... EXPERIENCE SHOULD TEACH US TO BE MOST ON OUR GUARD TO PROTECT LIBERTY WHEN THE GOVERNMENT'S PURPOSES ARE BENEFICENT. MEN BORN TO FREEDOM ARE NATURALLY ALERT TO REPEL INVASIONS OF THEIR LIBERTY BY EVIL-MINDED RULERS. THE GREATEST DANGERS TO LIBERTY LURK IN INSIDIOUS ENCROACHMENT BY MEN OF ZEAL, WELL-MEANING BUT WITHOUT UNDERSTANDING.

--JUSTICE LOUIS BRANDEIS IN HIS DISSENT IN OLMSTEAD v. UNITED STATES, 1928.

Most Significant Policy Decisions
in First 30 [redacted] Years
of the MGDPA

1. Adoption of the "Fair Information Practices" principles.

2. Treating all government data, no matter how it is physically recorded and maintained, the same.

3. Establishing the statutory presumption that all government data are public.

4. Adoption of the responsible authority concept.

5. Establishing litigation as the Act's enforcement mechanism (the private attorney general concept.)

6. Making all types of government entities (except non-urban townships) subject to the Act.

**7. Establishing that the legislature will be the only authority within the state that decides what data are not public.

8. Establishing the data classification system to categorize and describe the various types of government data.

9. Integrating a "fair information practices" type act and a "freedom of information" act into one comprehensive statute.

**10. Establishing the principle that the legislature is in primary charge of decisions as to whether government agencies may share not public data.

11, Treating two different kinds of privacy/confidentiality within the Act.

   A. Non-disclosure of data to the public. (Data classifications of not public.)

   B. Limiting uses and disseminations of some types of data collected by the government. ("Tennessen Warning" and statutory limits on use and dissemination.)

12. Providing that inspection of public government data is at no charge.

13. Giving the Commissioner of Administration authority to issue advisory opinions that have legal effects.

**Major drivers for the physical size and complexity of the MGDPA.

Development of the MGDPA
Historical Overview

1972-73: Department of Administration Assistant Commissioner Dan Magraw, technologist and civil libertarian, looks for legislative authors for data privacy legislation.

1973: Magraw finds Representative John Lindstrom of Willmar who is looking for ideas for data privacy legislation. They draft a bill based on the "Swedish Data Act". Rep. Lindstrom introduces H.F. 1316 which is passed by the House with some opposition from the media and from law enforcement.

1973: The Intergovernmental Information Services Advisory Council creates a Data Privacy Committee composed of government personnel and citizens to discuss data privacy legislation. With support of Rep. Lindstrom, H.F. 1316 becomes the focus of the Committee effort and significant amendments are drafted for consideration in the 1974 Legislative session.

1974: Senator Robert Tennessen of Minneapolis introduces legislation based on the "Fair Information Practices Principles" proposed in a federal Advisory Committee study published in August, 1973. Senator Tennessen amends H.F. 1316 with language adding fair information practice principles and other refinements. Representative Lindstrom accepts Senate amendments and H.F. 1316 is enacted into law as Chapter 479 of the 1974 Session Laws. Emphasis is on regulating personal data about individuals. As part of the Act, Commissioner of Administration is given significant duties including data collection and reporting. (Legislative authors and Department of Administration personnel informally agree that this is a very complex area of public policy and that they will continue to work closely to monitor how things are working.)

1974-75: New "Data Privacy Law", as it informally is referred to, begins, among other things, to restrict public access to various types of government data especially law enforcement data. Media begins strongly urging legislature to update very antiquated Minnesota law on public access to public records. (Media lobbying on this point continues until adoption of presumption of public access to government data in 1979 session.) Department of Administration presents report to 1975 session which includes a number of recommended legislative changes. A number of changes are made to Act in 1975 session. Those changes include the definitions which form the basis for the data classification system. A legislative Privacy Study Commission is created. No language is adopted to deal with public access to government data.

1976 :	Legislative discussion of the method to use in deciding how government data ought to be classified. (This discussion continues until 1979 and during that period there is much behind the scenes negotiating involving legislature, the media, a number of governmental associations and the representatives of the Department of Administration.) Legislature gives Commissioner of Administration authority to grant "emergency classifications of data". Commissioner's authority and emergency classifications to end 6/30/77. Legislature classifies civil and criminal investigative data as not public with an expiration data for the classification of 6/30/77.
1977:	All emergency classifications extended to 7/31/78, and investigative data provision expiration data extended to 7/31/78. Commissioner of Administration ordered to act on all classifications with 30 days of enactment. Other clarifying changes made to Act.
1978:	Only changes made to the Act extended expiration dates for emergency classifications and the investigative data provision to July 31, 1979.
1979:	Definition of government data added. Public access section, including presumption of public access, added with a an effective date of 1/1/80. Emergency classifications renamed "Temporary Classifications". Commissioner of Administration given permanent authority to issue temporary classifications with fixed expiration dates. Action to compel compliance added to remedies section. Investigative data expiration date extended to July 31, 1980.
1980:	Definitions for classifications of data not on individuals added to Act. Additional specific classifications added. Expiration date for investigative data provision extended to July 31, 1981.
1981:	More sections classifying specific types of data added. Other specific information policy issues addressed. Law enforcement and civil investigative data sections added to Act.
1982-Present:	Many more sections classifying specific types of data added. Other specific information policy issues addressed with some emphasis on addressing specific issues of sharing not public data
1990:	Provisions of Data Practices Act and Open Meeting Law harmonized.
1993:	**Authority for Commissioner of Administration to issue advisory opinions was added to the Act.**

Beginning in 1977, the legislature has enacted various other statutes dealing with issues of information policy, privacy and data practices. Among those statutes are the medical records statute, the private sector employee access to personnel records statute, the insurance fair information practices statute, the Internet privacy statute, the "do not call" statute and the video privacy statute.

In addition to various studies done by the Department of Administration, the Legislative Privacy Study Commission, House Research, the Government Information Access Council and the Information Policy Advisory Task Force all conducted studies of the Data Practices Act and made legislative recommendations, some of which been adopted.

LEGAL PRIVACY

THREE GENERAL TYPES

- CONSTITUTIONAL
- TORT
- INFORMATIONAL/TECHNOLOGICAL

CONSTITUTIONAL PRIVACY

- ONLY RELEVANT WHEN GOVERNMENT IS AN ACTOR
- FEDERAL IS SUBDIVIDED INTO:
  - FOURTH AMENDMENT PROTECTIONS AGAINST ILLEGAL "SEARCHES AND SEIZURES"
  - FAMILY MATTERS
    - "NEW" LAW
    - PROTECTION AGAINST GOVERNMENT INTRUSION INTO PERSONAL DECISIONS
      - CONTRACEPTION
      - ABORTION
- STATE CONSTITUTIONS WITH EXPRESS PRIVACY PROTECTIONS

PRIVACY IN TORT

** TORTS ARE THE NASTY THINGS WE DO TO ONE ANOTHER THAT ARE NOT CRIMINAL

** TORT OF INVASION OF PRIVACY IS SUBDIVIDED INTO 4 TYPES

-- INTRUSION INTO SECLUSION

-- APPROPRIATION OF NAME OR LIKENESS

-- PUBLICATION OF PRIVATE FACTS

-- FALSE LIGHT

*** AS OF JULY 30, 1998, MINNESOTA COURTS RECOGNIZED THE FIRST THREE TYPES AS LEGAL CAUSES OF ACTION IN MINNESOTA

INFORMATIONAL/TECHNOLOGICAL PRIVACY

- REACTION TO "DARK SIDE" OF INFORMATION/HIGH TECH SOCIETY
- FAIR INFORMATION PRACTICES ACTS
- ELECTRONIC SURVEILLANCE ACTS
- LIE DETECTOR STATUTES
- FREEDOM OF INFORMATION ACTS
- INDIVIDUAL ACCESS ACTS
- VERY NEW LAW

AT THE SAME TIME, THERE IS A GROWING CONCERN THAT AUTOMATED PERSONAL DATA SYSTEMS PRESENT A SERIOUS POTENTIAL FOR HARMFUL CONSEQUENCES, INCLUDING INFRINGEMENT OF BASIC LIBERTIES. THIS HAS LED TO THE BELIEF THAT SPECIAL SAFEGUARDS SHOULD BE DEVELOPED TO PROTECT AGAINST POTENTIALLY HARMFUL CONSEQUENCES FOR PRIVACY AND DUE PROCESS. (Emphasis added.)

-- From Elliot Richardson's 1972 charge to the Secretary's Advisory Committee on Automated Personal Data Systems.

FAIR INFORMATION PRACTICE PRINCIPLES*

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for individuals to find out what information about them is in a record and how it is used.

3. There must be a way for individuals to prevent information about them that was obtained for one purpose from being used or made available for other purposes without their consent.

4. There must be a way for individuals to correct or amend a record of identifiable information about them.

5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

*Taken from: Records, Computers and the Rights of Citizens; A Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, July 1973.

SOME SURVEILLANCE TECHNOLOGIES

COMPUTERS

ELECTRONIC SURVEILLANCE DEVICES

VIDEO CAMERAS

SATELLITE TRACKING

LIE DETECTORS

ENERGY UTILIZATION MONITORS

ELECTRONIC MONITORING

GLOBAL POSITIONING DEVICES

VOICE RESPONSE SYSTEMS

CELL PHONE MONITORS

CALLER I.D.

MAGNETIC STRIP CARDS

IMPLANTED SMART CHIPS

SMART CARDS

PHOTO COP

INTERACTIVE I.D. BADGES

DATA WAREHOUSES

INTELLIGENT HIGHWAY SYSTEMS

TARGETED DIRECT MAIL

RELATIONAL DATA BASES

1-800 AND 1-900 NUMBER DATA COLLECTION SYSTEMS

"COOKIES"

COMPUTERIZED TRANSACTION MONITORING

NATIONAL HEALTH CARE PATIENT IDENTIFIER

CYBERTRACKERS

ELECTRONIC KEY ACCESS SYSTEMS

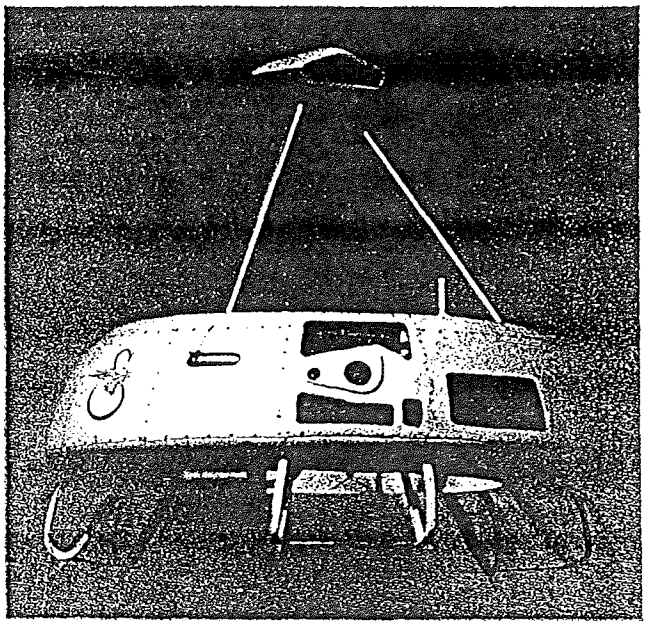
MINIATURIZED RECONNAISSANCE FLYING VEHICLES

IMBEDDED SOFTWARE SURVEILLANCE CODE

HUMAN GENOME MAPPING

? ?

"CYBER-PEEPER"



PRODUCT news

Saucer Snoop

Recently, the residents of West Palm Beach, Fla., encountered a flying saucer. But this was no alien ship. It was Cypher - a small, rotary-wing, unmanned flying vehicle designed for conducting surveillance and monitoring operations.

Cypher can fly through streets, hover and peek into windows, land on building roofs and transport small payloads.

Cypher uses a global positioning system to navigate and operates with a centralized computer (vehicle mission processor), navigational computation and air vehicle communications. The entire mission can be planned, executed and monitored from a single display system.

Commands are relayed to Cypher via a digital telemetry uplink. Aircraft status, mission data, test data and payload video are merged into a single data downlink signal that is transmitted to a mobile control van.

Cypher cruises at about 90 mph, climbs to 8,000 feet and navigates for about three hours.

For additional information, contact Sikorsky Aircraft Corp., 6900 Main Street, Stratford, #CT 06497. Call William Tuttle at 203/386-3829. E-mail: <btuttle@sikorsky.com>.

NEW TECHNOLOGIES THAT AFFECT PRIVACY

AN EXAMPLE: "SMART CARDS"

WHAT IS A "SMART CARD"?

WHAT PRIVACY ISSUES DOES IT PRESENT?

- OPERATION OF THE CARD ITSELF.
  - * WHO CONTROLS ACCESS TO THE CARD?
  - * WHO CONTROLS WHAT GOES ON THE CARD?
  - * HOW DOES THE CARD CARRIER KNOW WHAT IS ON THE CARD?
  - * WILL A NEUTRAL CARD READING SERVICE BE OFFERED?
  - * WILL "SERVICES" COME INTO BUSINESS TO ALTER CARDS? (BOOTLEG CARDS)
  - * "ZAP" POSSIBILITIES. HOW ABOUT REMOTE ZAPPING?
  - * REQUIRED USAGE. NATIONAL I.D. CARD. NATIONAL MEDICAL CARD. POST OFFICE PROPOSAL.
- TRACKING OF CARD USAGE BOTH TRANSACTIONAL AND LOCATIONAL.
  - * WHERE, WHAT, WHEN AND HOW CAN IT BE TRACKED?
- GENERAL ISSUE OF ACCESS TO DATA ON THE CARD AND SECURITY OF THE CARD AND THE DATA.
  - * BY THE CARD CARRIER. HOW DO I KNOW WHAT "IT" IS SAYING ABOUT ME?
  - * BY THOSE TO WHOM I PRESENT IT. MULTI-USE.
  - * SMART CARD USAGE THROUGH NETWORKS.

PRIVACY ISSUES RAISED BY NEW TECHNOLOGIES

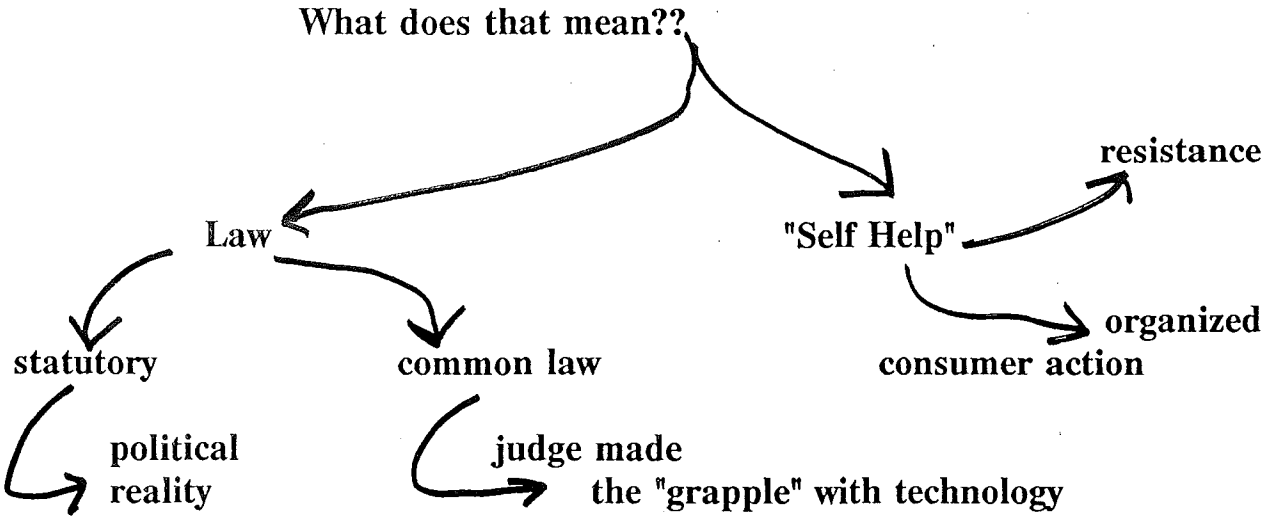
This concept we call PRIVACY. What is it?

View that technology adversely affects privacy.

-- **Use one of the new technologies as an example.**

If technology has an adverse affect, what are we (society, individuals and so forth) going to do about it?

If the normal answer is: Protect Privacy.



BIG BROTHER
IS WATCHING
YOU

BIG BROTHER
IS WATCHING
YOU

Portion of a dialogue between the "**Boss**", Willie Stark, and Jack Burden, his political "investigator".

The Boss said, "Well Jackie, it looks like you got a job cut out for you.

And I said, "I don't reckon you will find anything on Irwin." (A judge and a political opponent of the "Boss".)

And he said, "You find it."

... and I said, "But suppose there isn't anything to find?"

And the boss said, "There is always something."

And I said, "Maybe not on the Judge."

And he said, "Man is conceived in sin and born in corruption and he passeth from the stink of the didie to the stench of the shroud. There is always something."

All the King's Men

Robert Penn Warren

Quis custodiet ipsos custodes?

(Who will guard the guards themselves?)
--Juvenal