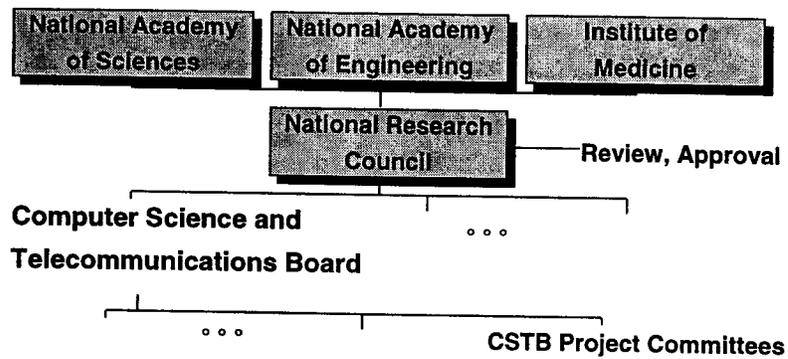# Computer Science and Telecommunications Board

of the

National Academies

www.cstb.org

David D. Clark, Chair

Marjory S. Blumenthal, Executive Director

© 2002

The National Academies

National Academy of Sciences	National Academy of Engineering	Institute of Medicine

National Research Council — Review, Approval

Computer Science and Telecommunications Board

o o o

o o o

CSTB Project Committees

2

CSTB • Computer Science and Telecommunications Board

The People of CSTB (Staff)

- Marjory Blumenthal, Exec Director
- Herb Lin, Senior Scientist
- Alan Inouye, Sr Program Officer
- Jon Eisenberg, Sr Program Offcr
- Jerry Sheehan, Sr Program Officer
- Lynette Millett, Program Officer
- Cynthia Patterson, Program Offcr
- Steven Woo, Program Officer
- Eric Basques, Program Officer
- David Padgham, Research Associate

- Janet Briscoe, Administrative Officer
- Margaret Huynh, Sr Project Assistant
- D.C. Drake, Sr Project Assistant
- Janice Sabuda, Sr Project Assistant
- Jennifer Bishop, Sr Project Assistant
- Brandye Williams, Office Assistant

3

CSTB • Computer Science and Telecommunications Board

The CSTB Board

DAVID D. CLARK, Massachusetts Institute of Technology, *Chair*

DAVID BORTH, Motorola Labs

JAMES CHIDDIX, AOL Time Warner

JOHN M. CIOFFI, Stanford University

ELAINE COHEN, University of Utah

W. BRUCE CROFT, University of Massachusetts at Amherst

THOMAS E. DARCIE, AT&T Labs Research

JOSEPH FARRELL, University of California at Berkeley

JEFFREY M. JAFFE, Bell Laboratories, Lucent Technologies

ANNA KARLIN, University of Washington

BUTLER W. LAMPSON, Microsoft Corporation

EDWARD D. LAZOWSKA, University of Washington

DAVID LIDDLE, U.S. Venture Partners

TOM M. MITCHELL, Carnegie Mellon University

DONALD NORMAN, Nielsen Norman Group

DAVID A. PATTERSON, University of California at Berkeley

HENRY (HANK) PERRITT, Chicago-Kent College of Law

BURTON SMITH, Cray, Inc.

TERRY SMITH, University of California at Santa Barbara

LEE SPROULL, New York University

JEANNETTE M. WING, Carnegie Mellon University

4

CSTB • Computer Science and Telecommunications Board

Introducing CSTB

We exist to give unbiased advice to the government and country on critical issues concerning IT and society.

We pioneered Internet tech/policy analysis—and have long addressed system security/trustworthiness.

We have depth and breadth of insight, impact--we know our stuff...and we know how to find and use the real experts.

We excel at objective treatment of complex, controversial topics that mix technical and nontechnical aspects.

5

CSTB • Computer Science and Telecommunications Board

How We Operate

- **Balanced Group(s) of National Experts**
  - The Board Plus its Committees for Projects
  - Cross-Sector, Cross-Discipline
  - Professional Staff Complement

- **Engage the Best Minds**
  - Senior/authoritative
  - Serving our unique position
  - Cross-section of communities or views
  - *Not* shrinking violets

6

CSTB • Computer Science and Telecommunications Board

What We Provide

- Influential Reports--We Write the Books . . .
  - Analytical — recommendations from objective analysis
  - Unbiased — the National Academies process
    - balances bias, eliminates COI; heavy vetting
  - Enduring Usefulness (reference value)
- Independent, Authoritative Analysis
  - Technology Whats, Hows, Whys, Whens
  - Interactions of Technology, Econ/Soc/Psych, Law, Policy +
  - Consensus and Awareness
- Special Meetings

7

CSTB · Computer Science and Telecommunications Board

CSTB's Interdisciplinarity

- CSTB Style
  - CSTB staff: multi-disciplinary backgrounds
    - Didn't hire a computer scientist until mid-2000!
  - CSTB projects: seldom narrowly technical in focus, typically broad committees
- CSTB Collaborations
  - Interactions with other NRC units over the years
  - Range of practice (staff-sharing, review, consultation)

8

CSTB · Computer Science and Telecommunications Board

CSTB Audience(s)

- Government agencies and Congress
- Industry (research and business components)
- Universities and other research institutions
- Researchers and educators
- "Public interest" groups
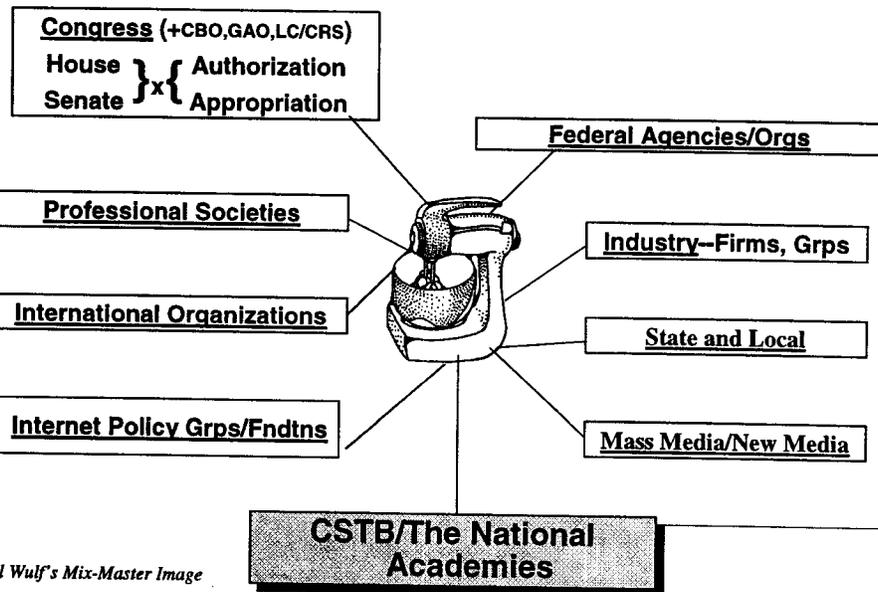
The audience goes beyond the sponsors.

Policy-makers, others value CSTB's genuine neutrality, non-advocacy.

Many CSTB Reports Become Trade Books.

9

CSTB · Computer Science and Telecommunications Board

CSTB in the Broader Policy Context

Congress (+CBO,GAO,LC/CRS)

House ⎱ ⎰ Authorization
        } x {
Senate ⎰ ⎱ Appropriation

Professional Societies

International Organizations

Internet Policy Grps/Fndtns

Federal Agencies/Orgs

Industry--Firms, Grps

State and Local

Mass Media/New Media

CSTB/The National Academies

Bill Wulf's Mix-Master Image

CSTB Funding

- Government agencies predominate
- Corporate contributions provide flexibility and broader impact
- Occasional private foundation, other
- Campaign for personal philanthropy

- National Academies Processes Assure *Independence of Results from Source of Funding*--Key to Impact!

11 **CSTB** · Computer Science and Telecommunications Board

CSTB'S Oeuvre

- 70 reports of different kinds, scales since 1987
- Different ways to categorize
    - 20+ on R&D and tech trends
    - 12+ on trustworthiness (security, privacy)
    - 20+ on economic and social impacts of IT
    - 22+ on applications of IT (e.g., health, mfg, gov't)
    - 20+ on (tele)communications and Internet
    - 10+ on law

12 **CSTB** · Computer Science and Telecommunications Board

CSTB on Trustworthiness

- *Computers at Risk*
- *Rights and Responsibilities...*
- *[Cont'd] Review of Tax Systems Modernization...*
- *Cryptography's Role in Securing the Info Society*
- *For the Record: Protecting Electronic Health Info*
- *Trust in Cyberspace*
- *Realizing the Potential of C4I*
- *The Digital Dilemma: Intel Prop in the Info Age*
- *Embedded, Everywhere*
- *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*
- *IDs—Not That Easy*
- *Youth, Pornography, and the Internet*

13

CSTB · Computer Science and Telecommunications Board

CSTB on Internet & Telecom

- *Toward a National Research Network*
- *Realizing the Information Future*
- *Changing Nature of Telecom/Information Infra*
- *...Convergence of Computing, Comms, and Entertainment*
- *The Unpredictable Certainty*
- *Cryptography's Role in Securing the Info Society*
- *The Evolution of Untethered Communications*
- *Networking Health*
- *The Internet's Coming of Age*
- *Looking Over the Fence at Networks*
- *Broadband: Bringing Home the Bits*

14

CSTB · Computer Science and Telecommunications Board

CSTB on R&D/Tech Trends

- *The National Challenge...*
- *Toward a Nat'l Research Network*
- *National Collaboratories*
- *Academic Careers ....Experimental CSE*
- *Realizing the Info Future*
- *Evolving the HPCCI to Suppt the Nation's Info Infra*
- *Computing and Comms in the Extreme*
- *More Than Screen Deep*

- *Modeling & Simulation: ...Defense & Entertainment*
- *Evolution of Untethered Comms*
- *Funding a Revolution*
- *Networking Health*
- *Making IT Better*
- *The Internet's Coming of Age*
- *Looking Over the Fence at Netwks*
- *Embedded, Everywhere*
- *Information Technology Research, Innovation, and E-Government*

15

CSTB · Computer Science and Telecommunications Board

CSTB on Soc/Econ Impacts

- *Information Technology in the Service Society*
- *Keeping...Convergence of Comp, Comm, & Entrtnmnt*
- *Research Recs to Facilitate Distributed Work*
- *Rights & Responsibilities*
- *Realizing the Info Future*
- *The Unpredictable Certainty*
- *For the Record*
- *Fostering Research on Econ & Social Impacts of IT*

- *Being Fluent with IT*
- *The Digital Dilemma*
- *Networking Health*
- *LC 21: A Digital Strategy for the Library of Congress*
- *Building a Workforce for the Information Economy*
- *Global Networks and Local Values*
- *Youth, Pornography, & the Internet*
- *Information Technology Research, Innovation, and E-Government*

16

CSTB · Computer Science and Telecommunications Board

Current Activities (Excl Dissem)

Trust-related:

S&T for Countering Terr'm—IT

The Internet Under Crisis Conditns

Information Fusion (exploration)

Internet Navigation and the DNS

Authentication Techs and Their
Implications for Privacy

Critical Information Infrastructure
Protection and the Law

Privacy in the Information Age

Improving Cybersecurity Research

Other:

Digital Archiving and NARA

Fundamentals of Comp Science

Frontiers at the Interface of
Computing and Biology

IT and Creativity

GIS and Information Tech

17

CSTB • Computer Science and Telecommunications Board

A Sampler of Prospective Activities

* Dependable Systems/Certification

* Cybersecurity
Practices/Benchmarks

* Planning for the Infospace

* Cyber-Attack/ Insider Threat

Whither High(est) Perf Computing?

Fluency with Info Technology—K-12

Telecommunications Research

Wireless Trends & Spectrum Mgt

Computer Graphics

Issues in Software Development/Open
Source: Technology, Economics, ...

Research Horizons: Operating
Systems

Software and Business Process Patents

Semantic Web

Digital Democracy

IT and Competition Policy

Extending Law into Cyberspace

Internet and Economic Development

Digital Driving (Vehicular Telematics)

Access and Equity: Info Tech for All?

Living with Information
Technology/Manageable Systems

IT in an Aging Society/IT and Access
for Differently Abled

Nonprofit Perspectives and Opportu-
nities in IT

Women in CS

Robotics

CSTB • Computer Science and Telecommunications Board

A Peek at Recent/Current CSTB Work Relating to Security and Privacy

19 **CSTB** • Computer Science and Telecommunications Board

Cybersecurity Today and Tomorrow: Pay Now or Pay Later

- Compiles understanding, knowledge, findings, and recommendations from > a decade of CSTB rpts:
- What's the new news now?
  - Information technology has changed dramatically in the last decade: Internet, e-commerce, PCs everywhere
  - What was news 10 years ago in cybersecurity is STILL relevant today!
  - Speaks to a very sorry state of progress in the field.

20 **CSTB** • Computer Science and Telecommunications Board

Cybersecurity: What's known?

- General Observations
  - Information system vulnerabilities are growing faster than our ability (and willingness) to respond
- Management
- Operational Considerations
- Design and Architectural Considerations
- What can be done
  - Individual organizations
  - Vendors
  - Public policy makers

21

CSTB · Computer Science and Telecommunications Board

Thoughts on Liability

- *Cybersecurity*...report did NOT endorse liability for software vendors.
  - "Policy makers should consider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge. Possible options include steps that would increase the exposure of software and system vendors and system operators to liability for system breaches and mandated reporting of security breaches that could threaten critical societal functions."
- *Computers at Risk* began to explore topic.

22

CSTB · Computer Science and Telecommunications Board

IDs—Not That Easy: Questions about Nationwide Identity Systems

- Ongoing study on authentication technologies and their privacy implications (finish late 2002)
- Renewed national interest in 'national identification card' in wake of September 11, 2001
- Committee well-positioned to comment
- Aim of the report to deepen and broaden the discussion by raising questions

23

CSTB • Computer Science and Telecommunications Board

IDs/Auth Study Committee

Stephen T. Kent, *Chair*
BBN Technologies

Michael Angelo
Compaq Computer Corporation

Steven M. Bellovin
AT&T Labs Research

Bob Blakley
IBM

Drew Dean
SRI International

Barbara Fox
Microsoft Corporation

Stephen H. Holden
University of Maryland, Baltimore County

Deirdre Mulligan
University of California, Berkeley

Judith S. Olson
University of Michigan

Joe Pato
Hewlett Packard Labs

Radia Perlman
Sun Microsystems

Priscilla Regan
George Mason University

Jeffrey Schiller
Massachusetts Institute of Technology

Soumitra Sengupta
Columbia University

James Wayman
San Jose State University

Daniel J. Weitzner
W3C/Massachusetts Institute of Technology

Lynette I. Millett, *Study Director (CSTB)*
Jennifer M. Bishop, *Sr. Project Assistant (CSTB)*

24

CSTB • Computer Science and Telecommunications Board

Background

- ID systems have been proposed as solutions to: counterterrorism, "deadbeat parents," fraud detection, electoral reform, . . .

- ID systems have been opposed for reasons from privacy concerns to human rights considerations to traditional antipathy

- Committee believes that serious and sustained deliberation is needed before nationwide identity systems are designed, developed, or deployed

IDs: It's Not That Easy

25

CSTB • Computer Science and Telecommunications Board

Overview of the Report

- Nationwide identity system debate has been hampered by the lack of a clear description of the goals of such a system.

- Many complicated policy and technological issues around such systems

- Ascertaining desirability and feasibility involves answering these numerous complex questions

- The report aims to catalyze a broad discussion

26

CSTB • Computer Science and Telecommunications Board

Candidate Proposals

- AAMVA's proposal to network state driver's license systems and promote minimum standards of interoperability for driver's licenses
- DOT's trusted traveler system
- Improved Social Security cards

- In general: large-scale identity systems for which widespread use and participation is expected should be subject to the analysis of this report –
they're all *nationwide identity systems*

27

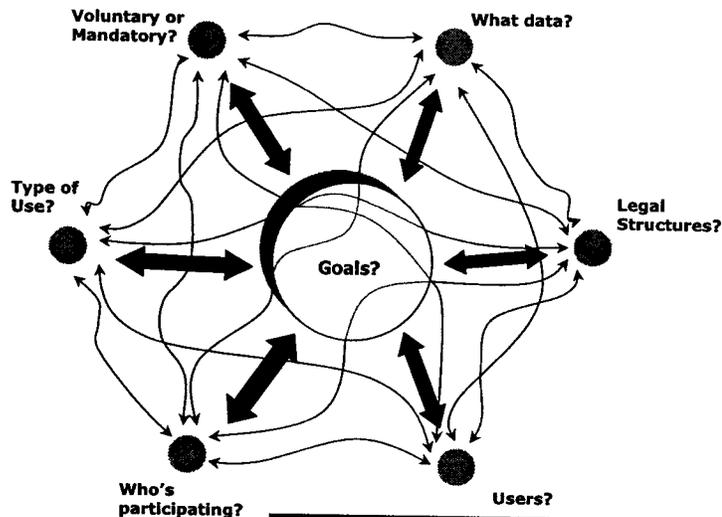**CSTB** • Computer Science and Telecommunications Board

Driving Questions

- What would be **the purpose** of the system?
  - Assumptions differ about ends
- **Who** would be issued an ID?
- **What data** would be collected?
- Who would **use** the system?
- What **types of use** would be allowed?
- Is participation **voluntary or mandatory**?
- What **legal structures** would be needed?

28

CSTB • Computer Science and Telecommunications Board

Interconnecting Policy Choices

Voluntary or Mandatory?

What data?

Type of Use?

Goals?

Legal Structures?

Who's participating?

Users?

29

CSTB · Computer Science and Telecommunications Board

What does Identity Provide

- What is identity?
- Individuals often have multiple identities
- What identity information is relevant to the purpose of the system?
- When are group identities (e.g., "older than 21") appropriate?

30

CSTB · Computer Science and Telecommunications Board

Who Gets an ID? How?

- How is identity initially established?
- What is the meaning of the ID?
- Where does the identity information reside?
- What kinds of access to and analysis of that information is allowed or disallowed?

31

CSTB · Computer Science and Telecommunications Board

Where Does the Information Go?

Format?

Machine Readable

Human Readable

Location?

Card   Database   Elsewhere
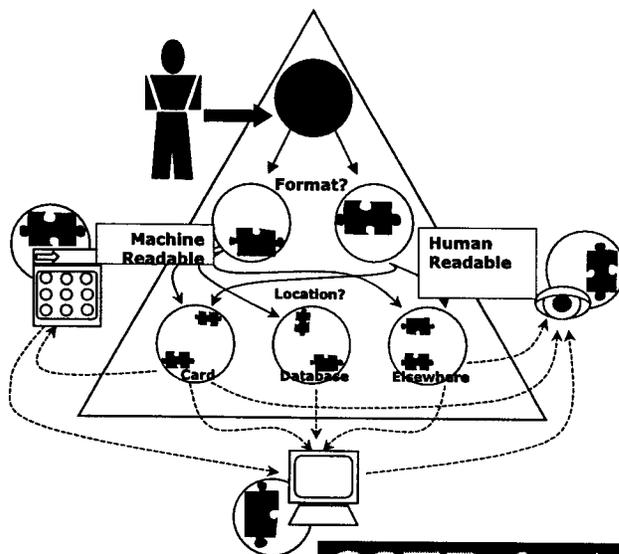
32

CSTB · Computer Science and Telecommunications Board

Who Uses the System?

- Under what circumstances may someone request an ID? Access data within the system?
- Would the private sector be allowed to use the system?
- Who will manage, oversee, and maintain the system?
- Will public-private partnerships be required?
- What are the implications of broad vs. narrow sets of users?

33

CSTB · Computer Science and Telecommunications Board

What Uses are Allowed?

- What questions can be asked of the system?
- Will data mining be allowed? By whom?
- Will real-time correlation of system transactions be needed?
- How will information be linked to other systems?
- What are the privacy implications of allowing broad queries and/or linkages?

34

CSTB · Computer Science and Telecommunications Board

Voluntary or Mandatory? Avoiding "Function Creep"

- Is participation in the system required?
- If voluntary, would the inconveniences that result from non-participation mean that participation is effectively mandatory?
- Is consent required when requesting an ID?

- **How can function creep in a large-scale identity system be avoided?**

35 CSTB · Computer Science and Telecommunications Board

Legal Structures?

- How would use of the system be regulated?
- What are the Constitutional implications?
- How does U.S. privacy law and policy apply?
- What are the federal/state/local considerations?

36 CSTB · Computer Science and Telecommunications Board

Benefits and Drawbacks

- Current identity systems have many flaws
- A large-scale nationwide identity system might drive other forms of ID out of use (function creep?)
- Many potential unintended side effects
- Identity theft – consequences could become even more dire

37

CSTB · Computer Science and Telecommunications Board

Technological Challenges

- The *ID* is part of a much larger *system*
- Security, access control – hard to build truly robust large-scale systems
- Architectural considerations
- Cost analysis
- What tradeoffs need to be made?

38

CSTB · Computer Science and Telecommunications Board

Binding Persons to Identities

- How to relate IDs to individuals?
- Two- (or N-)factor authentication
- Biometrics and cryptographic protections
- What are appropriate thresholds for false positives and false negatives?
- How should errors and exceptions be handled?

39

CSTB · Computer Science and Telecommunications Board

Back-end Systems

- Access to database
- What are the tracking, surveillance, and prediction requirements?
- Is high availability necessary?
- What backups and redundancy would be needed?
- Differing levels of access and query capabilities for different users?
- Procedurally, how would maintenance and administration work?

40

CSTB · Computer Science and Telecommunications Board

Data Correlation and Privacy

- Would consolidation of other databases be necessary?
- Centralization creates a single target for adversaries
- Denial of service risks
- Potential privacy invasions possible if correlative capabilities allowed

41   **CSTB** · Computer Science and Telecommunications Board

The Systems Effect

- Linking together of many social, legal, and technological components . . .
- . . . in complex and interdependent ways
- Success or failure depends on interaction of components
- Controlling interdependencies and mitigating security vulnerabilities important to overall effectiveness

42   **CSTB** · Computer Science and Telecommunications Board

IDs Concluding Remarks

- More analysis is needed with respect to the concept of a nationwide identity system
- Clear articulation of the goals and requirements is essential
- Prior public review is vital
- Given the broad range of potential uses, it is likely that no single system would suffice
- Significant, sustained, sophisticated discussion amongst and between all interested parties and stakeholders is crucial

43

CSTB · Computer Science and Telecommunications Board

Privacy in the Information Age

- New project (6/4-5/02 launch)
- Foundation supported (WKKF, Sloan, ATT, Carnegie)
- Broad charge: assess threats, opps, balances
- Interdisciplinary committee
- Policy-oriented
- Call for inputs: www.cstb-privacy.org
  - White papers, field trip ideas, people ideas, …

44

CSTB · Computer Science and Telecommunications Board

Privacy in the Info Age Committee

Lloyd Cutler, *Co-chair*, Wilmer, Cutler & Pickering

William Webster, *Co-chair*, Milbank, Tweed, Hadley & McCloy

James Waldo, *Vice-chair*, Sun Microsystems

Julie Cohen, Georgetown University Law Center

Robert Crandall, Brookings Inst

Oscar Gandy, Univ of Pennsylvania

James Horning, Network Associates Labs

Gary King, Harvard University

Ellen Knapp, PriceWaterhouseCoopers (*ret.*)

Brent Lowensohn, Kaiser Foundation Hospitals

Gary Marx, Massachusetts Institute of Technology

Helen Nissenbaum, New York Univ

Robert O'Neil, Univ of Virginia

Ron Rivest, Massachusetts Institute of Technology

Teresa Schwartz, Independent Legal Consultant

45

CSTB · Computer Science and Telecommunications Board

Computer Science and Telecommunications Board

DEPS/NRC

The National Academies

www.cstb.org

CSTB · Computer Science and Telecommunications Board