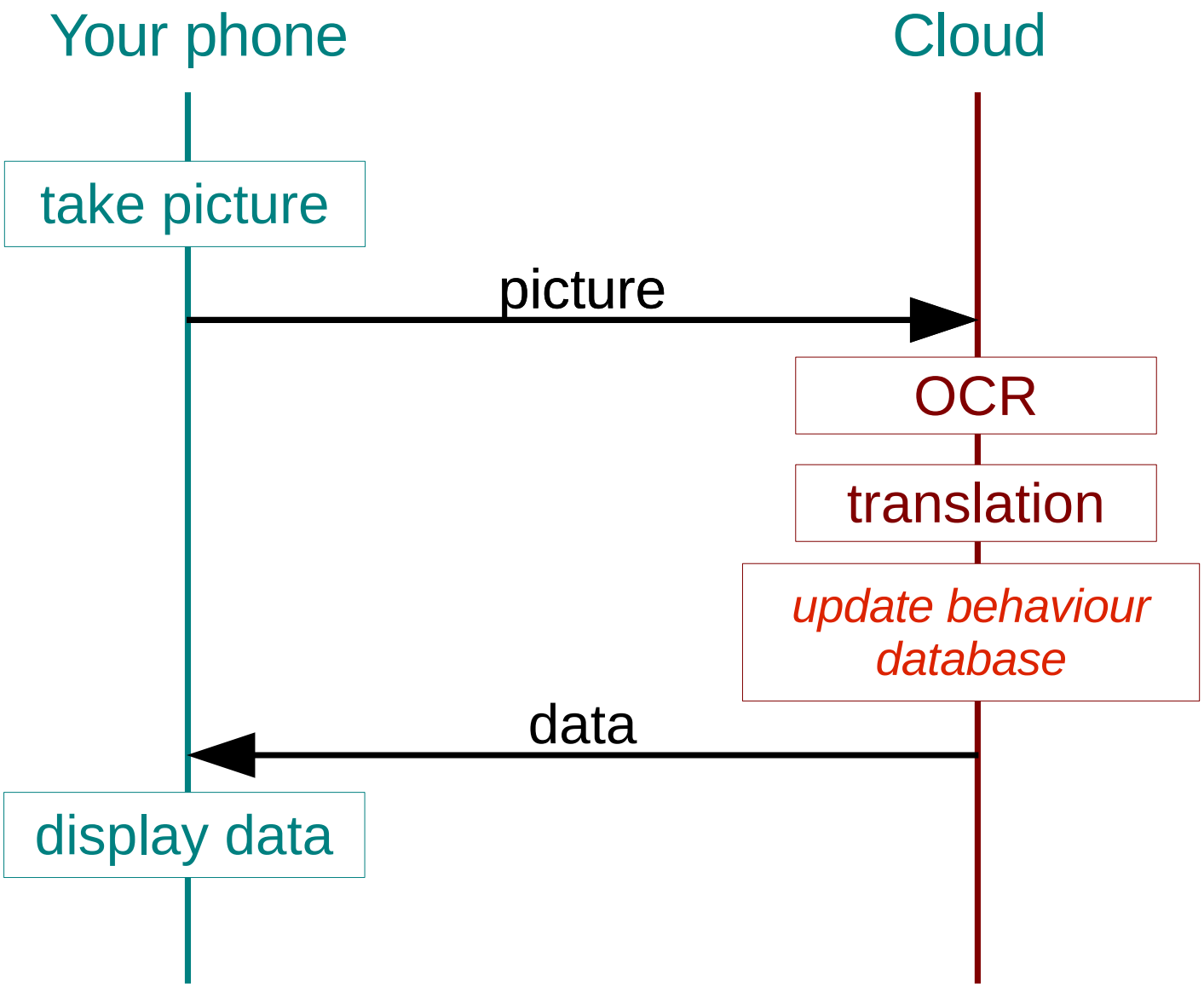
cups,



The Internet of things

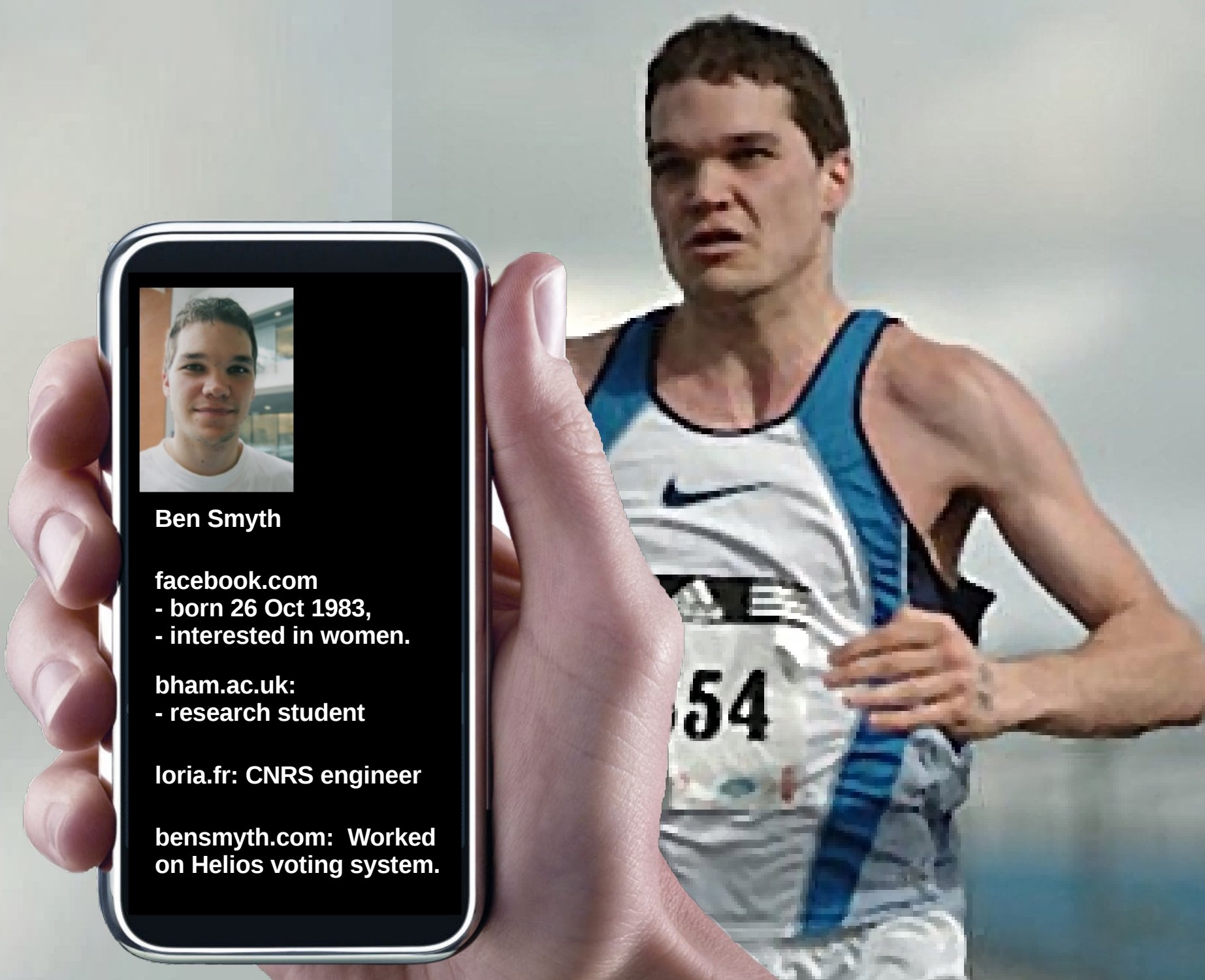
3. Cloud computing


Your phone
Cloud
take picture
picture
OCR
translation
data
display data


Your phone
Cloud
take picture
picture
OCR
translation
update behaviour database
data
display data

What all this enables. . .


2354


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.
54

- 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

Privacy


2 (1510)
17:05
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

Big brother

Governments

Threat from

Big brother

Governments

Middle brother

Corporations

Threat from

Big brother

Governments

Middle brother

Corporations

Little brother

Individuals

Threat from	**Official**
Big brother Governments	
Middle brother Corporations	
Little brother Individuals	

Threat from	**Official**	**Unofficial**
Big brother Governments		
Middle brother Corporations		
Little brother Individuals		

Threat from	**Official**	**Unofficial**
Big brother Governments	Governments that have access to databases • transport • communications • financial	
Middle brother Corporations		
Little brother Individuals		

Threat from	**Official**	**Unofficial**
Big brother Gover	Governments that have access to databases • transport	
Middl brothe Corpo		
Little brother 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.

  G. Crossman, H. Kitchen, R. Kuna, M. Skrein and J. Russell. Overlooked: Surveillance and personal privacy in modern Britain. Published by Liberty. www.liberty-human-rights.org.uk. October 2007.

- There are 563 such permitted organisations.

  Report by Interception of Communications Commissioner, 2007. Guardian, 27th February 2007.

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

  H. M. Government. The United Kingdom Security & Counter-Terrorism Science & Innovation Strategy. security.homeoffice.gov.uk/news-publications/publication-search/general/science-innovation-strategy1, 2007.

- To combat terrorism, MI5 and MI6 have sought full automated access to Transport for London's "Oyster" smartcard database.

  The Register. Spooks want to go fishing in Oyster database. www.theregister.co.uk/2008/03/17/spooks_want_oyster.

Threat from	**Official**	**Unofficial**
Big brother Governments	Governments that have access to databases • transport • communications • financial	
Middle brother Corporations	Companies that offer services • Transp./comms./financial • Gmail/Hotmail/Yahoo m. • Google docs • Facebook • Easychair	
Little brother Individuals		

Threat from	**Official**	**Unofficial**
Big brother Governments	Governments that have access to databases • transport • communications • financial	
Middle brother Corporations	Companies that offer services • Transp./comms./financial • Gmail/Hotmail/Yahoo m. • Google docs • Facebook • Easychair	
Little brother Individuals	Neighbours, friends and strangers who • point their phones at you • watch your facebook page	

Threat from | Official | Unofficial

Big br

Gover

Middl
brothe

Corpo

Little
brothe

Indivi

Facebook

Facebook users warned of burglary risk

Users of social networking sites such as Facebook and Twitter have been warned by police after two men were convicted of burgling a house whose owners had advertised the fact they were away.

Facebook users warned of burglary risk Photo: AP

By Nick Britten 4:41PM BST 15 Sep 2010

Comments

While fans of social media like to post broadcast every move, police said it can have a highly detrimental effect as it leaves their homes at the mercy of criminals.

And now insurers are warning they face higher insurance premiums if they were the victims of crime having publicised being away.

Wisbech magistrates' court heard that Peter Trower, 22 and

Facebook

News » UK News »
Twitter » Crime »

IN TECHNOLOGY

Facebook.com email address for sale on eBay

MySpace surrenders to Facebook

Follow us on social media

THE TELEGRAPH ON FACEBOOK »

The Telegraph on Facebook

Like 18,338

TECHNOLOGY MOST VIEWED

TODAY | PAST WEEK | PAST MONTH

1. John James Audubon's birth celebrated by Google doodle
2. Sony to challenge Apple with two tablet computers
3. End of an era as last mechanical typewriters are sold
4. Party death schoolgirl learned about drugs on web, says teacher
5. Google accused of representing Rio de

Threat from	**Official**	**Unofficial**
Big brother Governments	Governments that have access to databases • transport • communications • financial	Governments that spy on their people
Middle brother Corporations	Companies that offer services • Transp./comms./financial • Gmail/Hotmail/Yahoo m. • Google docs • Facebook • Easychair	
Little brother Individuals	Neighbours, friends and strangers who • point their phones at you • watch your facebook page	

Threat fro

Big brothe

Governme

Middle brother

Corporatio

Little brother

Individuals

y on their

IT Security & Network Security News

Chinese Government Ordered Hack on Google Servers: Wikileaks

By: Clint Boulton
2010-11-29
Article Rating: ★★★★☆ / 9

Share

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

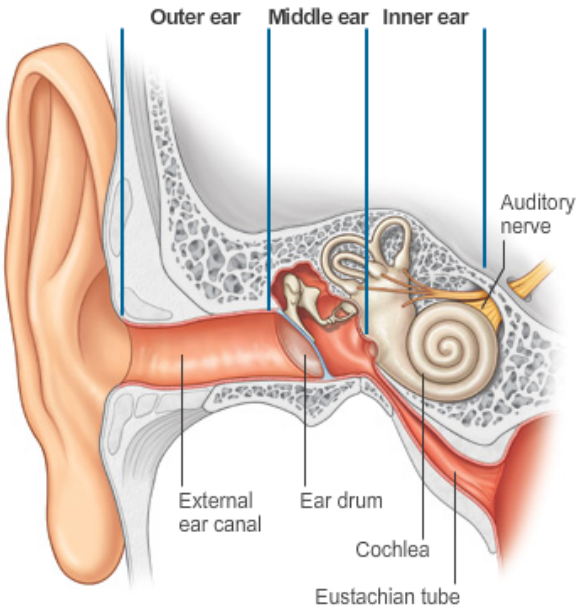
Threat from	**Official**	**Unofficial**
Big brother Governments	Governments that have access to databases • transport • communications • financial	Governments that spy on their people
Middle brother Corporations	Companies that offer services • Transp./comms./financial • Gmail/Hotmail/Yahoo m. • Google docs • Facebook • Easychair	Companies that spy on your behaviour • ISP and phone netw. op. • Phorm • Facebook "like" button • Google analytics
Little brother Individuals	Neighbours, friends and strangers who • point their phones at you • watch your facebook page	

Threat from | Official | Unofficial

Overview | Medicines info | Clinical trials

Vertigo | Symptoms | Causes | Diagnosis | Treatment | Prevention

Introduction



Learn more

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 reoccurs 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.

Like Horatiu Nicolae, Chris Sangwin and 13 others like this.

Last reviewed: 20/02/2009

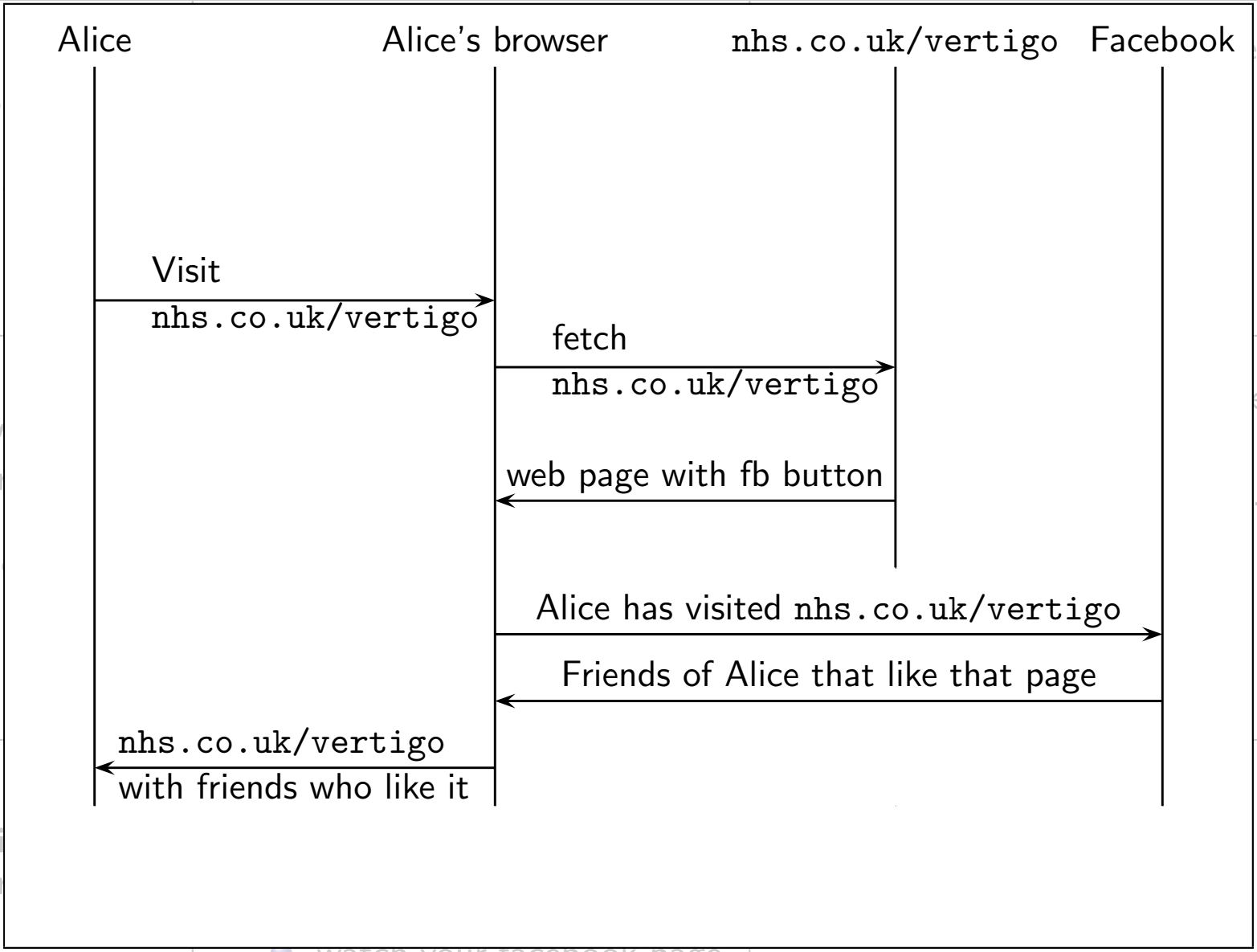
Next review due: 20/02/2011

Share: Save:

Done

Individuals

watch your facebook page

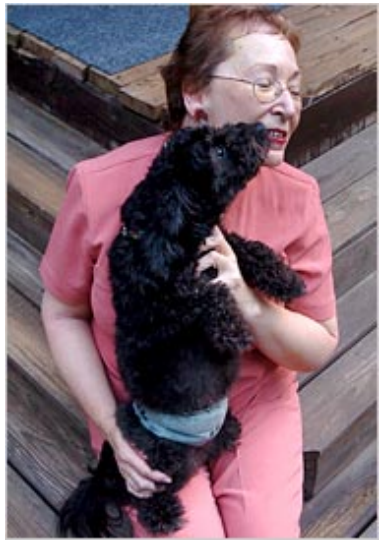

Alice
Alice's browser
nhs.co.uk/vertigo
Facebook
Visit
nhs.co.uk/vertigo
fetch
nhs.co.uk/vertigo
web page with fb button
Alice has visited nhs.co.uk/vertigo
Friends of Alice that like that page
nhs.co.uk/vertigo
with friends who like it

- 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.

Threat from	**Official**	**Unofficial**
Big	Governments that have access to	Governments that spy on their
Gov		
Mi bro		be-
Cor		p.
		n
Litt brother		
Individuals	point their phones at you watch your facebook page	

Web searches

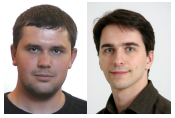
- single men in their 60s
- dog that urinates on everything
- several people with surname Arnold
- landscapers in Lilburn, Georgia



Thelma Arnold, 62 from Lilburn, Georgia, who loves her three dogs.

Threat from	**Official**	**Unofficial**
Big brother Governments	Governments that have access to databases • transport • communications • financial	Governments that spy on their people
Middle brother Corporations	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
Little brother Individuals	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

Threat from	**Official**	**Unofficial**
Big brot Governn	Governments that have access to	Governments that spy on their
Middle brother Corpora		your be- tw. op. utton
Little brother Individuals	point their phones at you watch your facebook page	you D tags Tracking your phone



Scott McNealy, CEO Sun Microsystems, 1999

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

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

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

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?

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.

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

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.

Vision

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

Digital rights management

unforgeable configuration report

WARNER BROS. ONLINE

Richard Stallman
Creator of GNU, Emacs, GCC, GPL, the Free Software Foundation

"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."

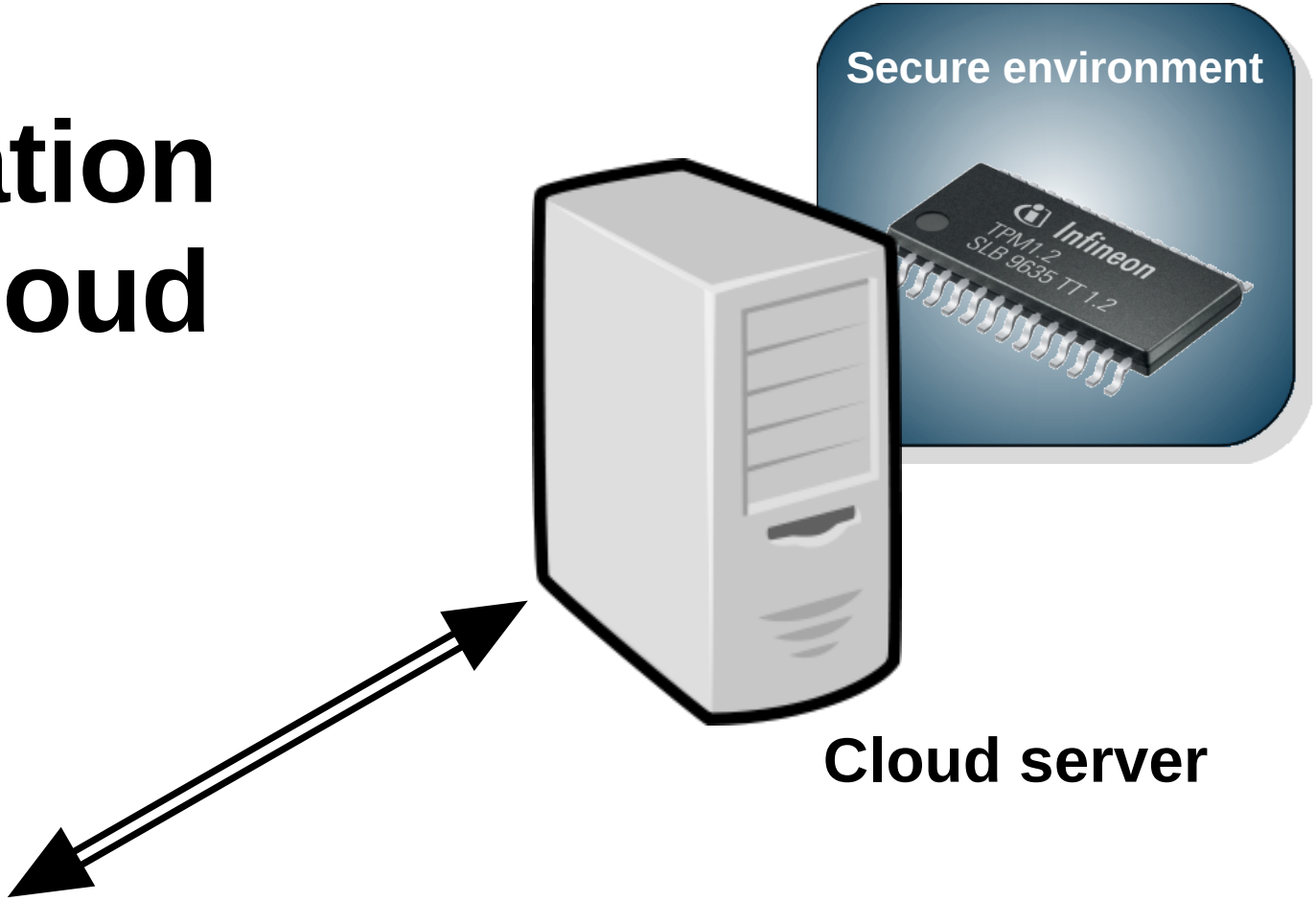
He calls it "treacherous computing".

Ross Anderson
Professor of Computer Security, University of Cambridge

- "TC can support remote censorship. In its simplest form, applications may be designed to delete pirated music under remote control."
- "In 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.

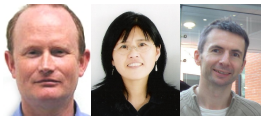
Attestation from cloud



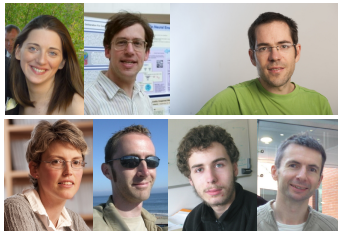
Cloud server

What we are doing about the TPM

- Improvements to its specification

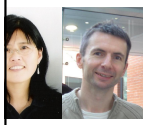


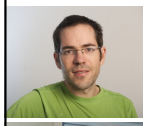
- Developing languages for describing its behaviour and verifying its properties

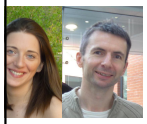


- Developing methods for using it in cloud-based applications

$$
\begin{aligned}
& \qquad\qquad\qquad\qquad\qquad\qquad \textbf{and } H' = H \wedge \mathsf{message}(\phi_0, \rho(M), x) \\
[\![\mathsf{in}(M,x);Q]\!]\rho H \ell \phi \mathsf{true} &= [\![Q]\!](\rho \cup \{x \mapsto x\})(H \wedge \mathsf{message}(\phi, \rho(M), x))(x :: \ell)\phi\mathsf{true} \\
[\![\mathsf{out}(M,N);Q]\!]\rho H \ell \phi \mu &= \{H \Rightarrow \mathsf{message}(\phi, \rho(M), \rho(N))\} \cup [\![Q]\!]\rho H \ell \phi \mu \\
[\![\text{let } x = g(M_1,\ldots,M_n) \text{ in} & \\
\qquad Q_1 \text{ else } Q_2]\!]\rho H \ell \phi \mu &= \bigcup \Big\{ [\![Q_1]\!]((\rho\sigma) \cup \{x \mapsto p'\sigma'\})(H\sigma)(\ell\sigma)(\phi\sigma)\mu \mid \\
& \qquad g(p'_1,\ldots,p'_n) \to p' \in def(g) \text{ and } (\sigma,\sigma') \text{ mgus and} \\
& \qquad M_1\rho\sigma = p'_1\sigma',\ldots,M_n\rho\sigma = p'_n\sigma' \Big\} \cup [\![Q_2]\!]\rho H \ell \phi \mu \\
[\![\text{if } M = N \text{ then } Q_1 & \\
\qquad \text{else } Q_2]\!]\rho H \ell \phi \mu &= [\![Q_1]\!](\rho\sigma)(H\sigma)(\ell\sigma)(\phi\sigma)\mu \cup [\![Q_2]\!]\rho H \ell \phi \mu \quad \textbf{where } \sigma = mgu(\rho(M), \rho(N)) \\
[\![\mathsf{lock};Q]\!]\rho H \ell \phi \mathsf{false} &= [\![Q]\!](\rho \cup \{vs_1 \mapsto vs_1,\ldots,vs_n \mapsto vs_n\})H\ell\phi_0\mathsf{true} \\
& \qquad \textbf{where } \phi_0 = (vs_1,\ldots,vs_n), \textbf{ with } vs_1,\ldots,vs_n \text{ fresh} \\
[\![\mathsf{unlock};Q]\!]\rho H \ell \phi \mathsf{true} &= [\![Q]\!]\rho H \ell \phi \mathsf{false} \\
[\![s_i := M;Q]\!]\rho H \ell \phi \mathsf{false} &= [\![Q]\!](\rho \cup \{vs_1 \mapsto vs_1,\ldots,vs_n \mapsto vs_n, vc \mapsto vc, vm \mapsto vm\})H\ell\phi\mathsf{false} \\
& \cup\{H \wedge \mathsf{message}(\phi_0, vc, vm) \Rightarrow \mathsf{message}(\phi_1, vc, vm)\} \\
& \cup\{H \wedge \mathsf{attacker}(\phi_0, vm) \Rightarrow \mathsf{attacker}(\phi_1, vm)\} \\
& \qquad \textbf{where } \phi_0 = (vs_1,\ldots,vs_{i-1},vs_i,vs_{i+1},\ldots,vs_n), \\
& \qquad \textbf{and } \phi_1 = (vs_1,\ldots,vs_{i-1},\rho(M),vs_{i+1},\ldots,vs_n) \\
& \qquad \textbf{with } vs_1,\ldots,vs_n,vc,vm \text{ fresh} \\
[\![s_i := M;Q]\!]\rho H \ell \phi \mathsf{true} &= [\![Q]\!](\rho \cup \{vc \mapsto vc, vm \mapsto vm\})H\ell\phi'\mathsf{true} \\
& \cup\{H \wedge \mathsf{message}(\phi, vc, vm) \Rightarrow \mathsf{message}(\phi', vc, vm)\} \\
& \cup\{H \wedge \mathsf{attacker}(\phi, vm) \Rightarrow \mathsf{attacker}(\phi', vm)\} \\
& \qquad \textbf{where } \phi = (M_1,\ldots,M_{i-1},M_i,M_{i+1},\ldots,M_n), \\
& \qquad \textbf{and } \phi' = (M_1,\ldots,M_{i-1},\rho(M),M_{i+1},\ldots,M_n), \\
& \qquad \textbf{and } vc, vm \text{ fresh} \\
[\![\mathsf{read}\ s_i \text{ as } x;Q]\!]\rho H \ell \phi \mathsf{false} &= [\![Q]\!](\rho \cup \{x \mapsto vs_i, vs_1 \mapsto vs_1,\ldots,vs_i \mapsto vs_i,\ldots,vs_n \mapsto vs_n, \\
& \qquad vc \mapsto vc, vm \mapsto vm\})(H \wedge \mathsf{message}(\phi_0, vc, vm))\ell\phi\mathsf{false}
\end{aligned}
$$







EasyChair: the little Facebook

Year	#confs
2002	2
2003	3
2004	7
2005	66
2006	276
2007	629
2008	1312
2009	2183
2010	3306
2011	>3690
2012	>161
2013	>5

EasyChair data about Mark Ryan, 2005-2011

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*.

EasyChair data about Mark Ryan, 2005-2011

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*.

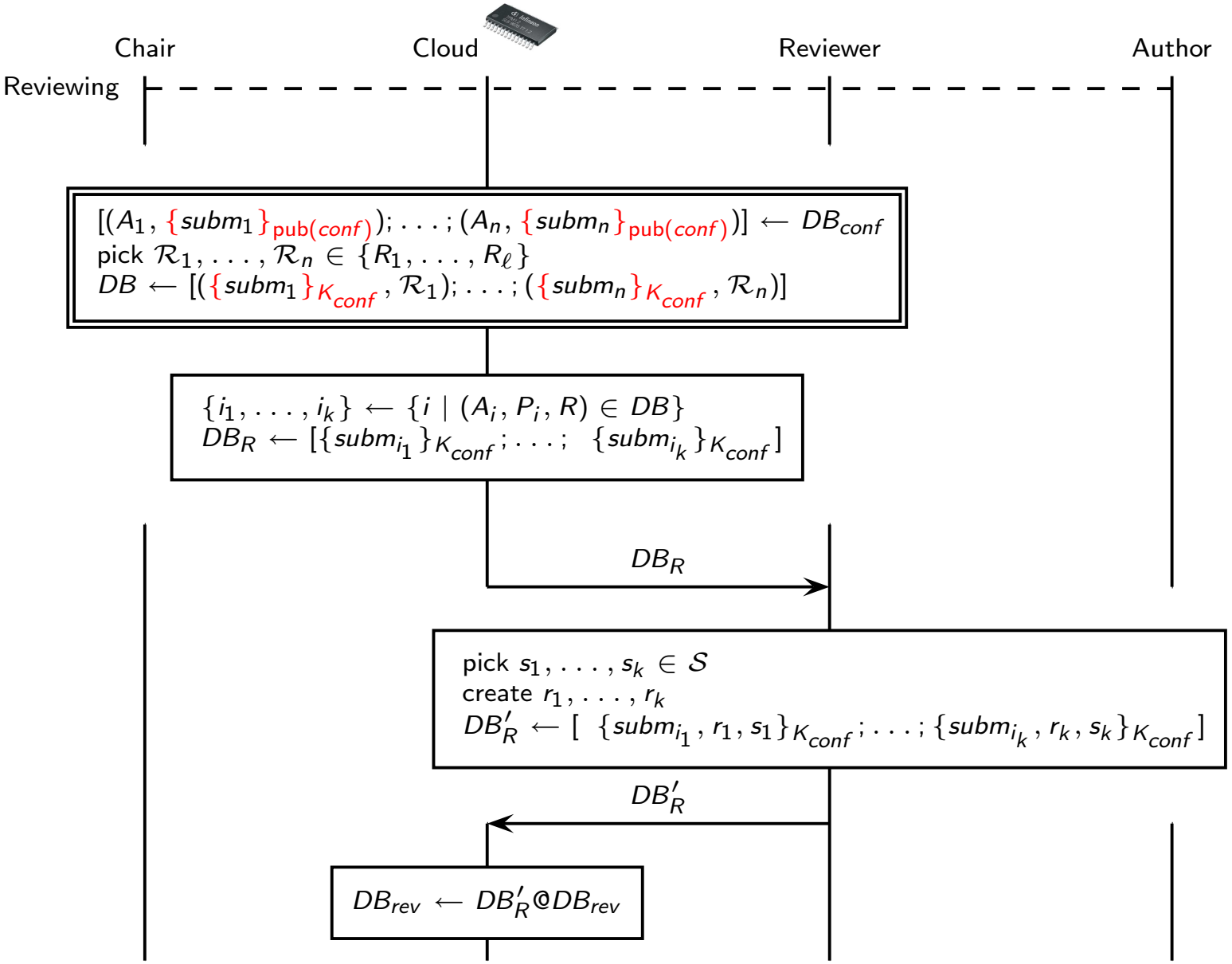
number of papers submitted	25
number of papers accepted	17
Acceptance rate	0.68
number of papers reviewed	107
number of times recommended accept	24
Recomendation agr. w. outcome	28%

EasyChair data about Mark Ryan, 2005-2011

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*.

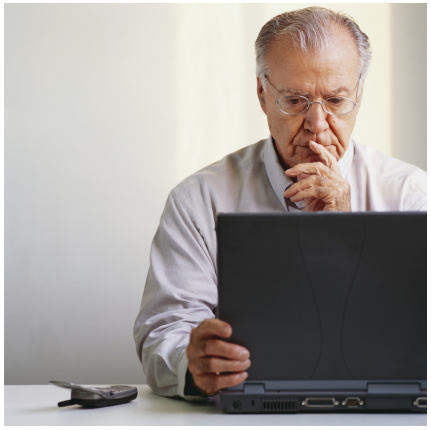
number of papers submitted	25
number of papers accepted	17
Acceptance rate	0.68
number of papers reviewed	107
number of times recommended accept	24
Recomendation agr. w. outcome	28%
Probability CSF 2012 re-invites him	0.2
Prob. will win ACM Turing award	$2^{-11.2}$


Chair
Cloud
Reviewer
Author
Reviewing
$[(A_1, \{subm_1\}_{pub(conf)}); \ldots; (A_n, \{subm_n\}_{pub(conf)})] \leftarrow DB_{conf}$
pick $\mathcal{R}_1, \ldots, \mathcal{R}_n \in \{R_1, \ldots, R_\ell\}$
$DB \leftarrow [(\{subm_1\}_{K_{conf}}, \mathcal{R}_1); \ldots; (\{subm_n\}_{K_{conf}}, \mathcal{R}_n)]$
$\{i_1, \ldots, i_k\} \leftarrow \{i \mid (A_i, P_i, R) \in DB\}$
$DB_R \leftarrow [\{subm_{i_1}\}_{K_{conf}}; \ldots; \{subm_{i_k}\}_{K_{conf}}]$
DB_R
pick $s_1, \ldots, s_k \in \mathcal{S}$
create $r_1, \ldots, r_k$
$DB'_R \leftarrow [\{subm_{i_1}, r_1, s_1\}_{K_{conf}}; \ldots; \{subm_{i_k}, r_k, s_k\}_{K_{conf}}]$
DB'_R
$DB_{rev} \leftarrow DB'_R @ DB_{rev}$

2. Electronic voting

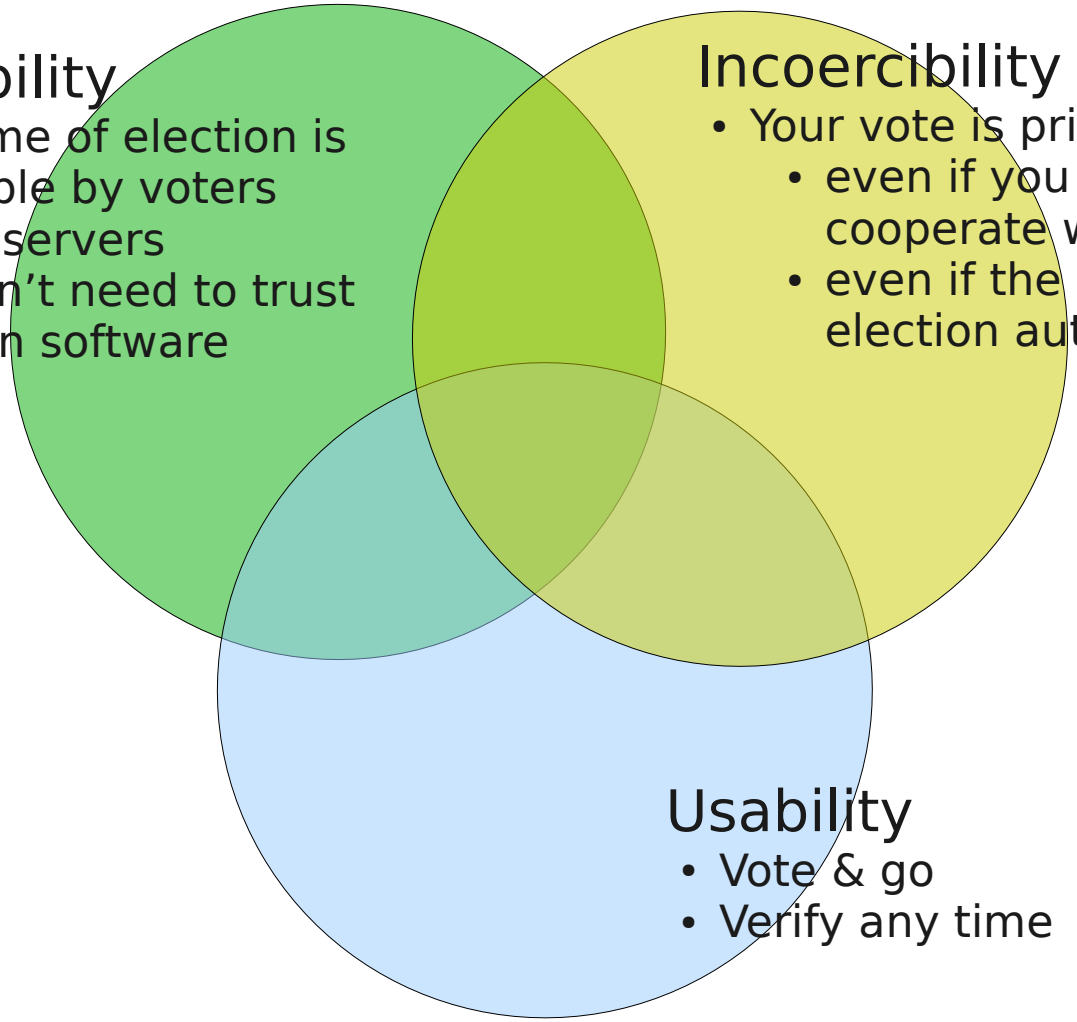
Electronic voting potentially offers

- 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.



Examples of people voting

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:
VP is coercion resistant if there exists a process V' such that for any $C = \text{new } c_1.\text{new } c_2.(\_ \mid P)$ satisfying

- $\tilde{n} \cap fn(C) = \emptyset$
- $S[C[V_A\{^?/_v\}^{c1,c2}] \mid V_B\{^a/_v\}] \approx_\ell S[V_A\{^c/_v\}^{chc} \mid V_B\{^a/_v\}]$

we have

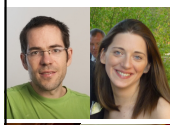
- $C[V']^{\backslash \text{out}(chc,\cdot)} \approx_\ell V_A\{^a/_v\}$,
- $S[C[V_A\{^?/_v\}^{c_1,c_2}] \mid V_B\{^a/_v\}] \approx_\ell S[C[V'] \mid V_B\{^c/_v\}]$.

Verifiability:
Soundness

$$\forall i, j. \quad \Phi^{IV}(v_i, r_i, y) \wedge \Phi^{IV}(v_j, r_j, y) \Rightarrow i = j \tag{1}$$

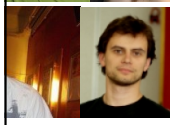
$$\Phi^{UV}(\tilde{v}, \tilde{y}, p) \wedge \Phi^{UV}(\tilde{v}', \tilde{y}, p) \Rightarrow \tilde{v} \simeq \tilde{v}' \tag{2}$$

$$\bigwedge_{1 \le i \le n} \Phi^{IV}(v_i, r_i, y_i) \wedge \Phi^{UV}(\tilde{v}', \tilde{y}, p) \Rightarrow \tilde{v} \simeq \tilde{v}' \tag{3}$$



$$\Phi^{EV}(\tilde{w}, \tilde{y}, p) \wedge \Phi^{EV}(\tilde{w}', \tilde{y}, p) \Rightarrow \tilde{w} \simeq \tilde{w}' \tag{4}$$

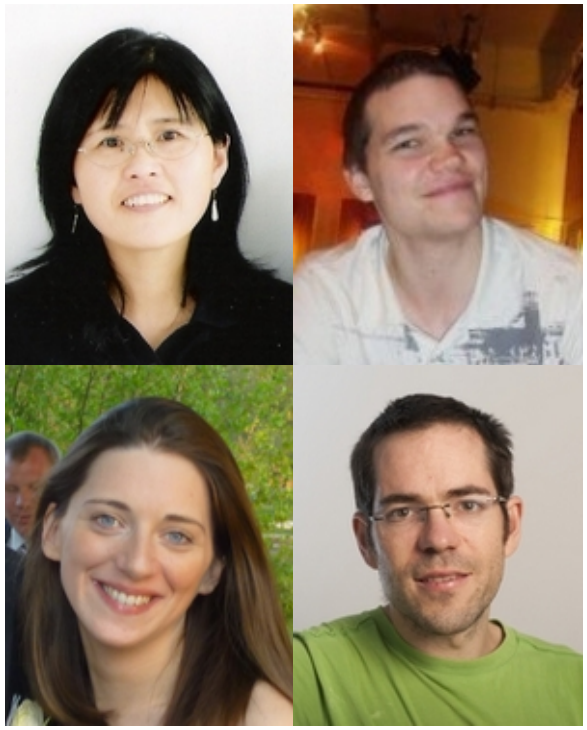
$$\bigwedge_{1 \le i \le n} \Phi^{IV}(v_i, w_i, r_i, y_i) \wedge \Phi^{EV}(\tilde{w}', \tilde{y}, p) \Rightarrow \tilde{w} \simeq \tilde{w}' \tag{5}$$

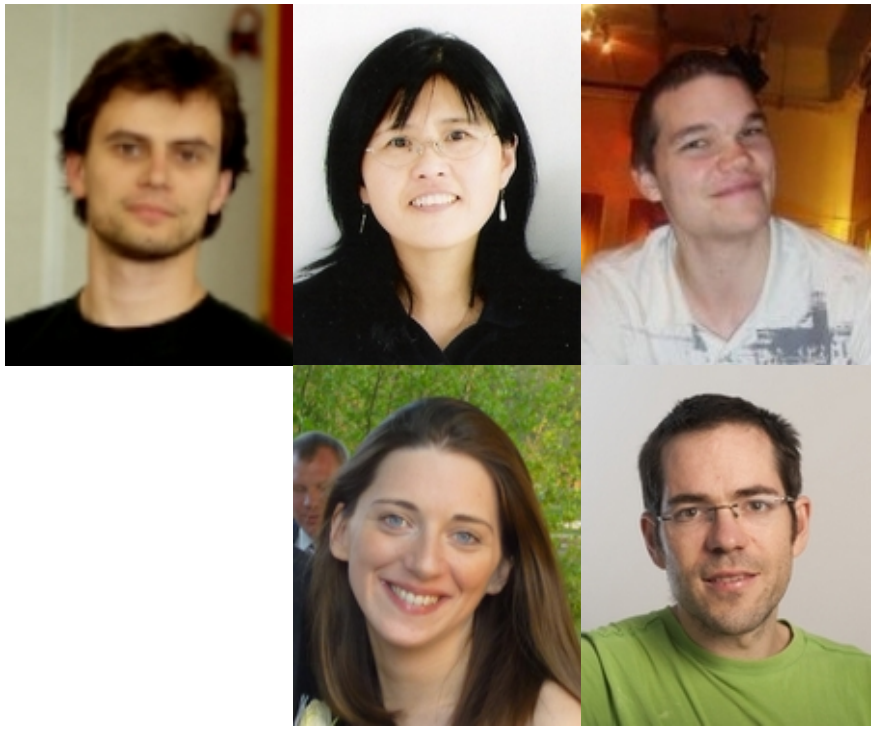


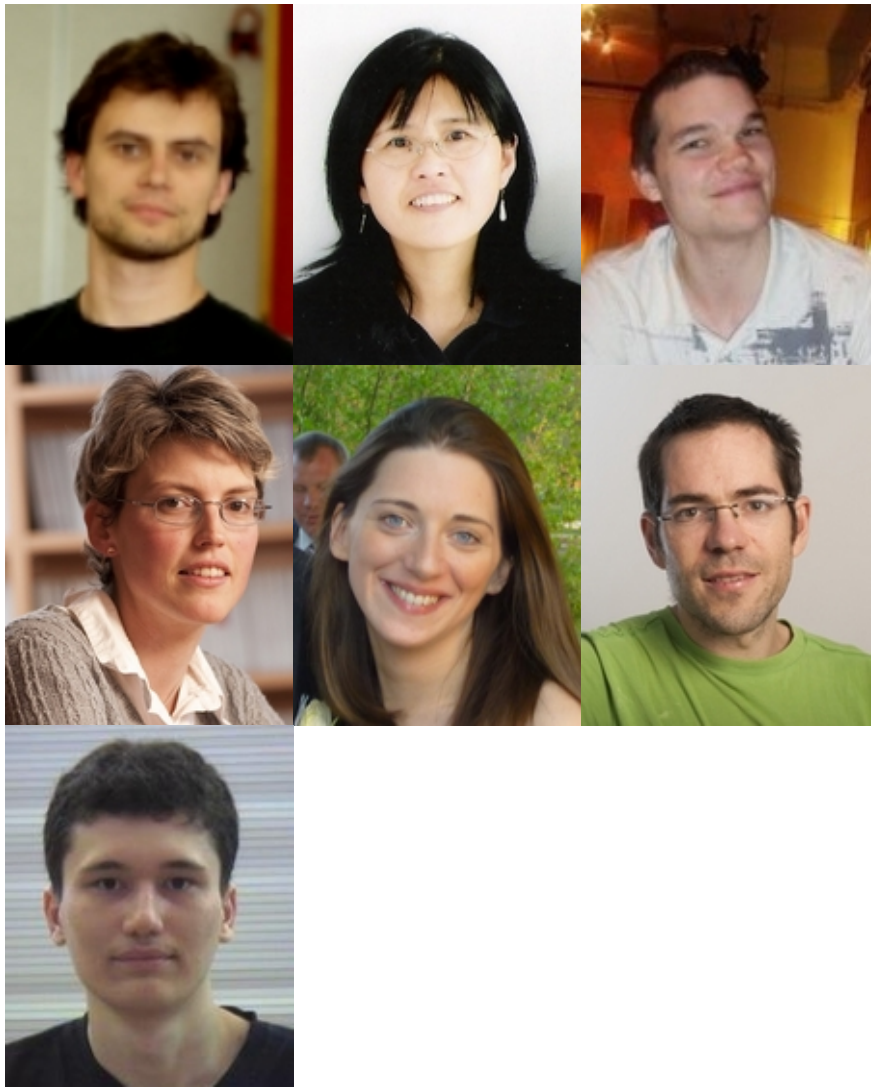
$$\Phi^{EV}(\tilde{w}, \tilde{y}, p) \wedge \Phi^{EV}(\tilde{w}, \tilde{y}', p') \Rightarrow \tilde{y} \simeq y' \tag{6}$$

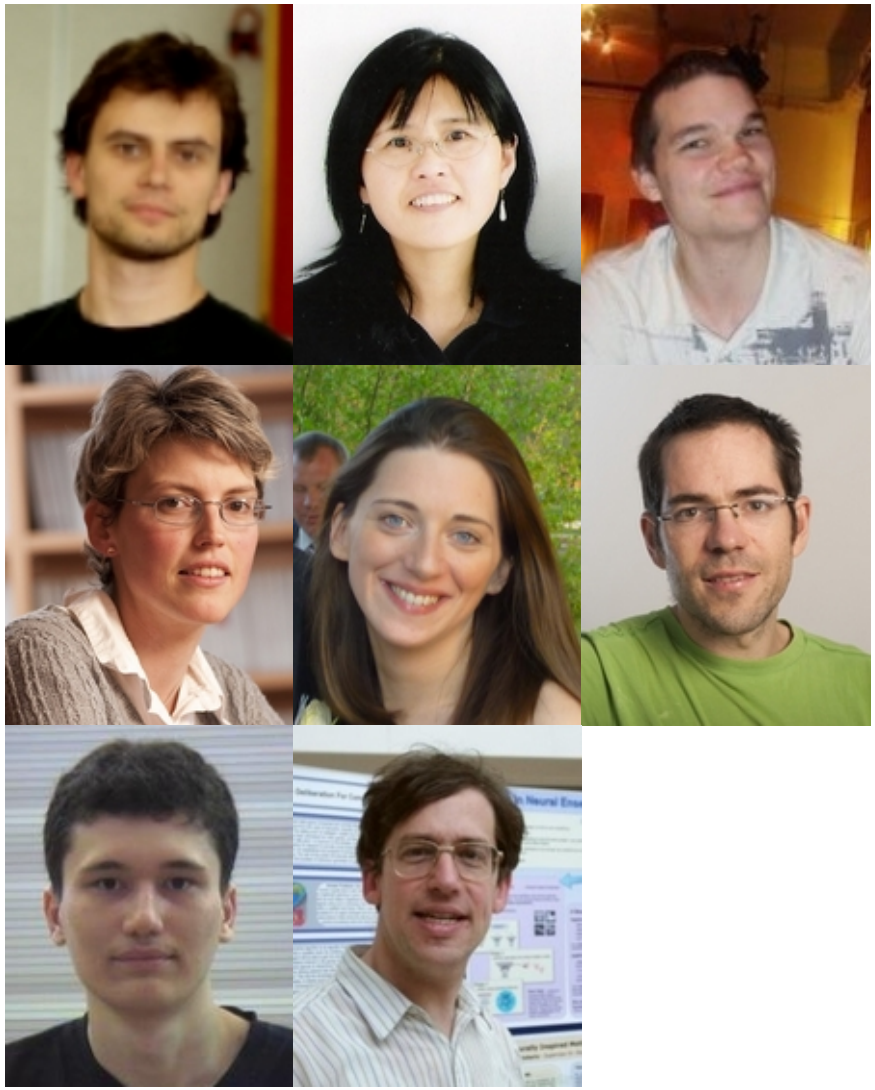
Effectiveness

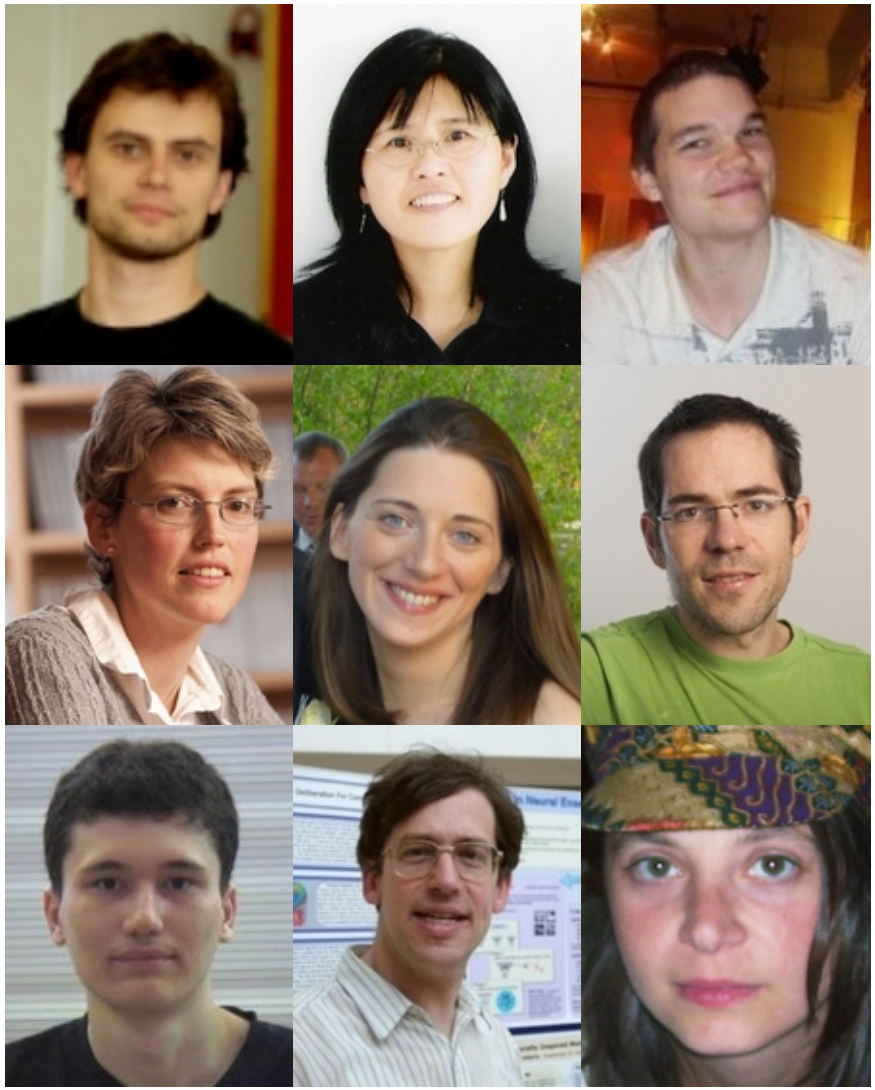
$$\bigwedge_{1 \le i \le n} \Phi^{IV}(v_i, w_i, r_i, y_i) \wedge \Phi^{UV}(\tilde{v}, \tilde{y}, p) \wedge \Phi^{EV}(\tilde{w}, \tilde{y}, p) \tag{7}$$

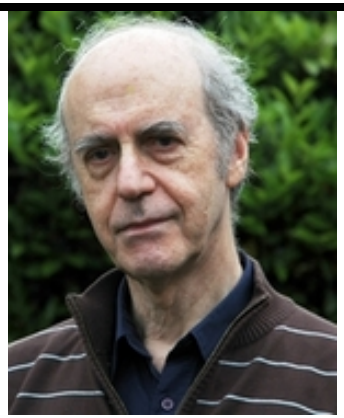


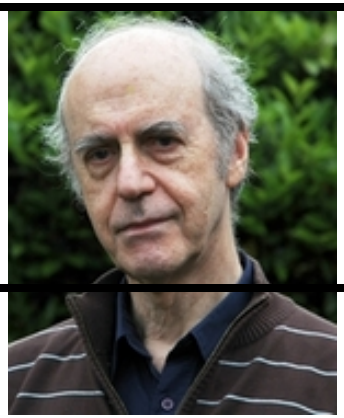


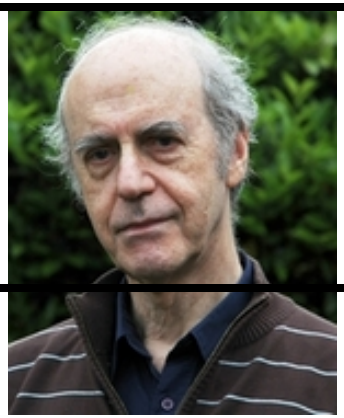


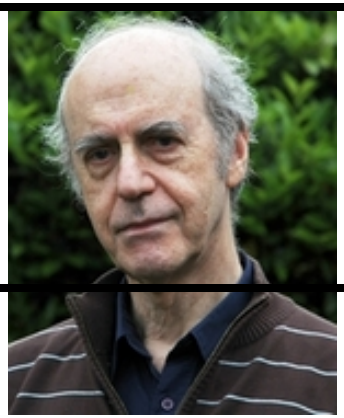




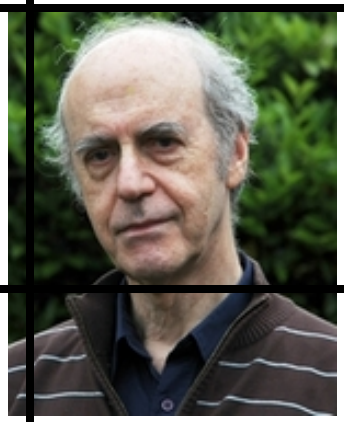


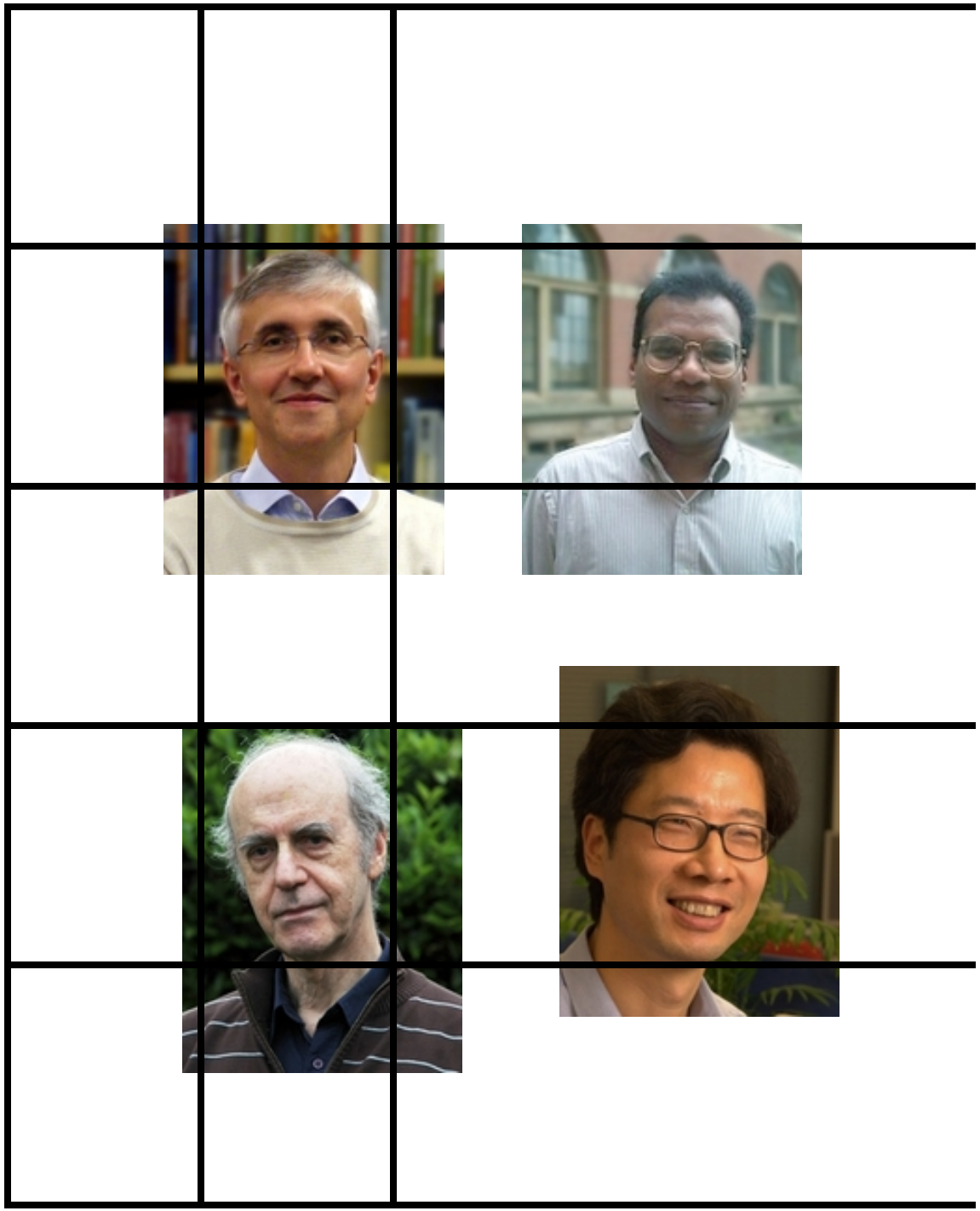


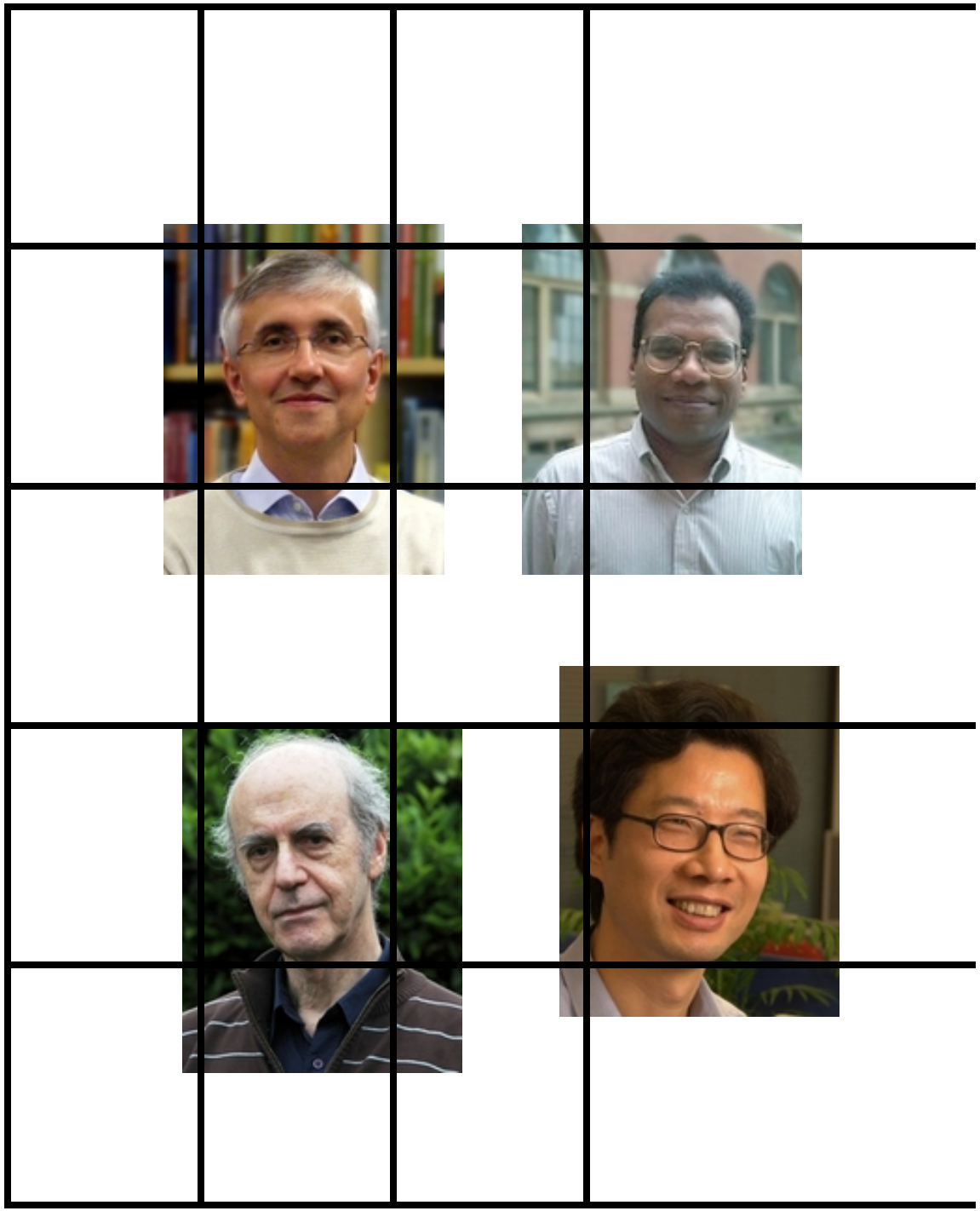


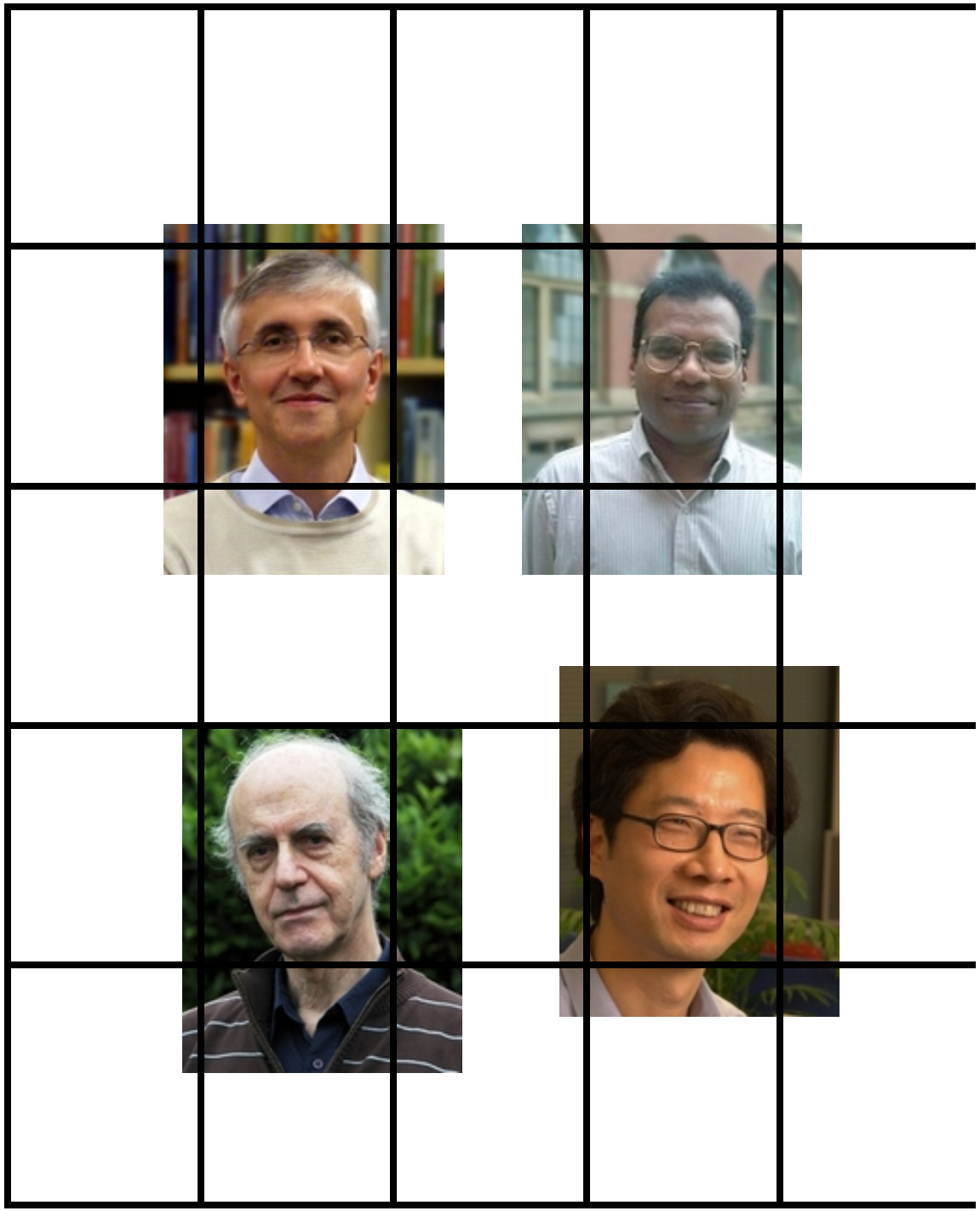


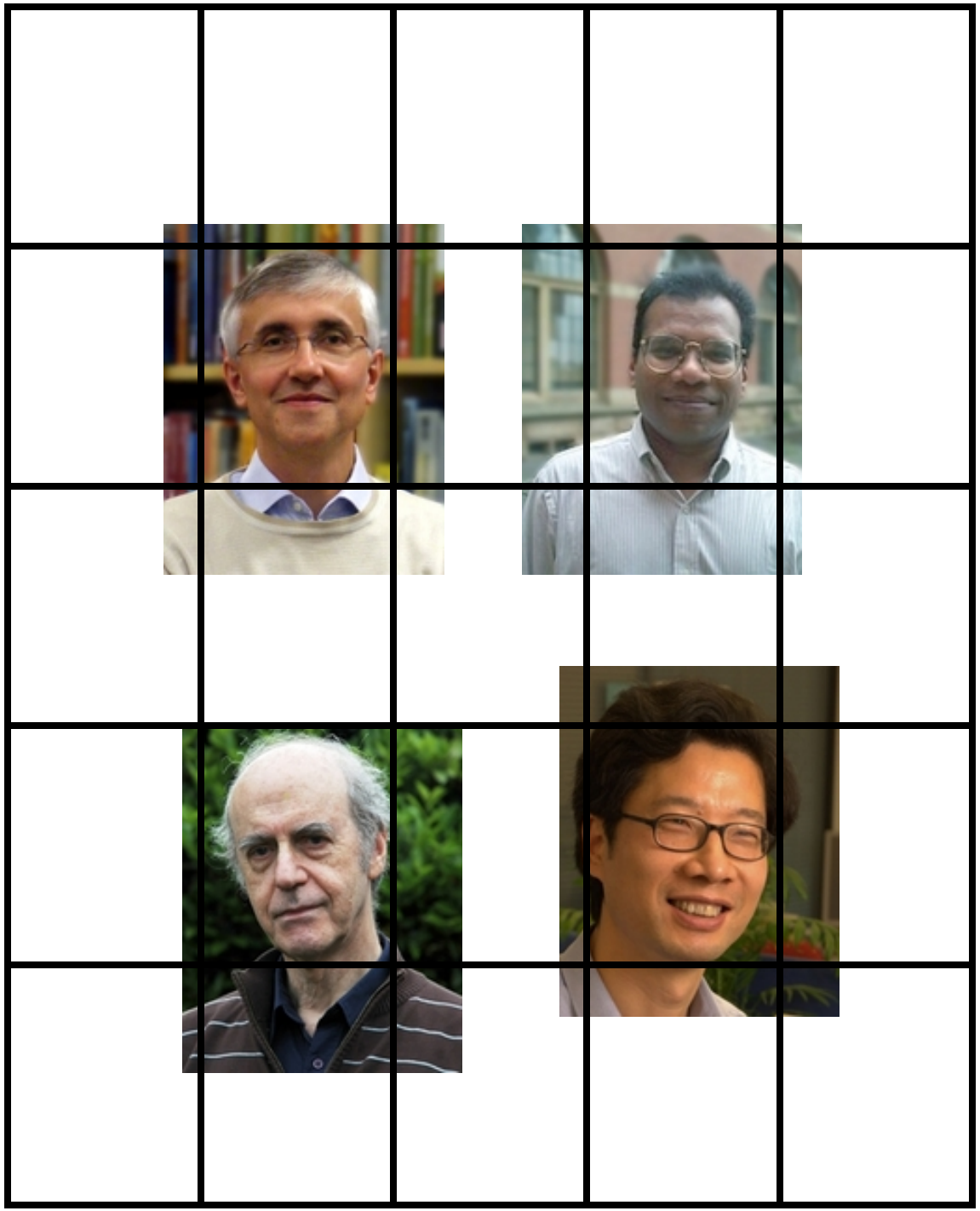










Big brother and little brother

Big brother and little brother

Big, middle and little brother (?)