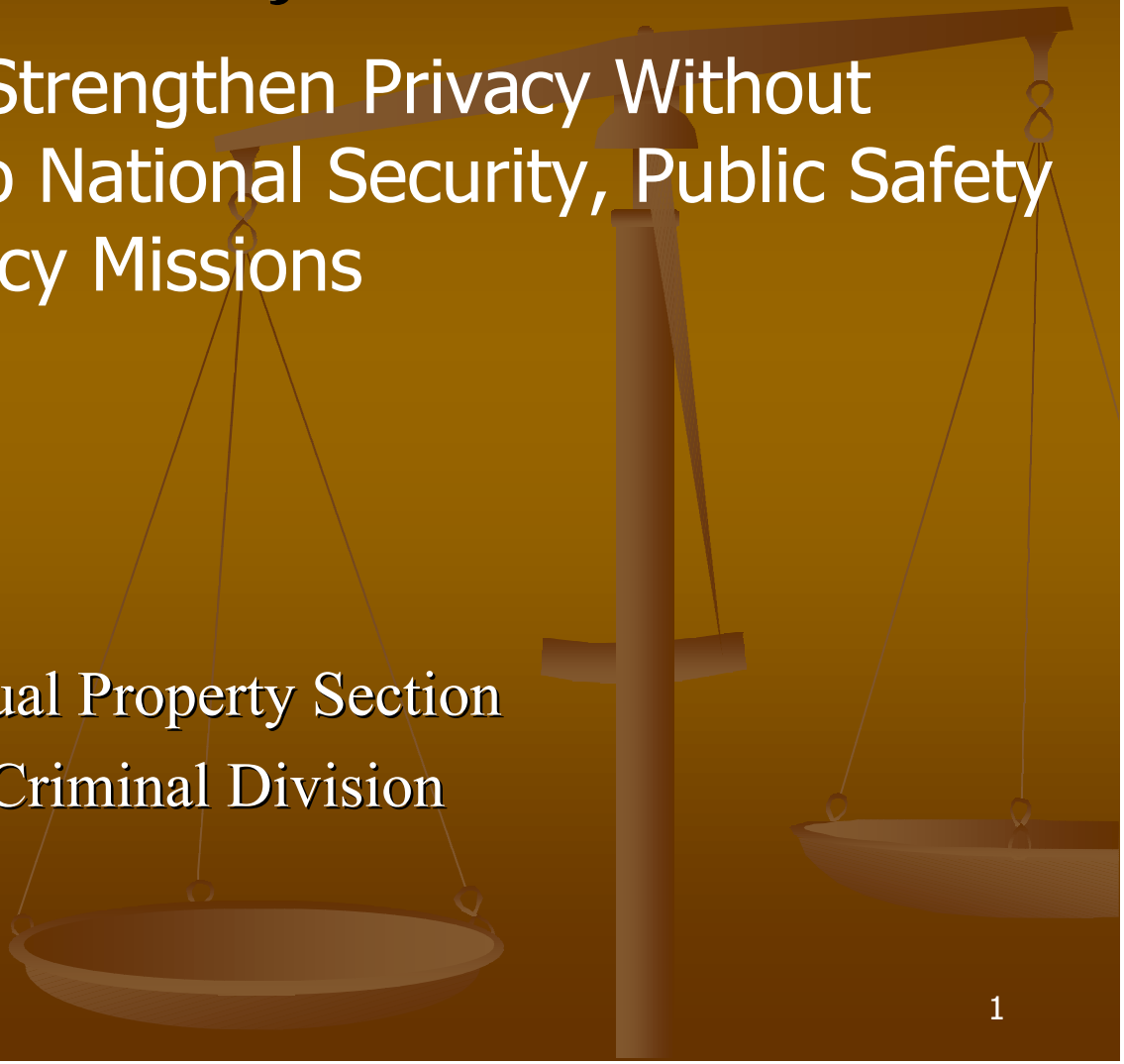
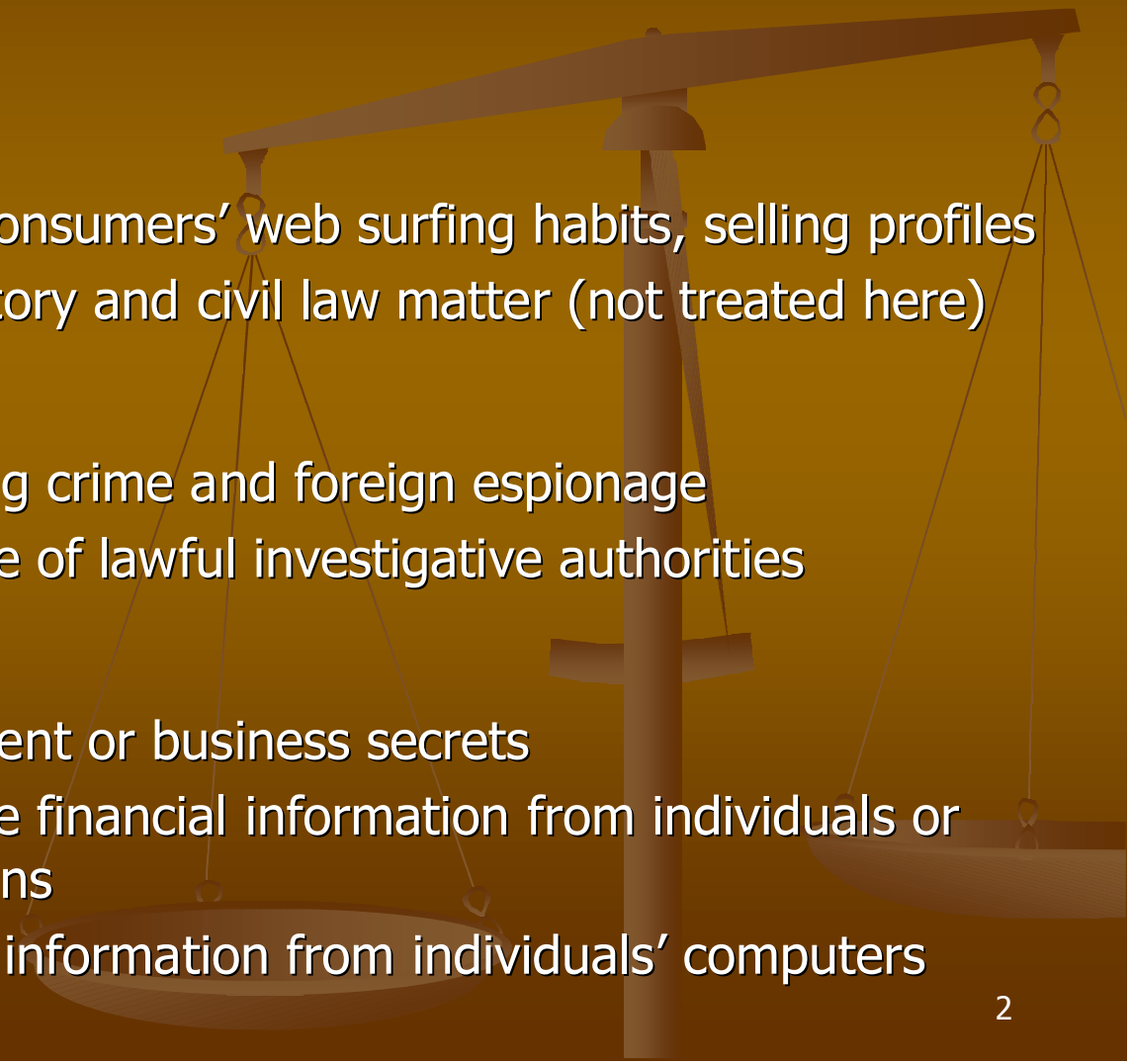
Privacy Protection and Public Safety:

Identifying Ways to Strengthen Privacy Without Creating Obstacles to National Security, Public Safety and Other Public Policy Missions



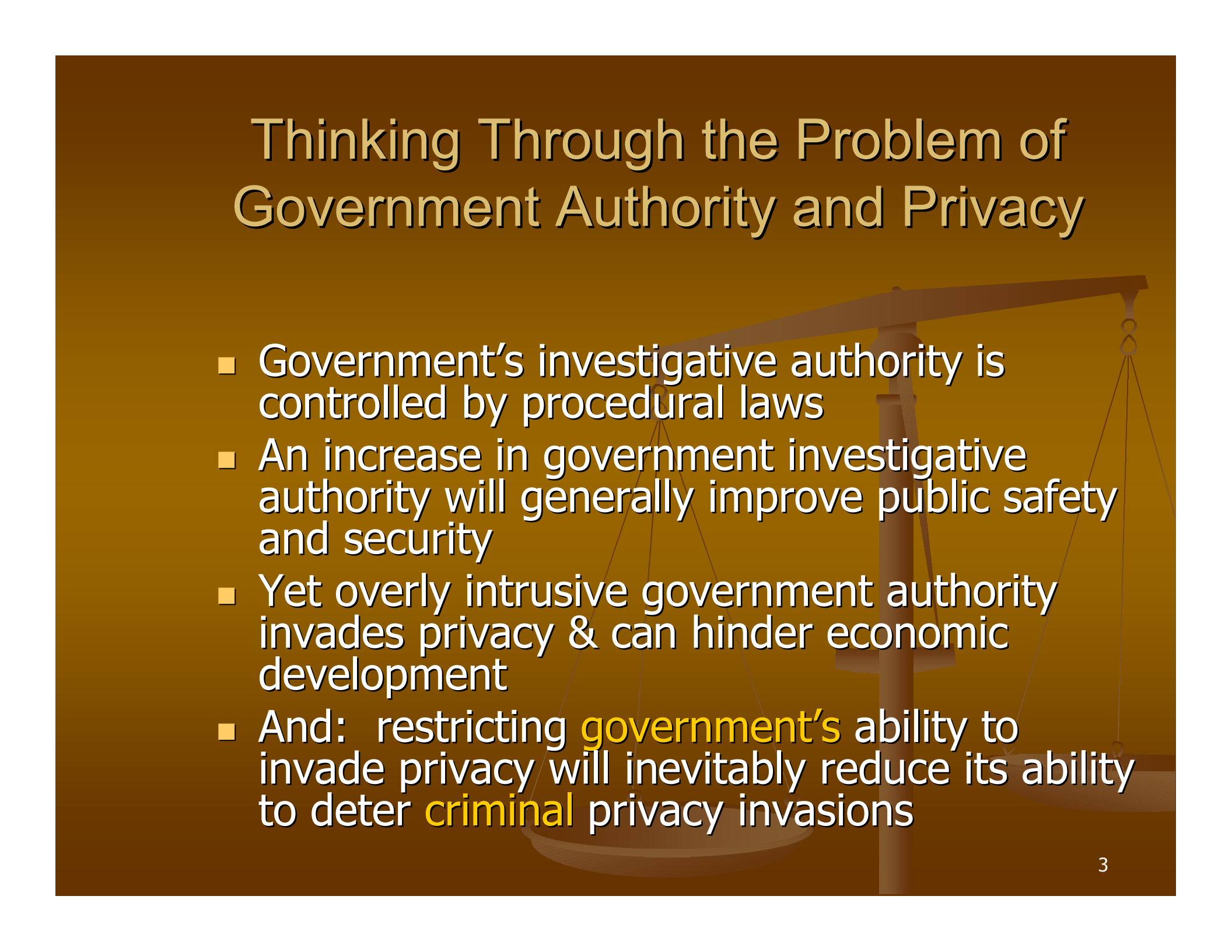
Joel Michael Schwarz
Computer Crime & Intellectual Property Section
U.S. Department of Justice, Criminal Division
(202) 353-4253
joel.schwarz@usdoj.gov

Who Can Invade Users' Privacy?



- Industry
  - E.g.: collecting consumers' web surfing habits, selling profiles
  - Generally, regulatory and civil law matter (not treated here)
- Government
  - While investigating crime and foreign espionage
  - Because of misuse of lawful investigative authorities
- Criminals
  - To steal government or business secrets
  - To obtain valuable financial information from individuals or financial institutions
  - To obtain private information from individuals' computers

Thinking Through the Problem of Government Authority and Privacy

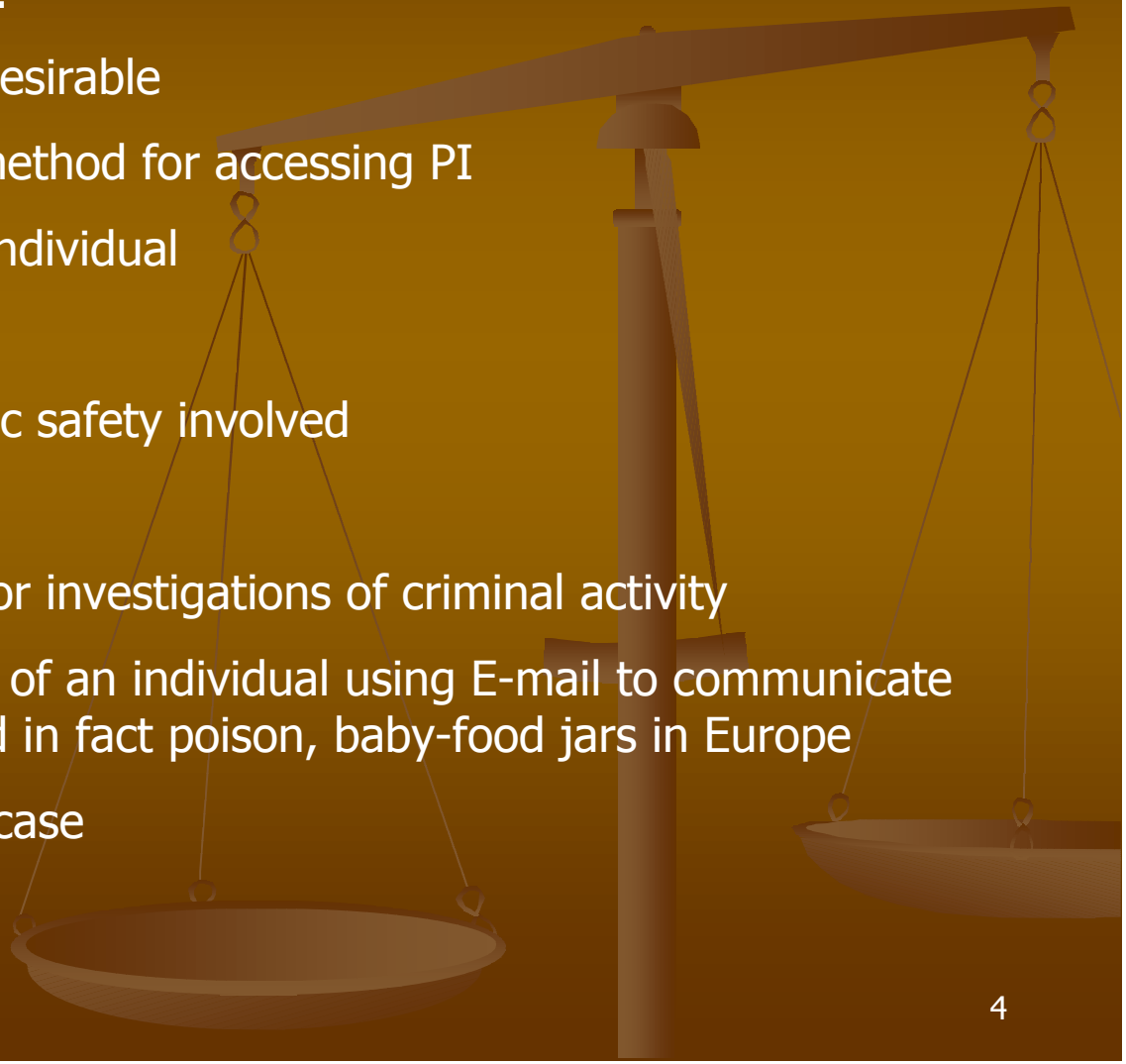


- Government's investigative authority is controlled by procedural laws
- An increase in government investigative authority will generally improve public safety and security
- Yet overly intrusive government authority invades privacy & can hinder economic development
- And: restricting government's ability to invade privacy will inevitably reduce its ability to deter criminal privacy invasions

When do public safety officials need access to PI, and how is it used by them in performance of their job?

- Public safety officials need to access/use PI during investigations of criminal activity. In each case we consider:
  - whether PI is necessary or desirable
  - best and most expeditious method for accessing PI
  - privacy expectations of the individual
  - needs of the investigation
  - the potential threats to public safety involved

- Some examples of access to PI for investigations of criminal activity
  - Gaining access to the E-mail of an individual using E-mail to communicate threats to poison, and who did in fact poison, baby-food jars in Europe
  - South American kidnapping case
  - these are not hypotheticals



Privacy Framework - Scope Section

Exceptions to the Principles for purposes of national security, public safety, etc. should be:

"(a) limited and proportional to meeting the objectives to which the exceptions relate; and,

(b) (i) made known to the public; or,
(ii) in accordance with law."

- Exceptions should be taken for "categories" of information – not "case by case"
  - ex. disclosure when inadvertently learn of a crime while servicing systems. We want to encourage industry to always share this information, not require them to have a privacy review in each individual case to decide whether to disclose
- Re: the proportionality test -- a large gain in public safety should not be the justification for a large wholesale disclosure of PI
  - e.g., trying to identify individuals who are in hospitals in Thailand, after the Tsunami. Goal is to focus search and rescue efforts on those still missing and ID those in hospitals, who may not be able to ID themselves:
    - may request list of patients who were brought in within past 24 hours
    - accessing list of all patients for the entire month of December, or those who were there before Tsunami, might be disproportionate to the goal

Principle 1 – Preventing Harm

Privacy protections should be designed to prevent the misuse of PI

- Laws often categorize this as "privacy infringements"
- In reality, there are 2 kinds of privacy infringements:
  - 1) "unlawful" privacy infringements and 2) lawful privacy infringements
  - We want to prohibit number 1, but not number 2

- Why wouldn't we want to prohibit number 2?
  - Because in order to protect public safety and perform its job, public safety officials must sometimes have access to personal information
  - Is this an infringement of privacy? Certainly.
  - Is this an unlawful infringement of privacy? No.

Indeed, this infringement of privacy does not even necessarily detract from privacy – but can often bolster privacy

Q: How can disclosure – which constitutes an infringement of individual privacy - enhances privacy?

A: Disclosure of PI enhances privacy because disclosure permits public safety officials to . . .

- recover the stolen PI data
- prevent the data from being further disseminated
- assist the victim in seeking civil recovery once the criminal is identified
- deter would-be criminals from even making the attempt to steal PI, since it would be clear to those criminals that they will be prosecuted and punished

- When prohibiting or punishing privacy infringements under our laws, we should qualify the references in those laws to "unlawful" privacy infringements
- We can define "unlawful" privacy infringements as excluding those actions taken pursuant to a domestic statute, authorized by a court or by duly issued legal process
- Ensure that the legal investigative processes that allow for these "lawful" privacy infringements contain their own, built-in privacy protections
    - ex. Search warrant – suppress evidence/criminal sanctions for abuse, etc.

Principle 2 – Notice

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include a number of variables (as set forth in the Framework)

- Since the disclosure of PI might have to be made to a public safety agency (either voluntarily or through legal process) – notice should include this poss.
- In laws/rules that pertain to notice, we might consider requiring that the provision of notice include notice of this fact
- For example, in the U.S. a notice used by doctor's offices:
  - "We will disclose your health information when we are required to do so by federal, state and other law. . . We will disclose your health information when order in a legal or administrative proceeding, such as a subpoena, discovery request, warrant, summons, or other lawful process. We may disclose health information to a law enforcement official to identify or locate suspects, fugitives, witnesses, victims of crime or missing persons."

Principle 3 – Collection Limitation

The collection of personal information should be limited . . . relevant to the purposes . . . and . . . should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

- In order to conduct public safety investigations, prevent terrorism and fight crime, law enforcement will sometimes use non-public investigative means such as:
  - Search warrants, Interception of Content, and Access to Stored Electronic Communications
  - Each of these mechanisms should have its own privacy protections built in (ex. In U.S., access to stored content by LE requires a search warrant issued by a judge, a high burden of proof, as well as limits, like minimization)
  - In order to maintain the integrity of these investigations, the use of these tools, and the collection of the information cannot be disclosed, and notice cannot be given before their use (most of these tools requires notice after the investigation)

In drafting privacy law, we should therefore exempt information collection by government/public safety entities from any collection limitation law, to the extent the collection is authorized by law or legal process

Principle 4 – Uses of PI

"Personal information collected should be used only to fulfill the purposes of collection . . . except: with consent; when necessary to provide a service or product; or, by the authority of law and other legal instruments, etc."

- The private sector is often the first to see evidence of crimes (theft of credit cards, unauthorized bank transactions, etc.)
- An essential part of fighting crime is the voluntary cooperation public safety officials receive from private industry
  - ex. inadvertently discover E-mail re: child molestation when servicing servers – shouldn't they turn over to public safety for child's sake?
- Legislation should not create deterrents to this voluntary cooperation, including not deterring the reporting/sharing information of crimes
  - CSI FBI Report (2004) – voluntary reporting 20% (30% in 2003)
- Sharing evidence of crime will not fall under consent category, or the provision of a service. Similarly, laws don't generally "require" sharing of information relating to a potential crime (thus, not covered by "authority of law" language)
- We want our legislation to permit this sharing voluntarily (even if not compelled)

Principle 5 – Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice . . .”

- While providing choice to individuals is an important privacy protection, there are situations when choice would not be appropriate.

1. Law enforcement investigations – very few criminals would voluntarily choose to allow their PI to be provided to law enforcement investigators, or to have it collected in the 1st place
2. Many domestic security and public safety agencies share information pursuant to domestic laws which permit, and in some cases require sharing (such as U.S.’ child pedophile database). They also share information pursuant to bi-lateral/multi-lateral treaties, and other legal instruments.
    - These should each have their own privacy protections built in. To allow someone, like a pedophile or terrorist, to choose whether to permit sharing, would be disastrous.

Privacy legislation/rules should have an exception from the right to “choice,” when collection, use or disclosure of PI is by public safety or domestic security.

Principle 8 – Access and Correction

Individuals should be able to:

obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; . . . Such access and opportunity for correction should be provided except where: . . . ;

(ii) the information should not be disclosed due to legal or security reasons [or to protect confidential commercial information].”

- As discussed in sub-(ii), laws must permit the denial of access/correction due to an ongoing law enforcement/domestic security investigation because:

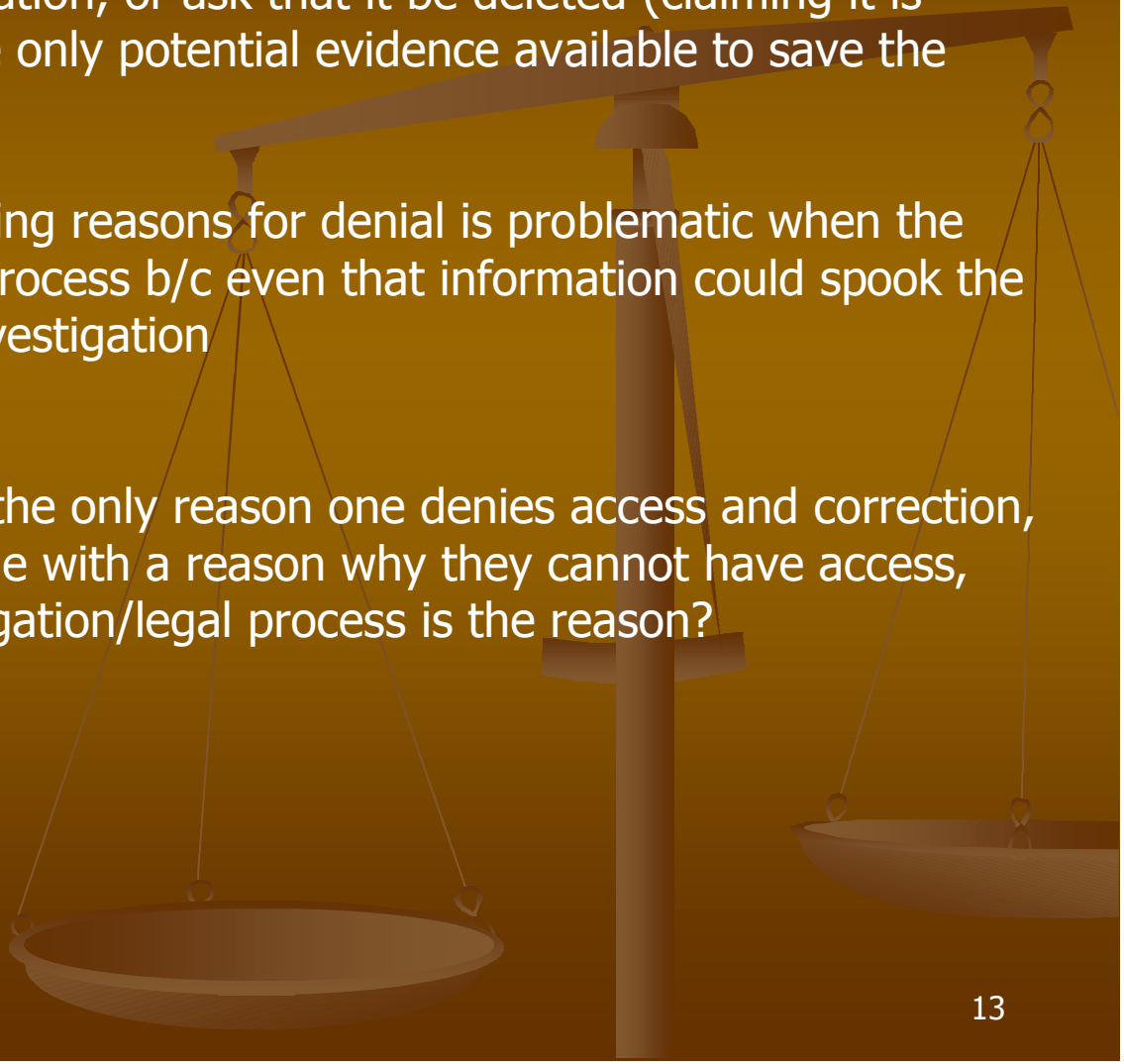
  1. Allowing an individual to view the fact that there have been legal requests made regarding his/her PI, will compromise the investigation, or could cause the individual to act more quickly lest s/he is caught

  2. Allowing the individual to change his/her PI would potentially allow the individual to cover the criminal tracks of evidence.

- For example, if a kidnapper signs up for an E-mail account, provides PI, sends a threatening E-mail and then asks to correct (read CHANGE) his PI, he could easily change it to false information, or ask that it be deleted (claiming it is wrong), thereby destroying the only potential evidence available to save the child

As the commentary clarifies, providing reasons for denial is problematic when the reason is an investigation or legal process b/c even that information could spook the individual enough to destroy the investigation

Q: If Investigation/legal process is the only reason one denies access and correction, how do you deny providing someone with a reason why they cannot have access, without giving away that an investigation/legal process is the reason?



Principle 9 – Accountability

". . . When personal information is to be transferred to another person or organization, . . . controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient . . . will protect. . . . "

- As the operators of our critical infrastructures (such as power, energy, etc.), private industry will often be 1st to know of threats to safety/security.
- Information controllers must feel comfortable sharing this information.
  - unlike private enterprise or outsourcing, industry will not be permitted to review the systems and procedures of governmental agencies.
- To facilitate this sharing and avoid any liability concerns by info controllers, laws could be drafted using language such as:
  - "information voluntarily turned over to public safety or domestic security agencies, for the purposes of facilitating public safety, reporting crime, terrorism, etc., will automatically be deemed adequate to satisfy all safeguard requirements under privacy law."