OECD and Privacy

Barb Lawler, Intuit

4/1/09

ISACA

Agenda

1. Setting the stage: privacy issues and trends
2. Historical context: the OECD family tree
3. OECD: the principles and examples
4. OECD in the 21st Century: APEC
5. Q&A

Takeaways:

- How OECD is the foundation for privacy concepts
- That the OECD concepts come remain fresh and relevant today

What does a CPO do?

CPO responsibilities

- Set global data privacy strategy and policy
- Create standards, training, tools and decision-making guides to aid implementation of privacy
- Build privacy and data requirements into products, services and systems
- Create great experiences for customers around managing their own personal information
- Influence public policy and industry standards
- Measure, assess and report privacy risk and compliance
- Assist or drive incident response

Barb Lawler

- Joined Intuit January 2006
- 9 ½ years in privacy
- 20+ years in marketing and data management at HP
- Built world-class privacy program at HP; first HP CPO
- Testified before House, Senate and IRS
- Business degree from San Jose Sate w/focus in advertising & Marcom
- Bay area native, lives in Los Gatos, 2 kids

Major Trends in Privacy

- **Behavioral tracking and advertising:** or mind your own business, businesses
- **Obama Nation and the focus on Health IT:** ARRA/HIPAA
- **Who *hasn't* had a data breach?**
- **State of the States**: Proscriptive security
- **In the financial crisis and bailout -** who's taking care of all that sensitive data?
- **Objects in mirror are closer than they appear -** beware FACTA amendments
- **"Borderless" personal information flows** require new accountabilities for business
- **Web 2.0 is redefining Web 1.0 privacy rules** and consumer/regulator expectations – "search privacy" and behavioral tracking across the web
- **Personal Information retention**
- **Increased enforcement** and litigation
- **Consumers (and employees) more privacy aware**

What exactly are the OECD Guidelines?

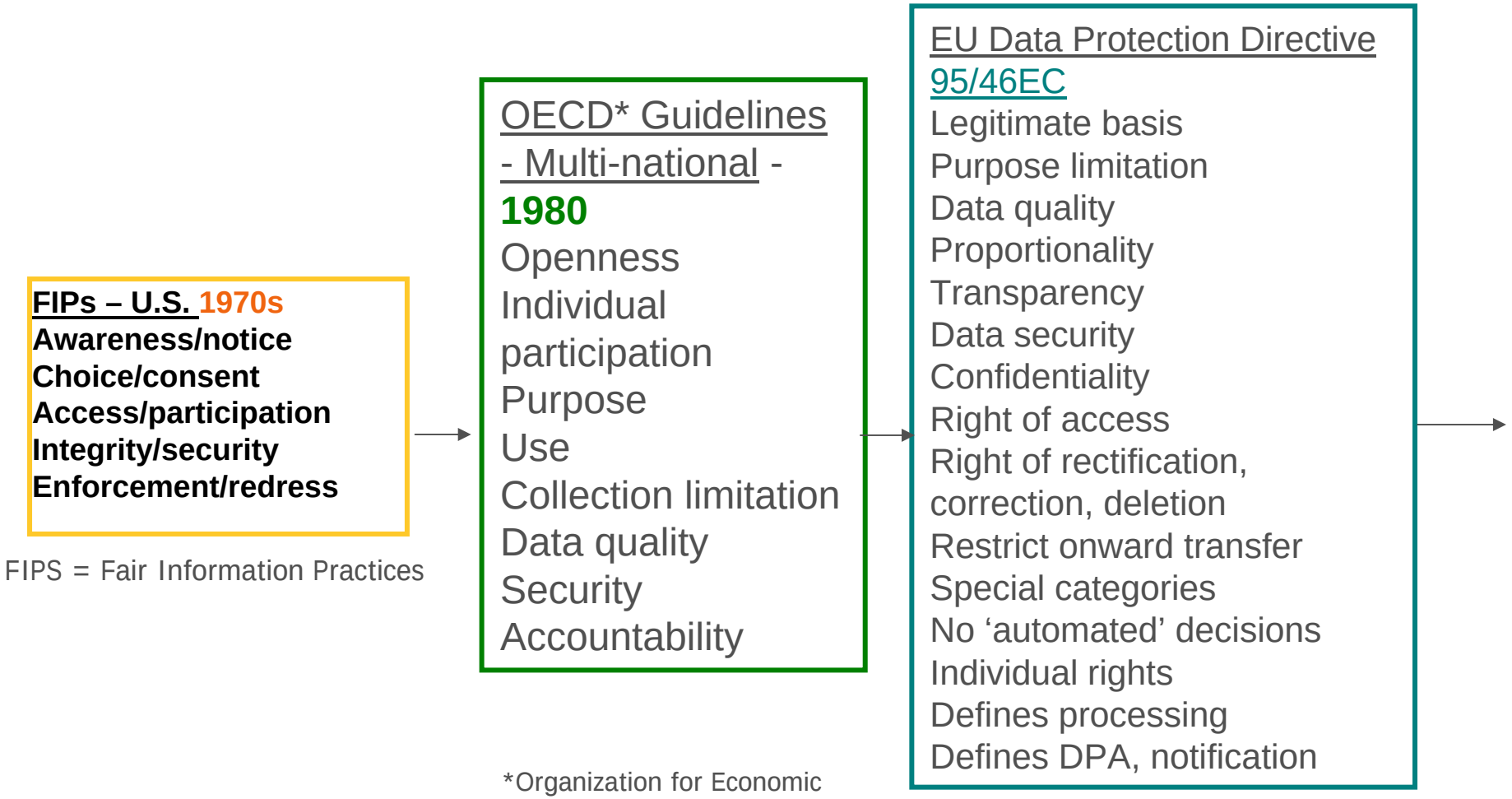
OECD: Organization for Economic Cooperation and Development

Developed in 1980

OECD Guidelines
Openness
Individual participation
Purpose
Use
Collection limitation
Data quality
Security
Accountability

Privacy principles – 3 decades of evolution

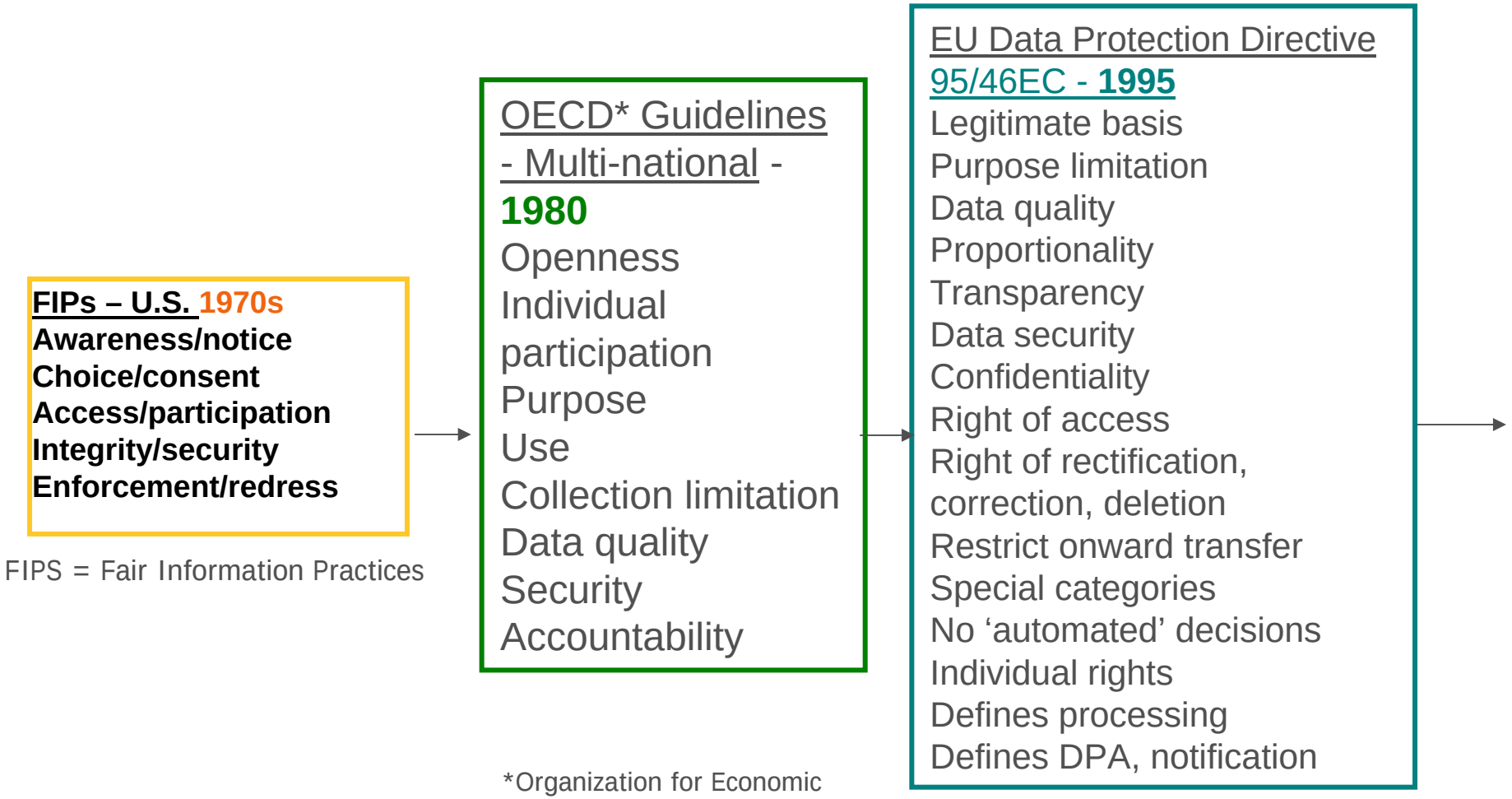
***Note:** Arrows show time progress, not direct feed from previous set of principles*



intuit

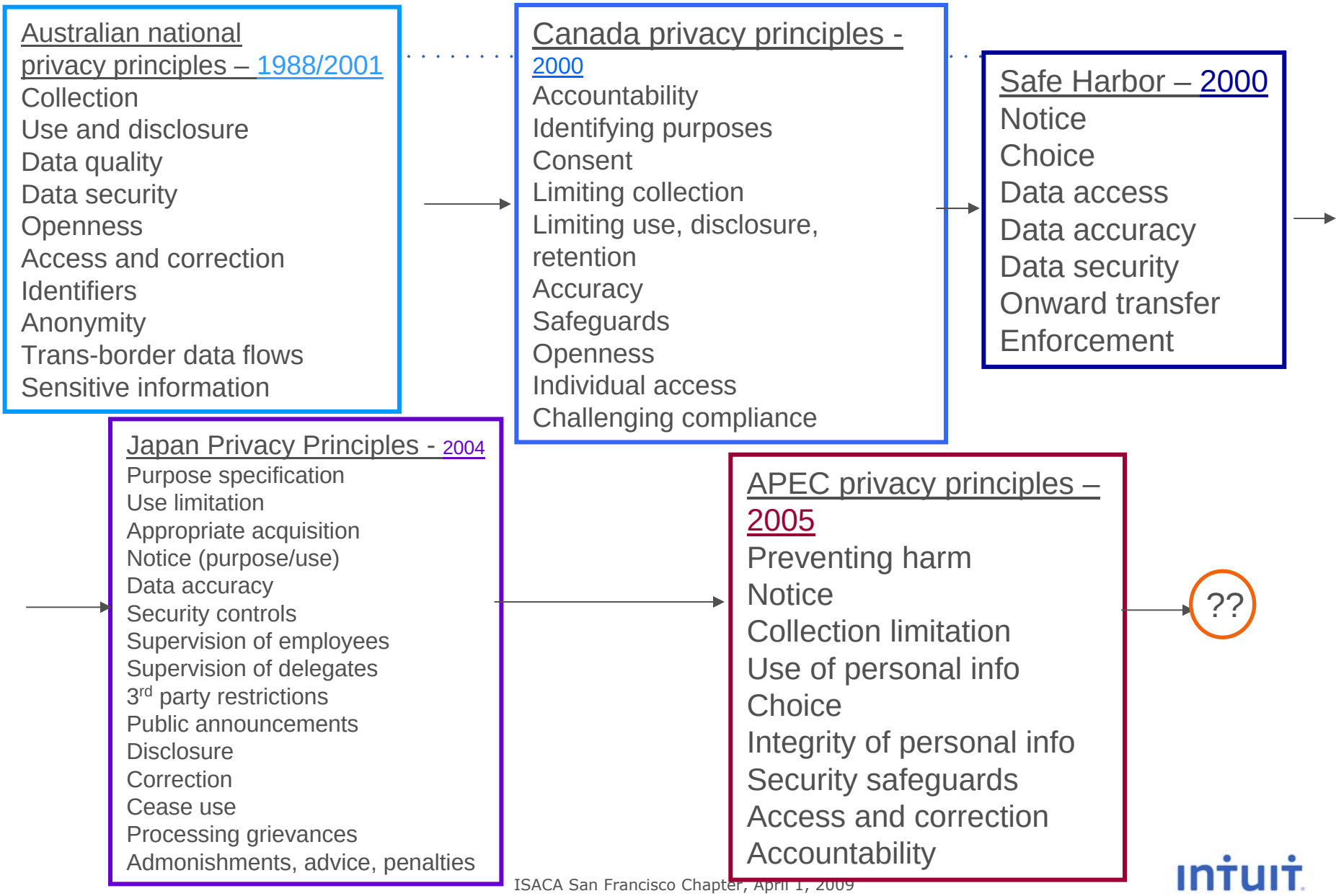
Privacy principles – 3 decades of evolution

***Note:** Arrows show time progress, not direct feed from previous set of principles*



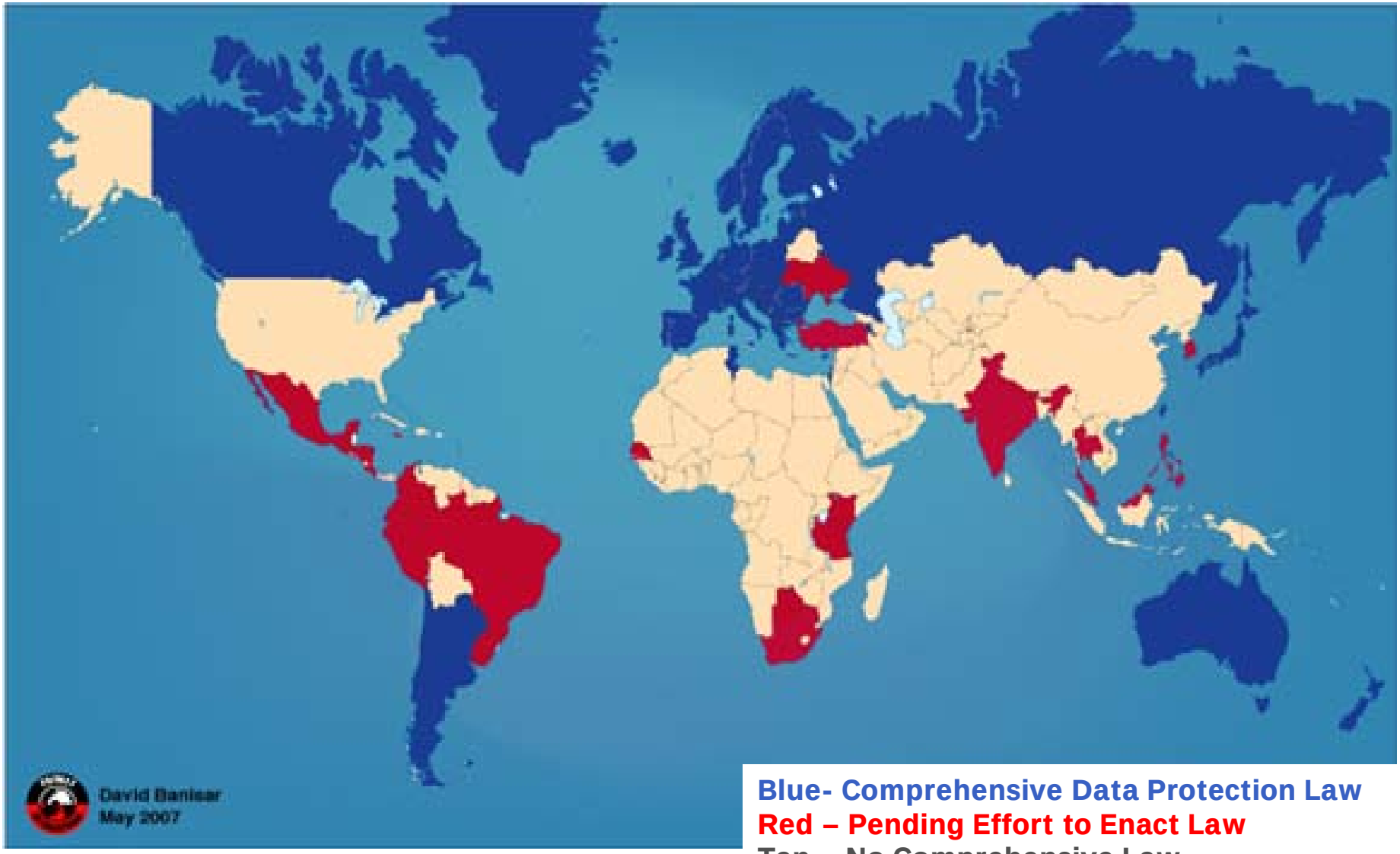
intuit

Privacy principles – 3 decades of evolution



intuit

Privacy Laws Around the World



Blue- Comprehensive Data Protection Law
Red – Pending Effort to Enact Law
Tan – No Comprehensive Law

intuit

OECD Principles designed to lay the foundation for more consistent privacy legislation

OECD: Organization for Economic Cooperation and Development

- Member countries have a common interest in reconciling fundamental but competing values such as privacy and the free flow of information
- Obstacles to trans-border data flows must be avoided
- Principles apply to public and private sector

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

OECD

OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data – 1980

www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM

intuit

OECD Principles: Collection Limitation

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Example:

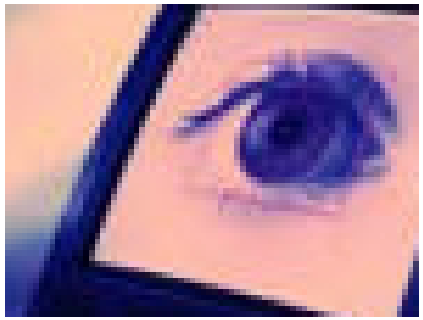
- ***Web form identifies minimum required fields***
- ***Behavioral tracking principles***

intuit

OECD Principles: Data Quality

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.



Examples:

- *A person can update or correct their information*
- *Is demographic information not relevant to completing a purchase transaction?*
- *Controls for data mining/business analytics*
- *Data Appends*
- *NCOA*

OECD Principles: Purpose Specification

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Examples:

- ***Describing purposes and uses in privacy statements, "just in time" notices and Terms of Use***
- ***Annotating web forms – "why do we collect this?"***

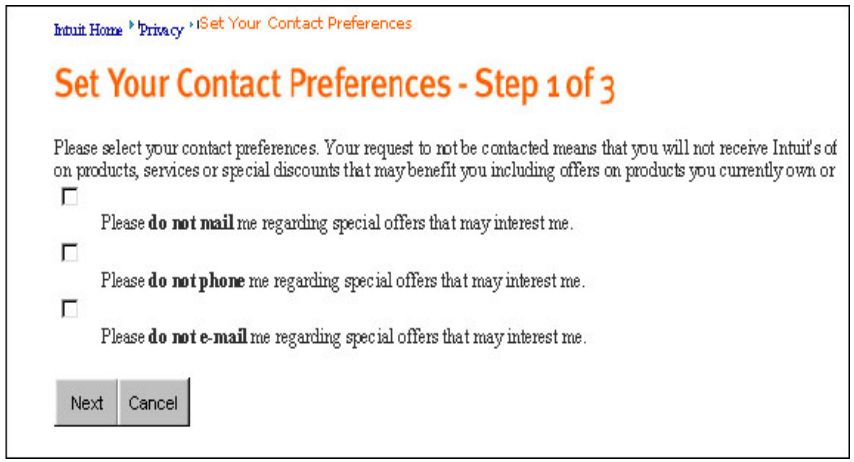
intuit

OECD Principles: Use Limitation

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- *a) with the consent of the data subject; or*
- *b) by the authority of law.*



Examples:

- ***Opt-in, opt-out for data sharing/disclosure***
- ***Do Not Call***
- ***DMA Marketing suppression lists***
- ***Company suppression (opt-out) lists***

intuit

OECD Principles: Security Safeguards

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Examples:

- *Security policies and practices*
- *Encryption of sensitive data*
- *Role/location-based access*
- *FACTA-114 Red Flags*

OECD Principles: Openness

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Examples:

- *Privacy statements on web sites*
- *GLB, HIPAA privacy notices*
- *P3P policies*

intuit

OECD Principles: Individual Participation

Individual Participation Principle

An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him/her;
- b) to have communicated to him/her, data relating to him
  - within a reasonable time;
  - at a charge, if any, that is not excessive;
  - in a reasonable manner; and – in a form that is readily intelligible to him/her;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial;
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

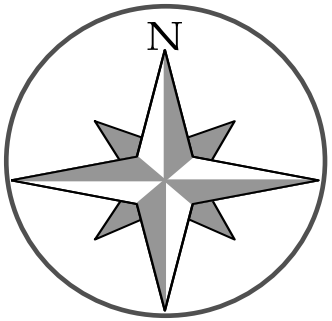
Examples:

- *Ability to view your HR file*
- *Request copy of or correction to your credit*

OECD Principles: Accountability

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.



Examples:

- *A responsible individual for overseeing compliance, e.g. CPO, CISO, CRO*
- *Audit Processes: Internal, 3rd Parties, Privacy Impact Assessments*
- *Training*
- *Executive, Board Reviews*
- *3rd Party Programs: TRUSTe, U.S.-E.U. Safe Harbor*

intuit

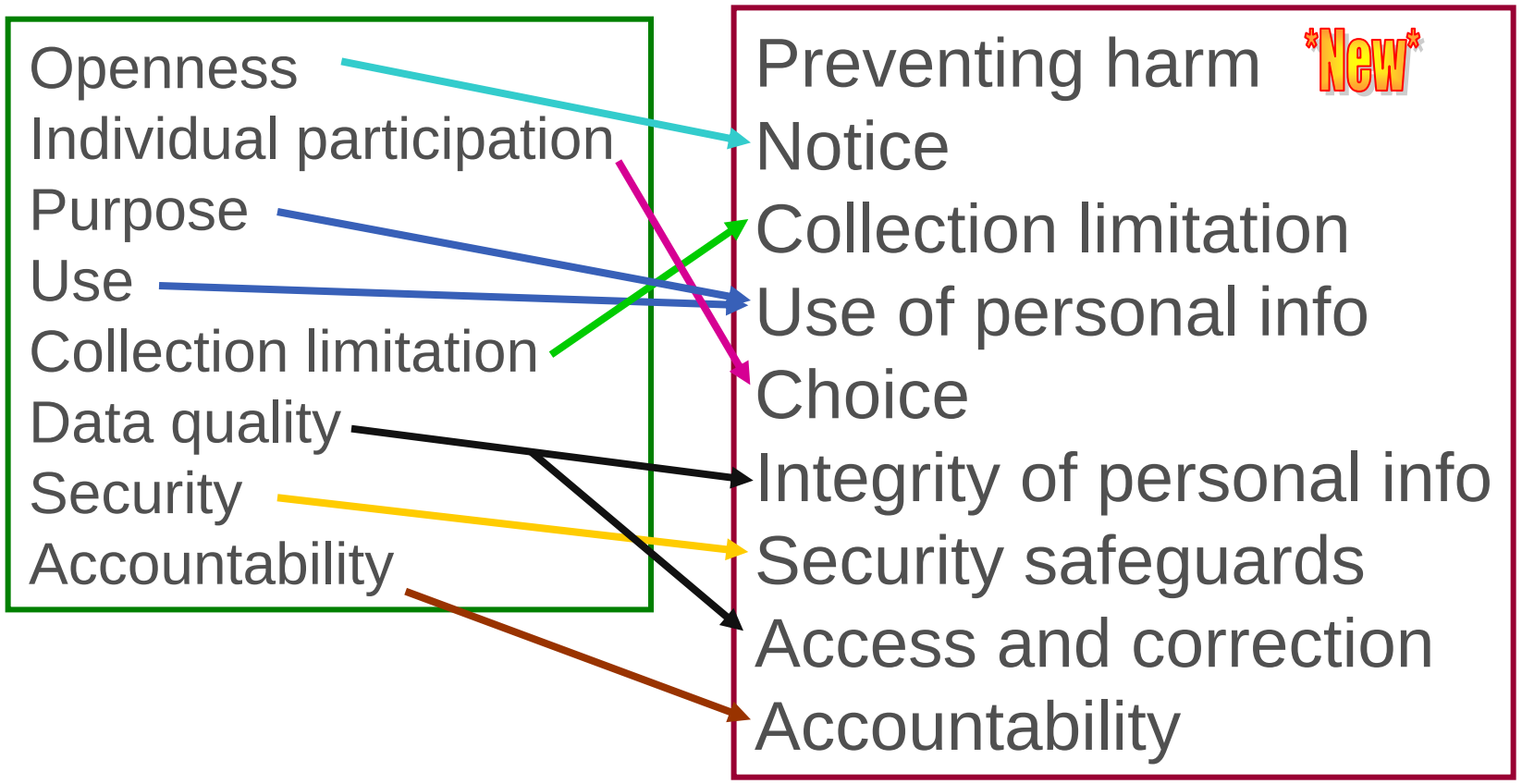
APEC Privacy Principles (2005)

The Asia-Pacific Economic Community (APEC) Member Economies endorsed the APEC Privacy Framework to encourage the development of appropriate information privacy protection and as a means to ensure the free flow of information in the Asia-Pacific region. It is not a law or directive as in the EU, but rather common guidance.

Resources

- www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html

APEC Privacy Principles (2005)



APEC represents a modern, global, 21st century view about the ubiquity of data collection and use, and global information flows in a global economy.

intuit

Intuit Master Privacy Policy

Intuit's Privacy Policy is built on the following globally recognized Privacy Principles:

Accountability – *how we keep our promises*

Notice – *we tell people what we are doing*

Choice – *we offer people choices about the use of their information*

Sharing and Third Parties – *we don't share outside of Intuit; vendors must follow our policy*

Security – *we safeguard information*

Data Use and Integrity - *we can use information to make better customer experiences, products and grow our business*

Access - *people can view & correct their personal information*

http://intuitcentral.intuit.com/cz/dept_pages/privacy_team/MasterPrivacyPolicy.htm

Questions?

Resources:
Dr. Alan Westin paper

FTC Commissioner Leibovitz
speech 3/10/09 (CDT Gala Dinner)

Privacy and Security

Privacy and Security both impact personal information, but are sometimes commingled …

Privacy is about people. Privacy is about the "what".
It is about personal information which can identify and/or locate a person.

Privacy drives many "hows", including security, business processes, product design and customer experience.

Security is about assets. Security is about the "how".
It is about protecting resources, including personal information, which provide value to the company.

Security is driven by and integrates a number of "whats", including privacy, compliance, confidential information and IP protection.

Privacy is often enabled by good security,
but good security does not equate to good privacy.

What is personal information?

Personal information includes data related to a person, which can be used to **identify or locate that person**. It often provides the ability to profile or infer other characteristics and behaviors about a person.

A "person" means Intuit potential and current customers, our customers' customers or employees; and it includes **potential, current and former employees and others in the workforce**.

- **Personal information may or may not be "sensitive".**
- **Personal information may be "public", not "private".**

- **There are many regulatory and industry definitions of personal information**

Privacy Headlines

Iron Mountain Loses GE Money Data Tape, January 2008

Facebook Founder Apologizes To Users For Social Advertising Roll-Out , December 2007

Microsoft Redesigns Ad Format On New Health Site To Address Privacy Concerns, November 2007

Nine Consumer Groups Seek Do-Not-Track List, November 2007

Google Reduces Lifespan Of Cookies In Response To Privacy Feedback, August 2007

Name Foul-Up Results In Exposure Of Consumers' Financial Data, November 2007

Report: Fears Over Online Privacy Soar, January 2008

Litigation Analysis: TJX Ran Afoul Of PCI Requirements, November 2007

TJX Reaches $40M Settlement With VISA, Fifth Third Bancorp, November 2007

Revised TJX Settlement To Offer over 450,000 Customers Vouchers Or Checks, September 2007

Records For 25 Million Individuals, 7.25 Million Families Lost After UK Govt. Tax Agency Foul-Up, November 2007

UK Govt. Tax Agency Apology Letters Contain Sensitive Personal Information, November 2007

Survey: Price Tag For Every Data Record Lost Is $197, December 2007

Pfizer Offers Credit Monitoring To Individuals Affected By Third Breach Since May, September 2007

Source: IAPP Daily Dashboard