
CHANGES AND CHALLENGES IN DATA TRANSFER

JOHN BORKING

**Director Borking
Consultancy**

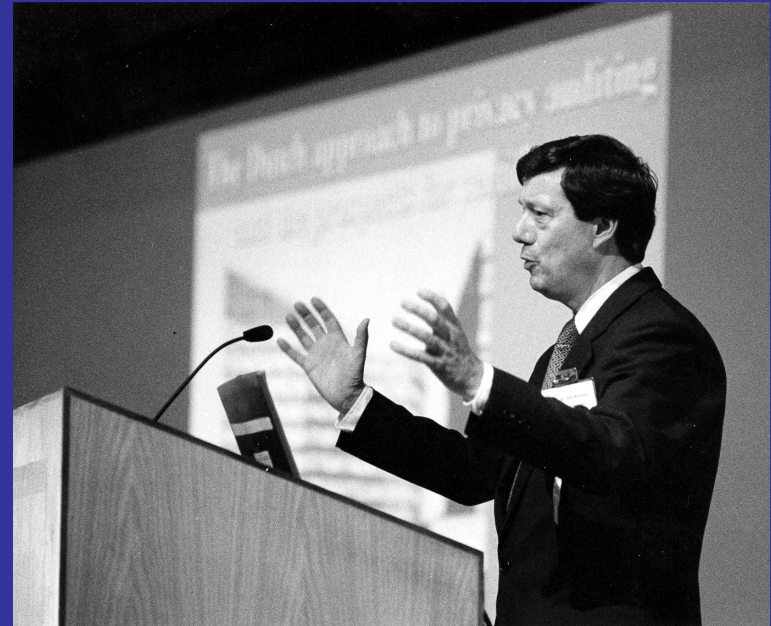
Computer Law Expert

**Dutch Data Protection
Authority (1994-2006)**

**Member Supervisory Board
Dutch Gaming & Lottery
Control**

ICT Mediator and Arbiter

**Subcontractor PRIME-
Project**



PRIME WHITE PAPER 2005

“Commercial interests, as well as improving public services, are important drivers in the collection of personal data. Increasingly, also (national) security has a stake in this field. The cliché that 9/11 has changed the world is especially true in the field of personal data. As ICT-mediated communication reveals much about people's behaviour, there is pressure from law enforcement and national security agencies to intercept this kind of communication or at least to have access to the traffic data associated with it.”

SINCE 911: THE ENEMY OF THE STATE

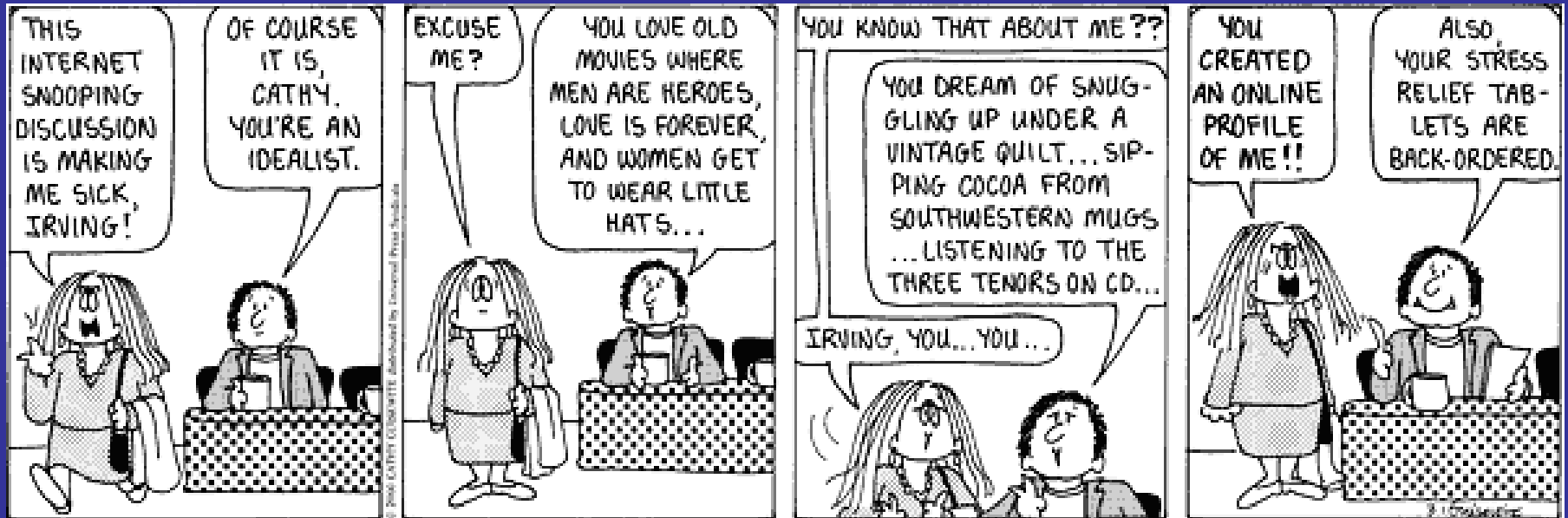
YOU & ME?

NONSENSE ?

- Air Carriers flying to, from, across U.S. territory have to provide electronic access to Passenger Name records (PNR) (EU Court of Justice C-317/04 & C-318/04)
- SWIFT transfers already for years systematically massive amounts of personal data for surveillance by U.S. government (Belgian DPA report Sept. 2006)

WHY IS CATHY (AND ARE WE) CONCERNED? Can everybody analyze data transfers?

Cathy



RAPID

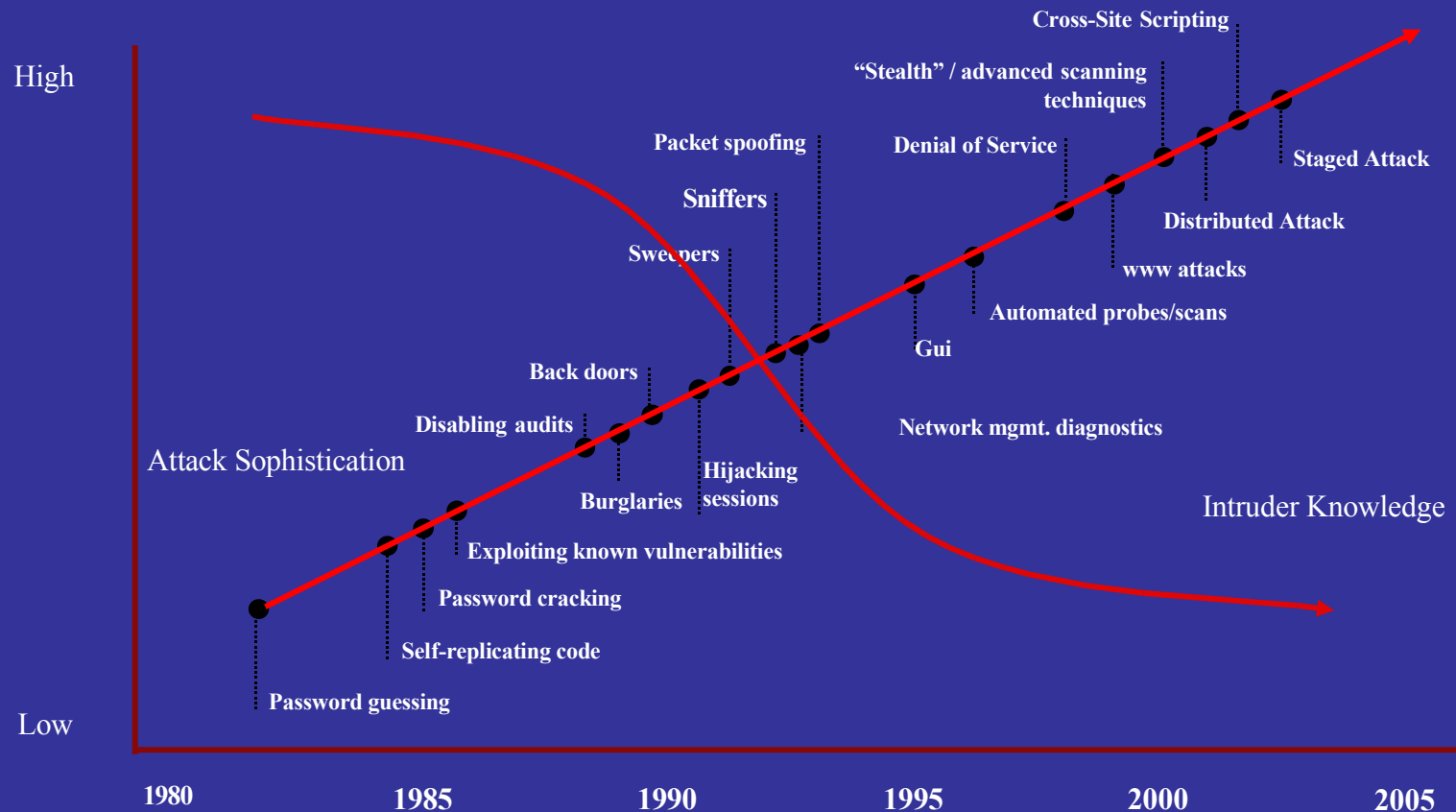
Roadmap for Advanced Research in Privacy and IDentity Management Technologies (2002)

•TRENDS

- Short-term: Multi-platform access to e-services
 - Personal data, Digital assets and Identities become “raw” material for a digital economy.
- Mid/Long: Ambient intelligence, seamless interactions with services
 - “Electronic environments that are sensitive and responsive to the presence of people”.
 - New models of privacy management

**WILL ORWELL'S PROPHECY
COME TRUE?**

Threats



1995 WHERE WE THOUGHT WE WERE GOING

- The world was on a road to peace
- Globalization was ramping up
- Corporate innovation was creating value and wealth
- We were connected by WWW
- The U.S. Lotus/Equifax case 1991 forgotten
- The EU privacy directive 95/46/EC adopted: EU wide privacy protection
- The PETs report published (No privacy enhancing tools yet)
- Dreaming about P3P
- AND TEN YEARS LATER?

2006 DID WE EXPECT THIS DEVELOPMENT ?

- BUSH DOCTRINE: US WAGING WAR ON IRAQ AND TERRORISM
- UNSAFER WORLD BECAUSE OF THE IRAQ WAR (U.S. secret services analysis)
- THE RISE OF CHINA AS ECONOMIC SUPER POWER
- ADOPTION OF THE EU DATA RETENTION DIRECTIVE 2006/24/EC

OUR REACTION

- CHANGING SECURITY AND PRIVACY ENVIRONMENT
 - Zero sum game Privacy vs. Security
 - Public accepts less privacy (I have nothing to hide)
 - Public safety vs. privacy
 - Citizens: I trust the government attitude
- ANTI-TERRORIST LEGISLATION
 - US Patriot Act, Canada's Bill Lawful Access, EU retention of traffic data, PNR-data, Council of Europe Convention on Cyber-Crime etc. etc.
- POLICIES MANDATING INDIVIDUALS' PERSONAL INFORMATION
- MORE AND MORE DATA (TRANSFERS)

(FUTURE) TRENDS

- The decline of anonymity
- Making the meaningless meaningful
- The colonization of time, space, physical borders
- The merging of previously compartmentalized data
- Technologies for involuntary & passive data collection
- Due to the blurring of public and private spaces and data, personal information much more available

BUT,
“THINGS ARE GETTING BETTER
ALL THE TIME” (the Beatles)

- Increased awareness of the issues concerning (maintaining) trust / privacy
 - Much more research into privacy protection and identity management while data capturing and data transfers
 - More technological safeguards in line with PRIME's vision
-

PRIME VISION

Individuals can act securely and safely in the information society while keeping sovereignty of their private sphere and thus creating trust

Thus:

- User informed consent and control
- Privacy negotiation
- Data minimization
- ID management
- Accountability when needed/ enforcement of enterprise promises

www.Prime-project.eu/

REQUIRED TECHNOLOGICAL SAFEGUARDS 1

- Ano-/Pseudo-nymity: general principle: I don't know you
- Hide relations between user identity & actions
- Transparency = not only a view, but also insight into processing of his/her personal data
- User empowerment: privacy protection under user's control, informed consent, opt-in/out
- Minimal data collection, transmission and storage
- System integration: built-in privacy protection and purpose binding
- Multilateral security: transitivity requires minimal trust between entities

REQUIRED TECHNOLOGICAL SAFEGUARDS 2

- Passive intrusion prevention- encryption
- Prove user authorization locally, transmit only conformation and authorization
- Communications protocols that hide device ID
- Limiting signal range
- Improved access controls/ context dependent (important in AMI)
- Unobtrusive, continuous, multimodal authentication
- Solving the problem of authorized but dishonest person
- Artificial Intelligence to catch unusual patterns warning the individual

W3C WORKSHOP

LOOKING AT THE CONTRIBUTIONS:
RESEARCH PROGRESS IS VISIBLE

- PRIVACY POLICY LANGUAGES & NEGOTIATION TOOLS
- ARCHITECTURES ENFORCING DATA HANDLING / ENTERPRISE ENFORCEMENT

BUT WHEN AND HOW EXPLOITABLE ? Fig leaf?

THANK YOU