Seeding Guidelines and more to come:

Ensure that attention is paid to the distribution and linking to personal data between entities in class diagrams. Ensure that privacy interface design guidelines, such as the 7Cs (Comprehension, Consent, Context, Confinement, Consistency) are incorporated into well-documented interface designs.

Ensure that Privacy Services (e.g., for Audit, Data Usage, Validation, Security) are integrated into behavioral diagrams e.g., Scenario diagrams.

Ensure that processes are in place to similarly capture and document the analysis and design behind third party code for privacy violations before incorporation in existing software.
Privacy Productivity by Design for Software Developers

Dawn N. Jutla, PhD
Increasing Privacy Productivity for Software Developers
- using simple methods that also document compliance

Dr. Dawn N Jutla, Sobey School of Business
Saint Mary's University, Halifax, Canada, NS
Convert the tension between privacy and advertising models into a positive sum scenario

Recruiters

Advertisers

Mobile App and Game Developers

Platform (e.g. Monster, Google, VISA, iPhone, Windows, Facebook, XBOX)

Users/Consumers/Gamers FREE or $$$
Mobile Marketing Aggregator

Assembles customer’s personal data

FROM:
(1) across many mobile services within an organization; and/or
(2) across mobile services from third party participating organizations; and/or
(3) online and offline public data

TO:
(1) create user profiles
(2) aggregate, analyze, massage, offer innovative marketing services

????????????????*??4?/??WGPBHWWG7SEDUFS5PJSKXX?3.6.0.97???.IPHONEba4e15c6d45****phone identifier fuzzied out by author??4?2??4?/????device.model.1?iOS4Device??3.6.0.97??4?-L???????%$????????en_CA?America/Halifax????????????????????????

????????ContactListOpened????????????ContactListOpened????????????MyInfoOpened????????????-ReceivedUnreadChatsInBackground??Count?0????????????????ApplicationActivated??BackgroundDuration?<30sec???
???.????????
Cloud innovators

As Flurry.com collects user data from tens of thousands of apps, its recommendation engine works with big data.

"At our peak, we handle more than 15000 session reports per second. Flurry tracks over 200 billion total data points per month, including any unique event or action tracked within any app sessions"

With such petabytes of continuous consumer data, Flurry builds citizen profiles from across multiple mobile apps, and effectively matches and suggests a client's company mobile app to its client's targeted customers all over the world, 365 days a year, 24 hours a day.
Personal Profile Data Flows...

Advertisers → Merchants

Marketing Aggregator (e.g. Flurry, MobClix, Traffic MarketPlace)

Application/App Provider (e.g. eDY, PayPal, Google Wallet, VISA, Skype, OpenFeint, Realtor)

Device and OS (e.g. iPhone, iPAD, iOS, Android Phones, DoCoMo phones, Windows Phones)

Carrier (e.g. network carriers: AT&T, Bell, DoCoMo, Rogers, Sprint, Telus)

Consumers

User-provided personal data (each platform and merchant may get different data attributes) in a single service

User profiles sent to advertiser networks and to merchants

Ads, offers, deals etc.
SalesForce Unveils Government Cloud, April 25, 2012

"The dedicated government instance will offer the same high level of security, reliability and availability as other salesforce.com instances and will support existing security and privacy standards and certifications including FISMA, SSAE 14, GSAA 705, ISO 27001, PCI DSS Level 1, Multi Factor, and TROIKA.**


Once it becomes law, Federal Agencies will be required to implement "automated and continuous monitoring" of IT systems for incidents that impact confidentiality, integrity and availability. The law further defines continuous monitoring to mean "monitoring, with minimal human involvement, through an uninterrupted, ongoing real-time, or near real-time process used to determine if the complete set of planned, monitored, and deployed security controls within an information system continue to be effective over time with rapidly changing information technology and threat vectors."

---

Palo Alto Networks

[ mongoose ]
"The dedicated government instance will offer the same high level of security, reliability and availability as other salesforce.com instances and will support existing security and privacy standards and certifications including FISMA, SSAE 16 (formerly SAS 70), ISO 27001, PCI-DSS Level 1, Safe Harbor, and TRUSTe."


Once it becomes law, Federal Agencies will be required to implement “automated and continuous monitoring” of IT systems for incidents that impact confidentiality, integrity and availability. The law further defines continuous monitoring to mean “monitoring, with minimal human involvement, through an uninterrupted, ongoing real time, or near real-time process used to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time with rapidly changing information technology and threat development.”
Requirement 7: By Business need to know...

Detailed PCI DSS Requirements and Security Assessment Procedures

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.
Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs.
Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know.
Requirement 8: Assign a unique ID to each person with computer access.
Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.
Payment Card Industry Data Security Standards (PCI DSS)

Critique: Don't say how privacy controls will be added to platforms that have advertisers on the same or different cloud instances.
User-provided personal data (each platform and merchant may get different data attributes) in a single service

User profiles sent to advertiser networks, aggregators, and to merchants for Ads, offers, deals etc.
Traditional Management

CPO/CSO

Privacy and security control requirements, policies, and implementation mechanisms are regularly maintained according to industry standards and regulations. Privacy and security training to all functional areas. Privacy best practices and communication.

Audit function is capable of conducting technical privacy reviews of software products and services, and ensure that auditing is carried out annually.

Tie employee privacy behaviors to the organizations’ employee code of conduct and/or to annual performance reviews.

Educate users
For online services including mobile apps...

Beyond Trust-e certification
Beyond Posting a Privacy Policy
Beyond Making a Privacy Policy available to the User on-demand
Beyond the Mobile Marketing Association and GSMA mobile app guidelines
To Reaching the Software Engineers in the Software Organizations

"TRUSTe requires certified apps to: securely transmit data using HTTPS; access only the customer data needed to provide the service; protect data from unauthorized access or disclosure; and provide an opt-out from marketing email communications."
The Future of Privacy

Change the Paradigm to Positive-Sum, NOT Zero-Sum

Courtesy: The Office of the IPC, Ontario
Privacy by Design: The 7 Foundational Principles

Proactive not Reactive: Preventative, not Remedial;

Privacy as the Default setting;

Privacy Embedded into Design;

Full Functionality: Positive-Sum, not Zero-Sum;

End-to-End Security: Full Lifecycle Protection;

Visibility and Transparency: Keep it Open;

Respect for User Privacy: Keep it User-Centric.
Growth of Privacy by Design Internationally

In January, Privacy by Design was featured in the draft EU Data Protection Regulation;

Last year, a Privacy by Design approach in the McCain-Kerry Commercial Privacy Bill of Rights;

Former Federal Trade Commissioner, Pamela Jones Harbour, strongly supports the use of Privacy by Design and advocates its application in F.T.C. Consent Decrees;

Jon Leibowitz, Chairman of the Federal Trade Commission, has recommended Privacy by Design;


In March, 2012, the FTC released its final report on protecting consumers’ privacy – specifically recommending that companies adopt Privacy by Design in building consumer privacy protection at every stage in their product development.

http://www.ftc.gov/opa/2012/03/privacyframework.shtm
Privacy by Design: Proactive in 25 Languages!

- English
- French
- German
- Spanish
- Italian
- Czech
- Dutch
- Estonian
- Hebrew
- Hindi
- Chinese
- Japanese
- Arabic
- Armenian
- Ukrainian
- Korean
- Russian
- Romanian
- Portuguese
- Maltese
- Greek
- Macedonian
- Bulgarian
- Croatian
- Polish

Courtesy: Office of the IPC, Ontario
Regulatory Approaches

Last year, FTC Chairman, Jon Leibowitz, stated, “... self-regulation of privacy has not worked adequately and is not working adequately for consumers. We'd like to see companies work a lot faster to make consumer choice easier;”

February 23, 2012 – the Obama administration called for stronger privacy protections for consumers as mobile gadgets, Internet services and other technologies have become more effective at tracking individuals;

The White House outlined a proposed Consumer Privacy Bill of Rights and urged companies and consumer groups to jointly craft new privacy codes of conduct, with participation from the US Department of Commerce.

These codes of conduct will initially be voluntary for, but those that agree to abide by them could be subject to FTC sanctions for violations.

Courtesy: Office of the IPC, Ontario
PbD, Sectoral Laws and Smart Grid

Sector specific laws may be helpful in the emerging Smart Grid – providing functional specifications that electricity distributors must adhere to;

The National Institute of Standards and Technology (NIST) recommended PbD as a methodology for future smart grid development;

Decision of the California Public Utility Commission to protect the privacy and security of customer electricity usage data (Rulemaking 08-12-009, Decision 11-07-056, July 28, 2011) – “...the Privacy by Design methodology offers a promising approach to ensuring that data practices promote privacy, not just in the FIP of data minimization, but in all aspects of privacy planning;”

The IPC has partnered with San Diego Gas & Electric to embed PbD into their Smart Pricing Program, thereby delivering new value to customers, advancing state policy and delivering economic benefits.
Proposed Scope of the OASIS PbD- Software Engineers TC

Establish privacy objectives and requirements that satisfy the 7 foundational principles of PbD

Software analysts and designers should use and document a Privacy Impact Assessment (PIA) for any new software service, preferably the PbD-PIA.

Ensure that software developers integrate privacy requirements (e.g. need for notice, disclosure, obtaining user consent, user access, data minimization, data security) into functional Use Cases for software products and services.
a. A Use Case should incorporate descriptions of data collection, data usage, data flows (input and output), the privacy and security policies under which the data flow is being received, and the privacy and security policies under which the data is accessed (data flow exits), and a link to the internal privacy policy (version/date to be specified). Analysts may use the OASIS PMRM methodology to aid in this step.

b. The Use Case should exhibit compliance to all policies and FIPPs, including data minimization, notice to consumers [if not previously notified], declaration of purpose to consumers [if not previously done], and means to obtain consent from consumers regarding the handling of their personal data [if not previously obtained].
Seeding Guidelines and more to come.

Ensure that attention is paid to the distribution and linking to personal data between entities in class diagrams.

Ensure that privacy interface design guidelines, such as the 7Cs (Comprehension, Consciousness, Choice, Consent, Context, Confinement, and Consistency) are incorporated into well-documented Interface designs.

Ensure that Privacy Services (e.g. for Audit, Data Usage, Validation, Security) are integrated into behavioral diagrams e.g. Scenario diagrams.

Ensure that processes are in place to similarly capture and document the analysis and design behind third party code for privacy violations before incorporation in existing software.
Increasing Privacy Productivity for Software Developers - using simple methods that also document compliance

Dr. Dawn N Jutla, Sobey School of Business
Saint Mary's University, Halifax, Canada, NS
Educate Software Engineers

Computer Science curricula that require new standard
guidelines to train next generation developers on how
to integrate privacy into SML analysis and design
documentation and check for privacy legislation
compliance in all third party and/or open-source code,
could be targeted.

After the standard is built..

We can go to the source
Educate Software Engineers

Computer Science curricula that require new standard guidelines to train next generation developers on how to integrate privacy into UML analysis and design documentation and check for privacy legislation compliance in all third party and/or open source code, could be large!!
Implement the standard in easy-to-use tools for software engineers to use
Internet-Available Consent Directive Analysis Model

Much More to do ...
Echoing words from Commissioner Cavoukian with very few amendments

Lead with Privacy by Design;

Change the paradigm from the dated “zero-sum” to the doubly-enabling “positive-sum;”

Deliver privacy AND security, AND any other functionality (emphasis on ADVERTISING), in an empowering “win-win” paradigm – abandon false trade-offs;

Embed privacy as a core functionality in software.

The future of privacy and our freedoms may depend on it!
Contact:
Dawn Jutla, PhD (Computer Science)
SOBEY SCHOOL OF BUSINESS
Halifax, NS, Canada
dawn.jutla@smu.ca
902 420 5157