Security in knowledge

THE CALL FOR A COMPREHENSIVE PRIVACY PROGRAM

Jeff Northrop, CISSP, CIPP

International Assoc. of Privacy Professionals

RSA CONFERENCE 2013

Session ID: AST2-F41

Session Classification: General Interest

Overview

- Why do we need a comprehensive privacy program?
- Building the case
  - Define privacy
  - Public perception of privacy
  - Government and business response
- Components of a privacy program
- Privacy best practices
- Wrap up

What is "Privacy"

- Public belief: Privacy as anonymity
- Corporate objective: Minimizing the risk of a privacy violation
- Privacy violation: Giving willingly or otherwise, personal information to a third party without consent

Public Desire for Privacy

- Public wants anonymity
- Notion of over-sharing (social media, *et al*)
- Fear a loss of control of their personal data
- Discomfort with profiling:
  - Harris study: 82% consider ability to be tracked an invasion of their privacy (http://www.networkworld.com/news/2012/100112-fiberlink-survey-262940.html)
  - Privacy & American Business study found 60% decided not to patronize a store because of doubts about the company's privacy protections (New National Survey on Consumer Privacy Attitudes to Be Released at Privacy & American Business Landmark Conference June 10, 2004)
- Online environment as foreshadowing

Anecdote #1: Creepy Behavior

Sumit Suman Dec 8, 2012 - Public

Recently, I visited the landing & pricing page at UberVu.com. I did not signup for anything, did not leave my email, did not connect with any of their social media properties.

One day later, I get an email (see attached image).

I'm sure they triangulated some information but how could they pin point to personally identify me? Is this common & so blatant (or even legal)?

Hello Sumit,

Thanks for visiting uberVU's web site, and I wanted to make sure you had all the information you need and all your questions were answered.

I'd welcome the opportunity to have a discussion about your current social marketing strategy, as well as discuss how the uberVU social media platform is enabling social marketers to turn social data into actionable insights.

Our customers spend less time pouring through the data and more time driving the engagement of their audience.

We can easily set up a time to show you the tool as a demo. Just let me know what date/time works for you.

Regards,

Anecdote #2: Do Not Track

- W3C created flag in browser header to express 3rd party tracking preferences
- Instigated by the public and technology working groups
- First instance of public and technology leading privacy public policy discussion
- Congress trying to act
- Industry groups discussing regulations

Business and Privacy

- Big Data driving business (efficiency, productivity, innovation, etc.) but escalating privacy tensions
- Remember, consumers fear loss of control...
- … While Big Data requires personal information for fuel
- Regulations try to address this tension but struggle

Government Response

- Primary tools: Notice and choice/consent
- Exceptions: HIPAA, FCRA, government collection
- FTC enforces on "reasonable expectation"
  - Social media settlements
- Looking for broader controls
  - Increasing proposals in Congress
  - US Privacy Bill of Rights

Business Response

- Growing prevalence of compliance programs
- Rise of the CPO
- Ubiquitous privacy policies
- With this in place, what could go wrong?

Anecdote #1: Intagram

- Policy change allowing use of personal images for advertising
- Public outcry, poll LA Times 66% "will not recover"
- Withdraw language
- All within a week!

Anecdote #2: Confetti on Parade

- Thanksgiving Day parade in NYC uses shredded Nassau County police records for confetti.
- Exposes all sorts of PII unintentionally

Moving Towards Accountability

- Moving from notice and choice/consent to accountability
- Balance business value versus individual risk
- Regulators looking for comprehensive privacy program

Comprehensive Privacy Program

- Demonstrable capacity for legal compliance
- Top-down support + appoint privacy officer
- Across disciplines + job functions
- Privacy inventory + impact assessment
- Policies, controls + training
- Plans for external communication

Privacy Best Practices

- Privacy by Design
- Meaningful transparency
- Obtain explicit consent
- User control
- Minimize, anonymize and secure
- Do as you say

Resources

- Building a Privacy Program: A Practitioner's Guide
  https://www.privacyassociation.org/publications/building_a_privacy_program_a_practitioners_guide/
- TRUSTe Program Requirements
  http://www.truste.com/privacy-program-requirements/
- Office of Information and Privacy Commissioner of Alberta - Getting Accountability Right with a Privacy Management Program
  http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf
- OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data
  http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
- Apec Privacy Framework
  http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- EU Article 29 Working Party Opinion on Accountability
  http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Questions?

Jeff Northrop, CISSP, CIPP

jeff@privacyassociation.org

http://www.linkedin.com/in/jnorthrop/

Security in knowledge