Can you keep a secret? Privacy, Confidentiality, Obscurity, Anonymity...

Artem Kazantsev, Sr. Security Analyst,
University IT Security Office
@DukeITSO
http://security.duke.edu

The plan: Privacy for masses

- Privacy at Duke as institution
- Privacy for you as an individual

Privacy at Duke

- What are our regulatory obligations to keep data private?
  - FERPA
  - HIPAA and HiTech
  - NC Identity Theft Law - N.C. Gen. Stat. § 14-113.20 to 14-133-.23
  - NC Data Breach Law – S1017
  - *(PCI DSS *)*

FERPA (1)

- Family Educational Rights and Privacy Act 1974 (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
  - “Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance”
  - http://registrar.duke.edu/student-records
  -

FERPA (2)

DIRECTORY INFORMATION

The following categories of information have been designated directory information:

- Name(s)
- Addresses
- Duke Unique ID
- Telephone listing(s)
- Email Addresses
- Place of birth
- Photograph(s)
- Major fields of study
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Dates of attendance
- Degrees and awards received
- Most recent previous educational institution attended

HIPAA

- Health Insurance Portability and Accountability Act (1996)
  Privacy rule:
  - The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities". PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual

HITECH

- Health Information Technology for Economic and Clinical Health Act, (Title XIII of the American Recovery and Reinvestment Act of 2009)
  - Subtitle D: Privacy

    The HITECH Act requires HIPAA covered entities to report data breaches affecting 500 or more individuals to HHS and the media, in addition to notifying the affected individuals
  - HITECH permits HHS to impose a penalty of up to $50,000 per violation capped at $1.5 million annually for the same violation.

NC Identity Theft Law

- North Carolina Identity Theft Protection Act of 2005
  - ...restriction on the collection, use, and safekeeping of a consumer's social security number and consumer financial information. The Act requires businesses, charities and government to notify individuals if a security breach has compromised any personal information and placed them at risk of identity theft.

NC Identity Theft Law

- North Carolina Identity Theft Protection Act of 2005
  - ...restriction on the collection, use, and safekeeping of a consumer's social security number and consumer financial information. The Act requires businesses, charities and government to notify individuals if a security breach has compromised any personal information and placed them at risk of identity theft.

NC Data Breach Law

- N.C. Gen. Stat § 75-65

  ...The notice shall include all of the following:

  - (1) A description of the incident in general terms.
  - (2) A description of the type of personal information that was subject to the unauthorized access and acquisition.
  - (3) A description of the general acts of the business to protect the personal information from further unauthorized access.
  - (4) A telephone number for the business that the person may call for further information and assistance, if one exists.

    (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
  - (6) The toll-free numbers and addresses for the major consumer reporting agencies.
  - (7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.
  -

Is the price right?

- Average cost of a breach for organizations is $200 per record
- Reference point:
  UNC Charlotte breach at 2012
  350,000 SSNs were exposed

Duke Data Classification

Data Category:

- Sensitive
- Restricted
- Public

http://security.duke.edu/sites/default/files/documents/Duke%20Data%20Classification%20Standard.pdf

Sensitive Data examples

- Social Security numbers
- Credit Card numbers
- ePHI (HIPAA protected data)
- FERPA protected data
- Donor data
- Contract data
- Financial data
- HR data

How we protected the private data? (1)

- Social Security Numbers:
  - In accordance with these recommendations and the directive issued by Dr Tallman Trask III, the current policy on the collection, storage, and use of Social Security Numbers at Duke is:

    Departments wishing to collect, store, or use SSNs in any way must
    - Show compelling institutional need
    - Receive approval from the Executive Vice President and the Chief Information Officer
    - Permit yearly audits (including server and application security) to ensure safe SSN handling

How we protected the private data? (2)

- Protected (Secure) Network:
  - Access only by VPN and authorized users only
  - Full OIT management
  - Encryption of backups
  - (soon) Multi-factor authentication and role-based access

Duke password-protected websites

- OIT account self-service and other Shibboleth sites:
  - protection with SSL / TLS encryption
  - (soon) Multi-factor authentication

Privacy for you

- Definitions?
  In general, the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed. In specific, privacy may be divided into four categories
  - *Physical: restriction on others to experience a person or situation through one or more of the human senses;*
  - *Informational: restriction on searching for or revealing facts that are unknown or unknowable to others;*
  - *Decisional: restriction on interfering in decisions that are exclusive to an entity;*
  - *Dispositional: restriction on attempts to know an individual's state of mind.*

    http://www.businessdictionary.com/definition/privacy.html

Privacy and Society

- Privacy is always a dichotomy between an individual's rights and the demands of the society
- Society in form of a government, corporations, political organizations, media, religious and other NPO put the pressure on people to sacrifice their privacy in the name of a common good
- Privacy is specific to a culture, a period of time, history and politics

Privacy vs Government

- Examples of violation of privacy by government(s):
  - Video and audio surveillance, facial recognition
  - (Warrantless) Wiretapping and communication interceptions
  - (Unreasonable) Stops and searches, profiling
  - Airport and other body scanners
  - (soon) Surveillance by drones

Privacy vs Corporations (1)

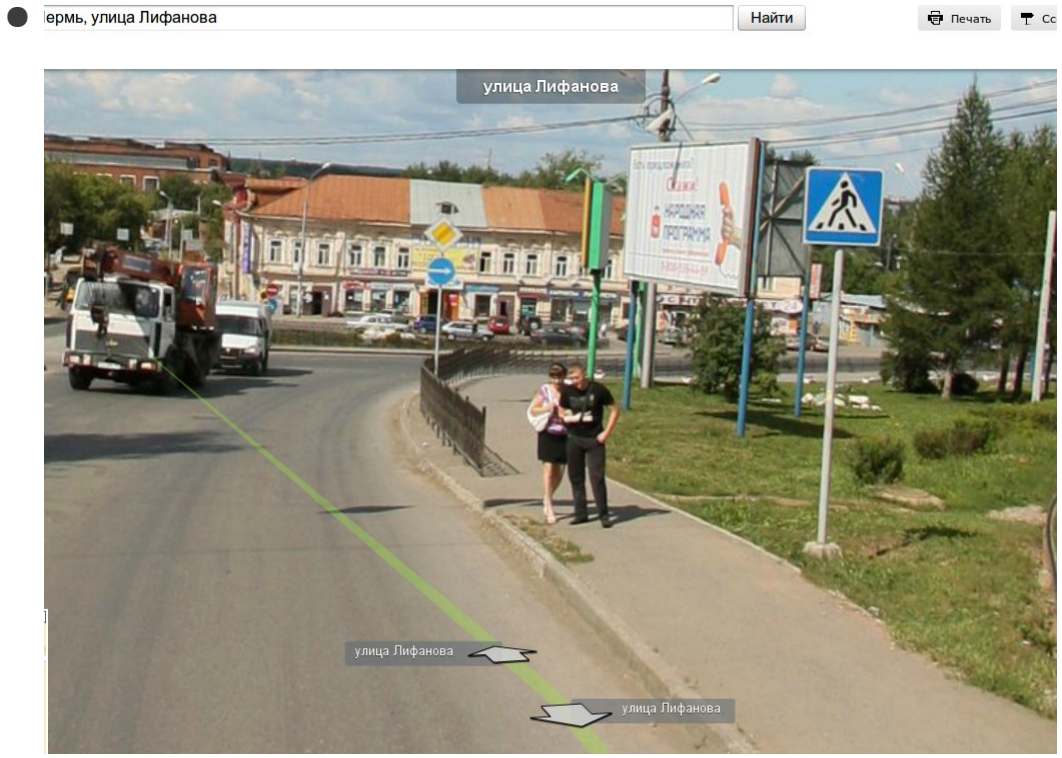
- *aah... What's his face...*
  - *Facebook privacy policy over the years:*
  - *http://mattmckeon.com/facebook-privacy/*
  - *Google on Tuesday acknowledged to state officials that it had violated people's privacy during its Street View mapping project when it casually scooped up passwords, e-mail and other personal information from unsuspecting computer users. http://topics.nytimes.com/top/news/business/companies/google_inc/index.html?inline=nyt-org*
  - *Bloomberg reports that San Jose-based U.S. Magistrate Judge Paul S. Grewal has issued a scathing ruling in a privacy suit involving the company in which he questions Apple's integrity and says that he will no longer take what the company says and face value.*

Privacy vs Corporations (2)

- Sun Microsystems Inc. CEO Scott McNealy: "Privacy is dead, get over it."

Why Privacy is a gray area?

- Example: http://maps.yandex.ru/-/CVR~ZW51



Privacy or Confidentiality?

- The same?
  - Yes / No
- To provide confidentiality:
  - Encryption
  - AAA (Authentication, Authorization, Accounting)

Privacy or Obscurity?

- Exercise:
  - locate public records of your home purchase and it's current value
  - locate public records of your neighborhood homes purchases and their current value
- The map of gun owners... Was it a privacy issue?

Privacy or Anonymity?

- Whistle blowers: take note...
  (why email addresses in Germany are hard to remember)

- **tor** application:
  a legitimate case of using it (to submit anonymous reviews to online publications)

Privacy: can I close the door?

- What ordinary people can do to protect their privacy?
  - Demand change from corporations
  - Unite with like-minded
  - Talk to your congressman or senator
  - Use technology