Privacy and Data Protection – Part II

KTH, Media Law
Pam Storr

Privacy Recap

- Legal requirements on data controller. Must consider:
  - why store personal data?
  - what personal data?
  - is the data correct & up-to-date?
  - how long can the data be kept?
  - is the data secure?
  - where is the data stored?
  - who can access the data?

Practical Perspective

- How does a company/organisation make sure it follows the various legal requirements?
- Examples of new technologies that may impact privacy:
  - cloud computing
  - mapping
  - tracking & surveillance
- Potential solutions

Company/Organisation Perspective

Storing Data

Storage of Data

- Where should information be stored within a company/organisation?
  - internally
  - externally

What are the benefits of storing information internally vs. externally?
Think about the kind of information a company/ organisation stores.
(Does it matter from a privacy perspective what kind of information is being stored?)

Company Information

- Clients/customers:
  - personal data
  - finance
  - communications
- Employees:
  - personal data
  - salaries
  - communications
- Company:
  - organisational structure
  - finance
  - employment
  - intellectual property, trade secrets etc.

Storing Information Internally

- Company policy for stored data, even if not communicated further
- Consider measures to keep data safe!
- Consider risks for data leakage etc.!
  - technical risks (security: encryption)
  - employees (security: access)

Technology 1:

Cloud Computing

Storing Information Externally

- Trend – cloud computing
  - storage of data externally
  - accessible from various places/devices
  - e.g. Dropbox
- Ease of use & convenient
- Using cloud provider's resources: servers/ storage space

Cloud provider has access to company information!

Cloud Computing: legal considerations

- Personal data:
  - does the information include personal data?
  - does the information include sensitive data? (perhaps avoid certain customer/employee data)
- Data back-up:
  - is the data backed up? where?
- Jurisdiction:
  - where is the cloud provider located?
  - which jurisdiction/law applies?
  - where is the data transferred to? (data in transfer, data at rest)

Privacy in Practice

Company Rules & Policies

- Additional rules & policies may apply within a particular company e.g.
  - specific data processing/storing requirements
  - auditing rules require certain data to be available within the company
  - employee privacy policy
  - customer privacy policy
  - …

National legislation

- National laws must always be adhered to! May provide additional rules/guidance

Consider where the company is established → national law on data protection/privacy

If international company may have to consider a number of national laws!

Other Areas of Law

- Other, sometimes conflicting, areas of law may be applicable – privacy may not always trump these areas
- E.g. Privacy vs. Freedom of Expression

http://www.wired.co.uk/news/archive/2013-02/27/google-spain-privacy-battle

Read Wired article; think about implications for privacy & openness/secrecy!

Other Areas of Law

- Obligation to hand out data to law enforcement etc.
  - most likely depends on national law
  - may be up to discretion of company

How privacy-aware are companies such as Amazon, Dropbox, Facebook, Microsoft, ...?
https://www.eff.org/pages/when-government-comes-knocking-who-has-your-back

Implementing Privacy

- Different ways to ensure privacy:
  - laws
  - society/market
  - business
  - technology

Implementing Privacy

Law	Business
§ obligation	company policies
privacy by design	standard-setting best practice
Technology	Society

Impact of New Technologies

New Technologies

- New technologies often challenge individual privacy:
  - tracking
  - profiling
  - targeted advertising

Legislation (in part) to combat these challenges:
- DPD (1995)
- PECD (2002)
- DRD (2006)

Impact of Technology

The advancement of technology:
- More and more data is being produced about each individual
- The potential for abuse increases:
  - a higher amount of data = more actors involved
  - more people have access to "our data"
- This results in some legal challenges in regulating privacy

Legal Challenges

International nature of information
- Data may be located in different places:
  - originated
  - sent
  - stored
- Countries: different privacy laws → jurisdictional aspects important!

(Much the same as for cloud computing)

Specific Challenges

- Nature of consent e.g. cookies, location data
  - opt-in (active) / opt-out (passive)
  - most often opt-out (i.e. not privacy by default)
- Exceptions: where consent not required:
  - necessary to provide service requested by user
  - e.g. location data for value-added services but NOT where data anonymised
- Law is often slow to react to technological advances

Technology 2:

Mapping (Google Street View)

Google Street View

- Google Street view investigated in >20 countries
- Street level maps; data collection included unprotected wi-fi data

http://epic.org/privacy/streetview/
http://www.pcworld.com/article/254729/lies_spies_and_wi_fi_google_fesses_up.html

huge amount of personal data

Google Street View

http://www.pcworld.com/article/254729/lies_spies_and_wi_fi_google_fesses_up.html

What kind of "user traffic" did that Google spyware uncover? Oh, just names, phone numbers, mailing addresses, IP addresses, entire email messages, cookies, chat sessions, search terms, medical information, passwords, snippets of video and audio files, and log-ins to dating networks and porn sites.

- Issues: improper data collection, privacy invasion (people, homes, cars etc.)
- Table of investigations, by country (from November 2010): http://www.guardian.co.uk/technology/blog/2010/nov/12/google-street-view-privacy-worldwide

Google Street View: Your Views

Consider the benefits/risks of Google Street View from:

- Google's (company) perspective
- an individual's perspective
- society's perspective

Google Street View

- Google Street View's privacy policy: http://maps.google.com/help/maps/streetview/privacy.html
- Opt-out system
  - [you/your house/your car] may be filmed;
  - you may send a request to blur out [you/your house/your car]
  - Google will decide whether or not it blurs/deletes any data

Reliance on technology – automated systems for blurring faces, car registration plates etc.

Technology 3:

Tracking (RFID)

Tracking Technology: RFID

- RFID: radiofrequency identity
  - microchips that receive & transmit information through radio waves
  - data "read" or scanned

Focus: private sector
company → company (B2B)
company → individual (B2C)

RFID Uses

- Examples include:
  - inventory & stock control
  - transport cards
  - animal (people) tagging
  - storage of biometric data
  - means of payment

Increasing Usage of RFID

- Best practice: deactivate RFID tag at point of sale (clothes, household goods etc.)
  → not law!
- RFIDs provide a unique identifier (like barcode)
  - if not deactivated → disclose location

Reality – don't always know how technology is used, and whether we are being tracked…

Examples of RFID Usage

- Unintended uses:
  - Oyster Transport Card in London
  - easy & convenient card – works out how much you have to pay etc.
  - location data used by police to track individuals
- Companies prevent shoplifting
  - combine with e.g. CCTV footage

Do you agree with these usages of RFID?

RFID

- Increasing reliance on companies themselves to determine levels of privacy

→ Best practice
→ Industry standards

What are other companies doing?

Technology 4:

Surveillance by State

Tracking Technology: State Surveillance

- Use of new technologies:
  - CCTV
  - Passports (RFID chips / biometric data)
  - Telecommunications
  - Etc.

Focus: law enforcement, state security

Example: IRIS border control (UK)

- iris recognition immigration system (IRIS)
- UK airports, launched 2006
- fully automated arrivals barrier
- takes picture of passenger's irises & compares with those held on database
- approximately 400,000 users

- 2011 – to be phased out; no longer possible to register
  - cost over £9 million, technology unreliable
  - to be replaced by facial recognition & biometric passports

Example: SAS fingerprints (Sweden)

- fingerprint scanned when check baggage (instead of showing passport) & when board plane
- launched 2008, voluntary scheme
- biometric data deleted at end of flight
- security – match passenger with baggage

Potential Problems

- Often centralised databases → security issues
- Prevention, rather than detection, of crime
  - profiling of citizens
  - *Minority Report*
- Surveillance society:
  - interception of communications
  - disclosure of encryption keys
  - retention of communications data
  - state spyware
  - use of technologies for other purposes than original design – e.g. Oyster card

Technology 5:

The Internet of Things (smart objects)

Tracking Technology: Ubiquitous Computing

- … also ubiquitous tracking!
- Internet of Things
  - no longer need computer, mobile phone etc.
  - smart objects connect with each other
  - sensors e.g. parking, heat, "smart home"
  - "value-added services", consumer demand
- Popular technology
  - increasing demand
  - convenience

but what about privacy implications?

Smart Homes

- Company providing service
- Collection of personal data
  - access to data?
  - handout to 3rd parties?

http://readwrite.com/2013/03/18/smart-homes-our-next-digital-privacy-nightmare

"In reality, our smart devices hold more information than our brains," says Arabo. "This makes them a good target for hackers, malware and unauthorized users."

As is often the case with digital privacy issues, there's no clear legal precedent to draw from. Courts and legislative bodies tend to move considerably more slowly than the pace of technological innovation, so we end up with awkward grey areas like this.

Privacy v. New Technologies

Can they work together?

If so, how?

Things to consider…

Privacy of users
New technologies
Personal data
Anonymisation of data
Consent
Convenience
Business models
Security

Huge amount of personal data

- Security issues
  - data leakage etc.
- Some data irreplaceable if lost/misused!
  - biometrics
- Reputation is hard to regain if lost

New technologies should be encouraged
BUT only if understood…

Potential Solutions

Privacy through Technology

- Privacy by design: privacy is the default
- Built into the system from the beginning
- Technology as the solution

May be good solution for a company – name & reputation!

Privacy by Design?

- One solution: privacy-enhancing technologies (PETs)
- Build privacy into a system at time of creation
- These can e.g.:
  - block / delete cookies;
  - block RFID readers / deactivate RFID chips;
  - disable targeted advertisements.

Regulation by technology

PIA

- Privacy Impact Assessment
  - evaluate the potential effects on privacy of x and find ways to mitigate or avoid any adverse effects
- Proactive approach – consider privacy first
- E.g. EU proposal – RFID use

Regulation by society → industry standard

Implementing Privacy

Law § obligation privacy other laws	Business company policies reputation transparency
privacy by design PETs Technology	standard-setting best practice technology-specific rules PIA Society

How to ensure privacy?

Be familiar with and follow applicable laws!

Consider how a particular company can best ensure privacy:

- company policies (business)
- best practice (society)
- privacy by design (technology)

Privacy Checklist

- ✓ What are the applicable privacy regulations (may be more than one area)?
- ✓ Is there a legitimate reason for processing personal data?
- ✓ Is collected data still required? Should it be deleted?
- ✓ Is the data personal or sensitive?
- ✓ What kind of processing is being used?
- ✓ What is the purpose of having the data?
- ✓ Where is the data originating/communicated/ stored?

Privacy Checklist

- ✓ Is there transfer of data to a third country (outside the EU)?
- ✓ What data may be kept by other bodies?
- ✓ What policies exist within the company?
- ✓ What other rules/regulations exist regarding company data?
- ✓ What is best practice within the industry?
- ✓ What kind of reputation does the company wish to have?

Thank you for your attention!

Questions?