Privacy Act of 1974:
A Basic Overview

1

ASAP Conference: Arlington, VA
Monday, July 27, 2015, 9:30-10:45am

Presented by:
Jonathan Cantor, Deputy CPO, Dep't of Homeland Security (DHS)
Alex Tang, Attorney, Off. of Gen'l Counsel, Fed. Trade Comm'n (FTC)

Disclaimer: The views expressed by the presenters are their own.

Purpose of the Act

2

To regulate the collection, maintenance, use, and dissemination of personal information held by the Executive Branch of Government

- In effect since Sep 27, 1975. That's 40 years!
- Public Law 93-579
- Codified as 5 U.S.C. 552a

Congress' goals

3

- To curb the illegal Government surveillance and surreptitious investigation of individuals during the Watergate scandal and the civil rights movement
- To anticipate potential abuses presented by the Government's increasing use of computers to store and retrieve personal data by means of a universal identifier

Basic policy objectives

4

- To **restrict disclosure** of personally identifiable records maintained by Executive branch agencies
- To grant individuals increased **rights of access** to agency records maintained on themselves
- To grant individuals the **right to seek amendment** of agency records that are not accurate, relevant, timely, or complete
- To establish a **code of "fair information practices"** governing the collection, use, maintenance and disclosure of personally identifiable information

Definitions

5

- Why are definitions important?
  - The Privacy Act is a technical statute and the definitions can bring an agency in or out of the reach of the statute.
- Who has to comply with the Privacy Act?
- Who can use the Privacy Act?
- What does the Privacy Act apply to?

Who has to comply?

6

- **"Agency"**
  - Adopts the FOIA definition, see 5 U.S.C. 552(f)
  - Federal Executive Branch agencies (departments, military, Gov't corporations, other Executive Branch establishments, Postal Service, independent agencies, etc., but not Congress, GAO, Federal courts)
  - Section 7 applies to state and local agencies
    - Unlawful for any Federal, state, or local agency to deny a right, benefit or privilege because an individual refuses to provide a SSN
    - Any Federal, state or local agency requesting an SSN must inform: if disclosure is mandatory or voluntary; by what statute or authority; and the uses
  - When an agency transfers its Privacy Act records to Nat'l Archives & Records Admin. (NARA)—552a(*l*)
    - Temporarily transferred for storage—agency remains responsible
    - Permanently accessioned—NARA is responsible

Government contractors

7

- Subsection (m) makes provisions of the Act binding on contractors who operate a system of records to accomplish an agency function
- For the purposes of criminal penalties, subsection (m) contractors are considered agency employees

Who can use the Privacy Act?

8

- **An "individual"**
  - United States citizen or an alien lawfully admitted for permanent residence
  - Deceased individuals are not covered
    - Next of kin have no Privacy Act rights in the deceased's records, but FOIA may be used to protect their privacy interest in those records
  - Legal guardians
    - Parents (and legal guardians of any individual declared incompetent due to physical or mental incapacity or age by a court of competent jurisdiction) may act on behalf of the individual, see 552a(h)
  - Corporations and organizations not covered
    - Uncertain whether Privacy Act applies to records about sole proprietors, but FOIA may protect them from disclosure

What does the Privacy Act apply to?

9

- **"Systems of records"**
  - **Record:** any item, collection, or grouping of information that is "about" an individual, under agency "control," if it contains the name of (or any other identifying number, symbol, or other identifying particular assigned to) the individual—(a)(4)
    - Not purely personal notes
    - Not supervisory notes (memory refreshers)
  - **System of records:** any group of records from which information is **retrieved** by the name of an individual or by some other identifying particular assigned to the individual
    - Must identify the individual
    - Must be retrieved by an identifier

Retrieved vs. retrievable

10

- OMB guidelines explain that a system of records exists if:
  - There is an indexing or retrieval capability using identifying particulars built into the system, and
  - The agency does in fact retrieve records about individuals by references to some personal identifier
  - See *Henke v. Department of Commerce*, 83 F. 3d 1453 (D.C. Cir. 1996) (capability to retrieve is not sufficient)

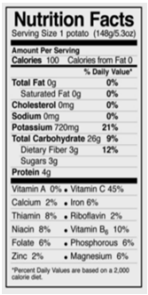
System of records notices

11

- Agency must publish a system of records notice (SORN) for each new Privacy Act records system in the *Federal Register*, after review by OMB and Congress. 5 USC 552a(e)(4)
  - Why is this important? Most of the rights and requirements of the Privacy Act depend on whether the "system" definition is met.
- Must also publish new or amended routine uses at least 30 days prior to effective date

System of records notices

12



1. System name
2. Security classification
3. System location
4. Categories of individuals covered by the system
5. Authority for maintenance of the system
6. Purpose(s)
7. Routine uses of records maintained in the system, including categories of users and the purposes of such uses
8. Disclosure to consumer reporting agencies
9. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system: storage; retrievability; safeguards; retention and disposal
10. System manager(s) and address
11. Notification procedure
12. Record access procedure
13. Contesting record procedure
14. Record source categories
15. Exemptions claimed for the system

No disclosure without consent or a legal exception

13

- General Rule--**No** disclosure unless you have:
  - written request from the subject;
  - prior written consent from the subject authorizing a 3rd party to gain access (e.g., the individual's lawyer or other representative); or
  - any of 12 exceptions established in 5 U.S.C. 552a(b)(1)-(12)

The 12 disclosure exceptions

14

(b)(1) Intra-agency disclosures – "need to know"
- Covers agency "officers and employees," but not contractors

(b)(2) Disclosure **required by** FOIA

(b)(3) Routine use published by the agency (SORN) and "compatible" with the purpose for which the records were compiled
- Permits discretionary disclosures not covered by other 11 exceptions
- Allows for "public" systems of records (e.g., agency web site staff directories, public comment or financial disclosure databases indexed by individual name))
- Enables routine disclosures to contractors and agents

(b)(4) Bureau of Census
(b)(5) For statistical research and reporting
(b)(6) NARA
(b)(7) Law enforcement
(b)(8) Compelling circumstances affecting health and safety
(b)(9) Congress
(b)(10) GAO
(b)(11) Court order
(b)(12) Debt Collection Act

Accounting of certain disclosures

15

- Each agency must maintain an accounting of disclosures from a system of records, except when disclosures are made under:
  - (b)(1) (intragency/need-to-know)
  - (b)(2) (FOIA)
- Agencies must make the accounting available to the subject, except for disclosures made under (b)(7) (law enforcement)

Notice requirements

16

- Must publish SORN (see earlier) in *Federal Register*
- (e)(3): Must provide the individual with a Privacy Act statement on the form used to collect information from the individual or on a separate form the individual can retain
  - Contents of statement: Authority, purpose, routine uses, voluntary/mandatory, consequences for failure to provide information
  - Is it required when collecting information *from someone else* (i.e., a "third party") about the individual?
  - Is it required when collecting information *orally* (e.g., in person or over the phone)?
- (e)(8): Make reasonable efforts to notify the individual when his/her records are disclosed in response to legal process (after process becomes public record)

Individual access and amendment rights

17

- Individuals may seek access to their records in a Privacy Act system or the required accounting of disclosures
  - Some records about an individual may fall outside the Privacy Act (i.e., not retrieved by that person's name or other identifier), but access to those records may be obtained via FOIA
- Individuals may also seek to amend (correct) their records
- Each agency must publish rules, in the Code of Federal Regulations (CFR), explaining how individuals may exercise these rights, including appeals process
  - Fee rules cannot include charges for search or review (cf. FOIA)
- Some systems may be legally exempted
  - Exemptions generally apply to the records system as a whole
    - Cf. FOIA, where exemptions are applied on a record-by-record basis
  - Exemptions differ in scope (the general exceptions are broader than specific ones)
  - A list of exempt systems must be published with the Privacy Act access and amendment rules in the CFR

Exemptions

18

- One information-specific exemption: (d)(5), which exempts information compiled in the reasonable anticipation of a civil action or proceeding from the **access** provisions of the Privacy Act.
  - Akin to the attorney work product privilege
  - Not limited to purely judicial proceedings, but also covers administrative hearings
  - Applies across exempt and non-exempt Privacy Act systems

Exemptions

19

- Two "general" system exemptions—(j)(1) & (2)
  - (j)(1): systems maintained by the CIA
  - (j)(2): systems maintained by a criminal law enforcement agency or component and compiled for a criminal law enforcement purpose
    - Are the records maintained by an agency or component that, as its "principal function," performs "any" activity relating to *criminal* law enforcement?
    - Are the records compiled for a criminal law enforcement purpose (e.g., identifying offenders, investigations, reports)?

Exemptions

20

- Seven "specific" system exemptions—(k)(1)-(7)
  - (k)(1): systems containing classified information
  - (k)(2): investigatory material, not within the scope of (j)(2), compiled for law enforcement purposes
    - Generally means civil law enforcement records systems
    - Under this exemption, the agency cannot deny access to any exempt system record if its maintenance resulted in the denial of any right, privilege, or benefit for which the individual is otherwise eligible, so long as confidential sources, if any, are not revealed to that individual
  - (k)(3): systems maintained in providing protective services for the U.S. President or other individuals
  - (k)(4): statutory statistical records systems
  - (k)(5): background investigation materials, but only those records reflecting confidential sources
    - Includes determinations for Federal civilian employment, military service, Federal contracts or access to classified records

Exemptions

21

- Seven "specific" system exemptions—(k)(1)-(7), cont'd
  - (k)(6): testing materials used solely to determine an individual's qualifications for appointment or promotions in the Federal service, if disclosure would compromise the objectivity or fairness of the examination process
    - Cf. FOIA Exemption (b)(2)
  - (k)(7): evaluation materials used to determine potential for promotion in the military, but only to the extent disclosure would reveal a confidential source

Other agency requirements

22

- To ensure fairness to the individual, maintain only accurate, relevant, complete, and timely information and make reasonable efforts to ensure records meet this standard before disclosing them outside the agency (does not apply to FOIA, which requires disclosure as-is)
- Collect information directly from the source
- Do not maintain records of individuals' exercise of their First Amendment rights (unless pertinent and within scope of authorized law enforcement activity)
- Establish rules of conduct and instructions (training) for persons involved in designing, developing, operating or maintaining PA systems
- Have appropriate administrative, technical and physical safeguards to ensure security and confidentiality (pre-dates FISMA)

Computer matching

23

- 1988 and 1990 Privacy Act amendments
- Applies to computer matching of Privacy Act records with non-Federal records relating to eligibility or debt collection for Federal benefits programs and computer matching of personnel and payroll systems with non-Federal records
- Requires written matching agreements (provided to Congress and made available to the public) between the source agency and Federal recipient or non-Federal agency describing purpose, legal authority, justification, individual notice, data verification, records disposition, information security procedures, etc.
- Source agency must discontinue matching if it has reason to believe the agreement is not being followed; agreements cannot be renewed without certification of compliance
- Each agency conducting or participating in matching programs must establish a Data Integrity Board to oversee and coordinate implementation

Civil Remedies—552a(g)

24

- Amendment lawsuits for injunctive relief
- Access lawsuits for injunctive relief
- Accuracy lawsuits seeking monetary damages for willful/intentional violations
- Monetary damage lawsuits for any other violation that is willful/intentional
- Agency may also be liable for attorneys fees and costs
- Civil actions are filed against the agency, not individual officers or employees, but criminal actions can be brought against individuals

Criminal Penalties—552a(i)

25

- Misdemeanor and fine not to exceed $5,000:
  - Any officer or employee who knowingly and willfully discloses identifiable information to any person who is not entitled to receive it
  - Any officer or employee who willfully maintains a "secret" system of records
  - Any person who knowingly and willingly requests or obtains Privacy Act protected records under false pretenses

Key Privacy Act resources

26

- Office of Management & Budget (OMB) has primary responsibility for Privacy Act oversight—552a(v)
  - See Office of Information and Regulatory Affairs (OIRA) within OMB, see White House web site
  - OMB Privacy Act guidelines, 40 Fed Reg. 28,948-78 (July 1975)
  - OMB Circular A-130, Appendix I
  - Other OMB Privacy Act guidance (e.g., for computer matching agreements)
- Consult your agency or component Privacy Act Officer
- Agency implementing CFR regulations (access, amendment, exempt systems)
- Agency SORNs *in Federal Register* and agency web sites, also compiled for all agencies in the Office of Federal Register's periodic *Privacy Act issuances*
- *Privacy Act Overview* (Dep't of Justice, 2012 edition)

Questions?

27