PRIVACY AND SECURITY BY DESIGN

Dr Ian Brown, Senior Research Fellow
Oxford Internet Institute

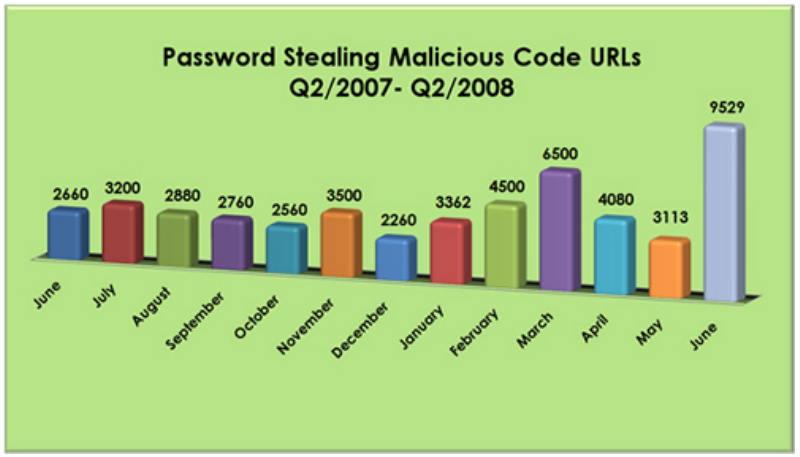

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK

HOW CAN WE…

- Design and execute strategic responses that carefully target security threats, avoiding where possible tactical arms races?
- Get the best return on security investment?
- Build citizens' trust and maintain privacy and democratic legitimacy?

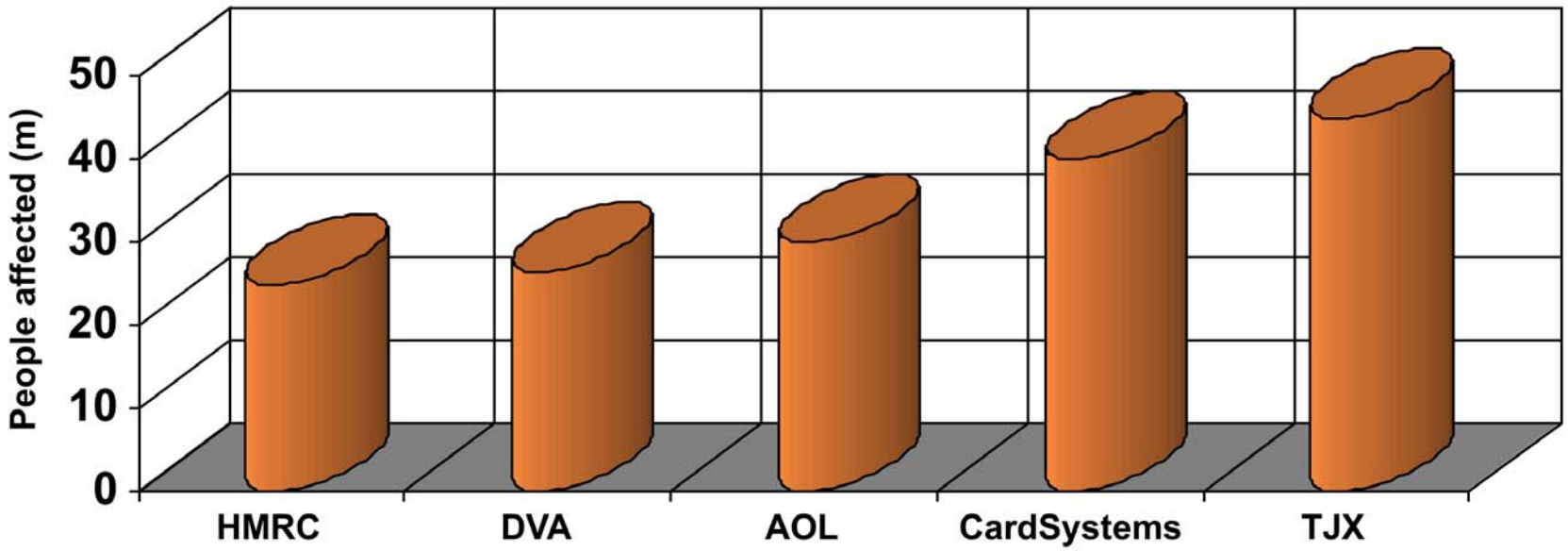
CYBER FRAUD

- Highly efficient criminal economy has sprung up (bot herders, coders, mules, phishermen)
- Phishing (Symantec observed 207,547 unique phishing messages 2H 2007) – with increased targeting
- Denial of Service extortion (Symantec observed 5,060,187 bots 2H 2007)



Anti-Phishing Working Group Q2 2008 report

TOP 5 DATA BREACHES SINCE 2000



Data: attrition.org

SCALE OF FRAUD



Internet Crime Complaint Center 2007 Annual Report p.3

Rank	Advertiser	Percentage of Advertised Goods, Top 10	Percentage of Goods and Services, Top 10	Value of Goods	Potential Worth
1	Maggie	25%	27%	$144,448	$6.4 million
2	Spooki	22%	15%	$128,459	$3.3 million
3	Luna	19%	18%	$108,798	$3.2 million
4	Shadow	14%	11%	$80,309	$1.7 million
5	Expo	9%	12%	$52,599	$2.0 million
6	Ripley	8%	6%	$10,728	$0.9 million
7	Fergie	1%	3%	$5,523	Not applicable
8	Fintan	1%	3%	$5,262	$0.4 million
9	Pepper	1%	2%	$4,040	$0.3 million
10	Pranda	<1%	4%	$2,185	Not applicable

Symantec Report on the Underground Economy 2008 p.49

OUR REAL GOALS

- Availability & integrity of Critical National Infrastructure
- Protection of personal/confidential information
- Manageable levels of fraud
- …all in cost-effective form, where costs include inconvenience, enhancement of fear, negative economic impacts & reduction of liberties

GOVERNMENTAL RESPONSES

- Protecting govt infrastructure – $294m requested by DHS for 2009; $6bn requested for NSA initiative
- Critical infrastructure programmes – e.g. CPNI, InfraGard
- Law enforcement response – e.g. PCeU; FBI has 800+ full-time agents, received 320,000 complaints in 2007
- Centres of expertise and information-exchange – e.g. ENISA, IC3, CERTs
- Updating legislation – Council of Europe Cybercrime Convention



CROSS-GOVERNMENT OPTIONS

- Fund security R&D with INFOSEC agency participation
- Use procurement, licensing and standardisation power to require significantly higher security standards in systems and services
- Use diplomacy to pressure state actors behind Russian Business Network, DDoS attacks, classified network incursions etc.

REDISTRIBUTING LIABILITY

- House of Lords concluded liability must be shifted to some combination of software vendors, ISPs and financial institutions
- Intended to incentivise innovations such as RBS off-line consumer card terminal



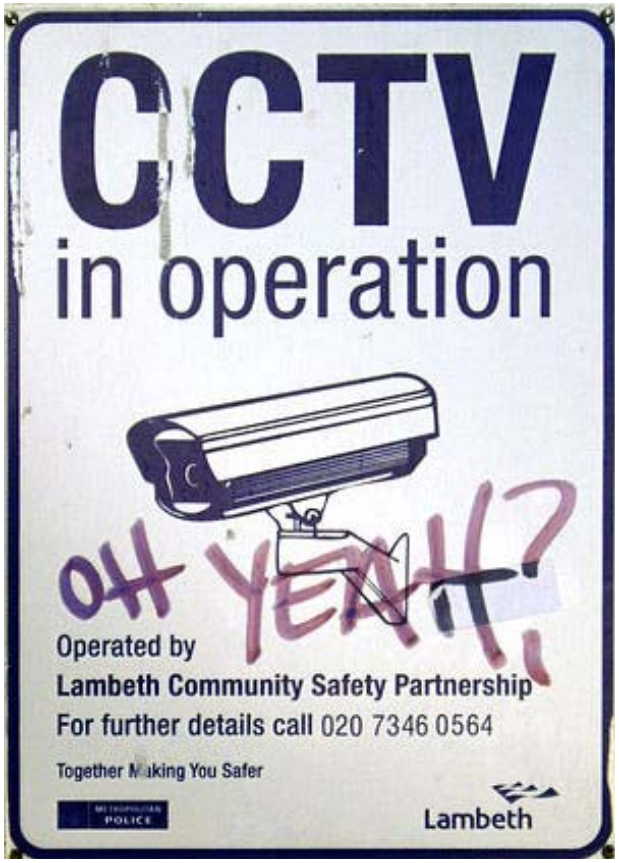
SECURITY LEGITIMACY

- Informed, democratic consent
  - Do citizens and their representatives have full information on costs & benefits?
  - Privacy Impact Assessment?
- Compatibility with human rights (*S & Marper v UK, Liberty v UK, I v Finland*)
- Continued legislative and judicial oversight and technological constraint
  - Privacy by Design



DESIGNING FOR PRIVACY

- Data **minimisation** key: is your data really necessary?
- Limit personal data collection, storage, access and usage
  - States have a positive duty to design systems to protect privacy (*I v Finland* 2008)
  - "processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity" (WP 115)
- Users must also be **notified** and **consent** to the processing of data – user interfaces?



Ade Rowbotham (2005)

CREDIBLE IMPACT ASSESSMENT

- Risk must be quantified to be meaningful, even for low-probability high-impact events
- How strong is evidence that "solution" will work?
- How widely do stakeholders agree that cost << benefit? Include direct cost, inconvenience, enhancement of fear, negative economic impacts, reduction of liberties
- "Any analysis that leaves out such considerations is profoundly faulty, even immoral"

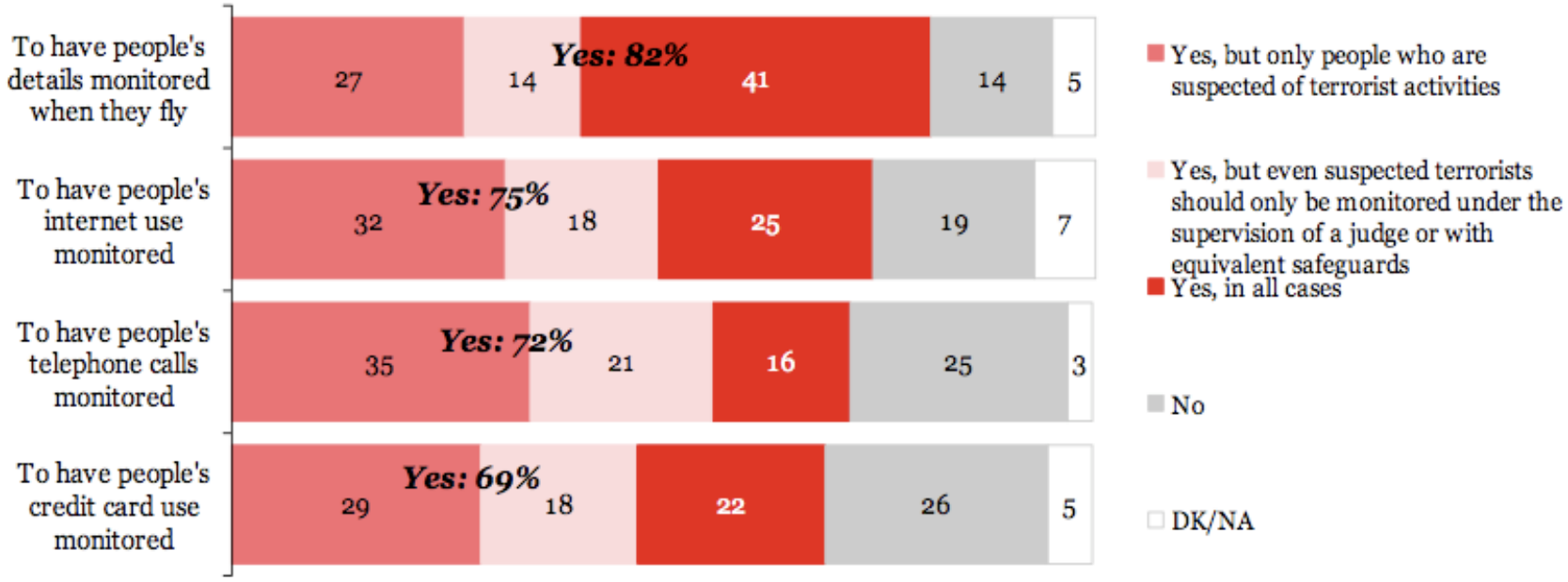
John Mueller (2008) The quixotic quest for invulnerability, *International Studies Association*, New York

STRATEGIC IMPACT

- Do systems damage societies' key values e.g. by censoring websites or undertaking warrantless wiretaps?
- "Techniques that look at people's behavior to predict terrorist intent are so far from reaching the level of accuracy that's necessary that I see them as nothing but civil liberty infringement engines." –Jeff Jonas, Chief Scientist, IBM Entity Analytics



SURVEILLANCE AND SECURITY



Source: Eurobarometer #225 Data Protection in the EU, Feb. 2008 p.48

HOW NOT TO DO IT

- "We really don't know a whole lot about the overall costs and benefits of homeland security" –senior DHS economist Gary Becker (2006)
- "Policy discussions of homeland security issues are driven not by rigorous analysis but by fear, perceptions of past mistakes, pork-barrel politics, and insistence on an invulnerability that cannot possibly be achieved." – Jeremy Shapiro (2007)
- "Finding out other people's secrets is going to involve breaking everyday moral rules." –David Omand (2009)

KEY QUESTIONS

- How can we target security interventions to maximise long-term RoI?
- How can law enforcement best work with partners across government and industry to reduce damage?
- Are we getting the right balance between reducing vulnerabilities, increasing availability, protecting privacy and monitoring/response?