Privacy vs. Data: Business Models in the digital, mobile Economy

Lecture 12
Trade off between Privacy and Service Value

SS 2016

Dr. Andreas Albers

Agenda

- Trade-off between Personal Data and Value Proposition
- Perceivable Benefits of Personal Data Disclosure
- Issues originating from Lack of Personal Data
- Privacy Issues / Challenges of Privacy Protection
- Privacy as Competitive Edge
- Business Cases driven by Privacy as USP

Privacy vs. Value Proposition by Online Businesses

Personal Data is essential in an Attention Economy

Privacy is essential right of every individual

Online Service offerings and privacy are always a trade-off

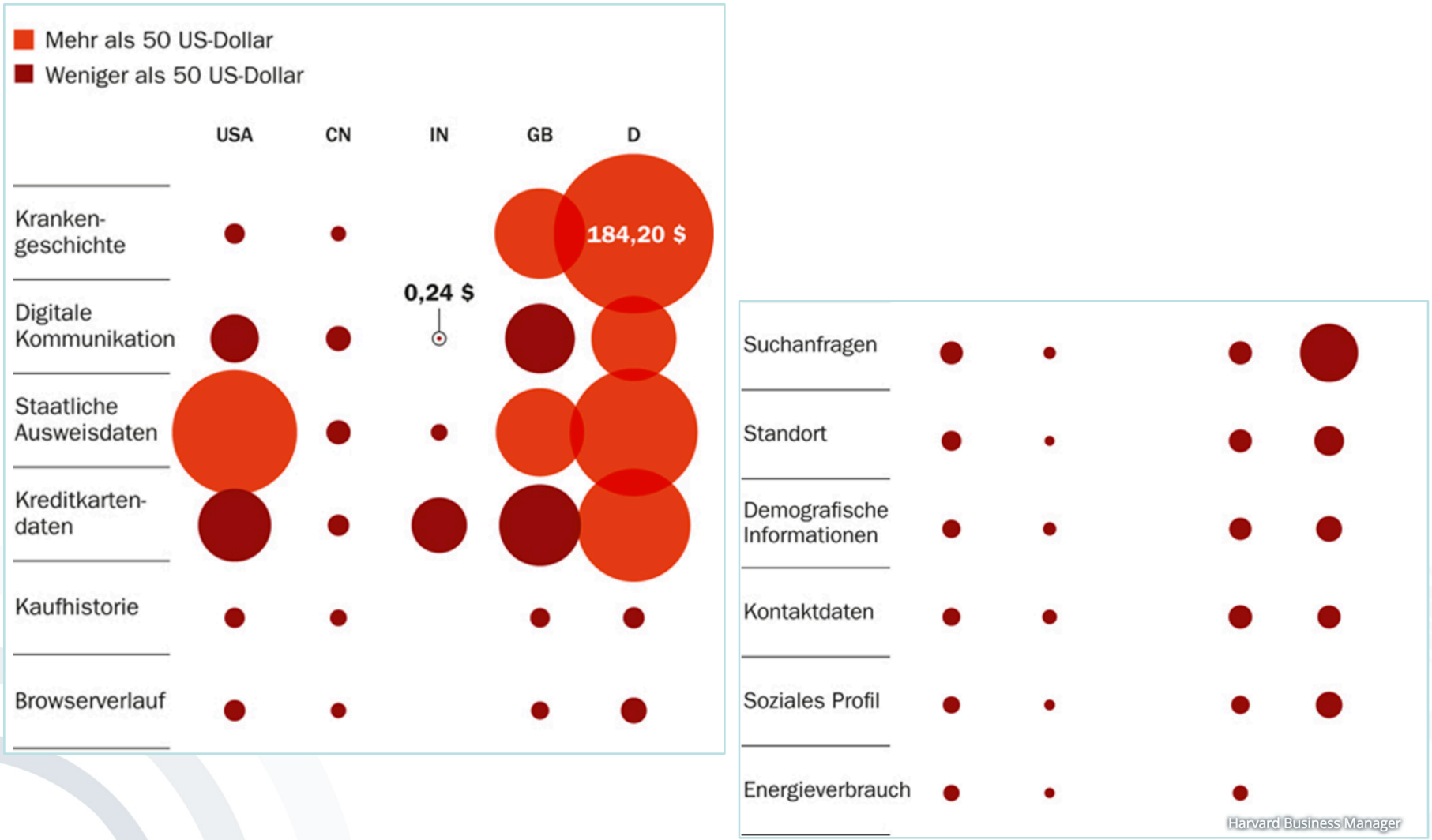
- With digital businesses trying to collect all the personal data that is available
  - this trade-off is currently to the disadvantage of individuals
  - Privacy protection (research) is needed more than ever

Privacy vs. Value Proposition by Digital Businesses

- Most Digital Businesses take advantage of (as much as possible) personal data about users in order to …
  - offer targeted advertisements
  - enable service personalisation
  - improve services and products
  - tighten service security
  - differentiate from competition
  - conduct market research
  - …

- Users want to disclose as little as possible personal data to Digital Businesses in order to protect their privacy and prevent possible …
  - unfair price discrimination
  - unintended/unfair reviews (e.g. credit worthiness / health) reports
  - spamming or fraud
  - sales of contact information to Third Parties
  - Cyber-Stalking
  - unintended linking of social roles
  - black mailing
  - …

The Monetary Value of Personal Data



Source: http://www.harvardbusinessmanager.de/blogs/was-sind-ihnen-ihre-daten-wert-a-1061019.html

Agenda

- Trade-off between Personal Data and Value Proposition
- Perceivable Benefits of Personal Data Disclosure
- Issues originating from Lack of Personal Data
- Privacy Issues / Challenges of Privacy Protection
- Privacy as Competitive Edge
- Business Cases driven by Privacy as USP

“Highly” Perceivable Benefits of Personal Data Disclosure

- Location-based Services (Exit App)

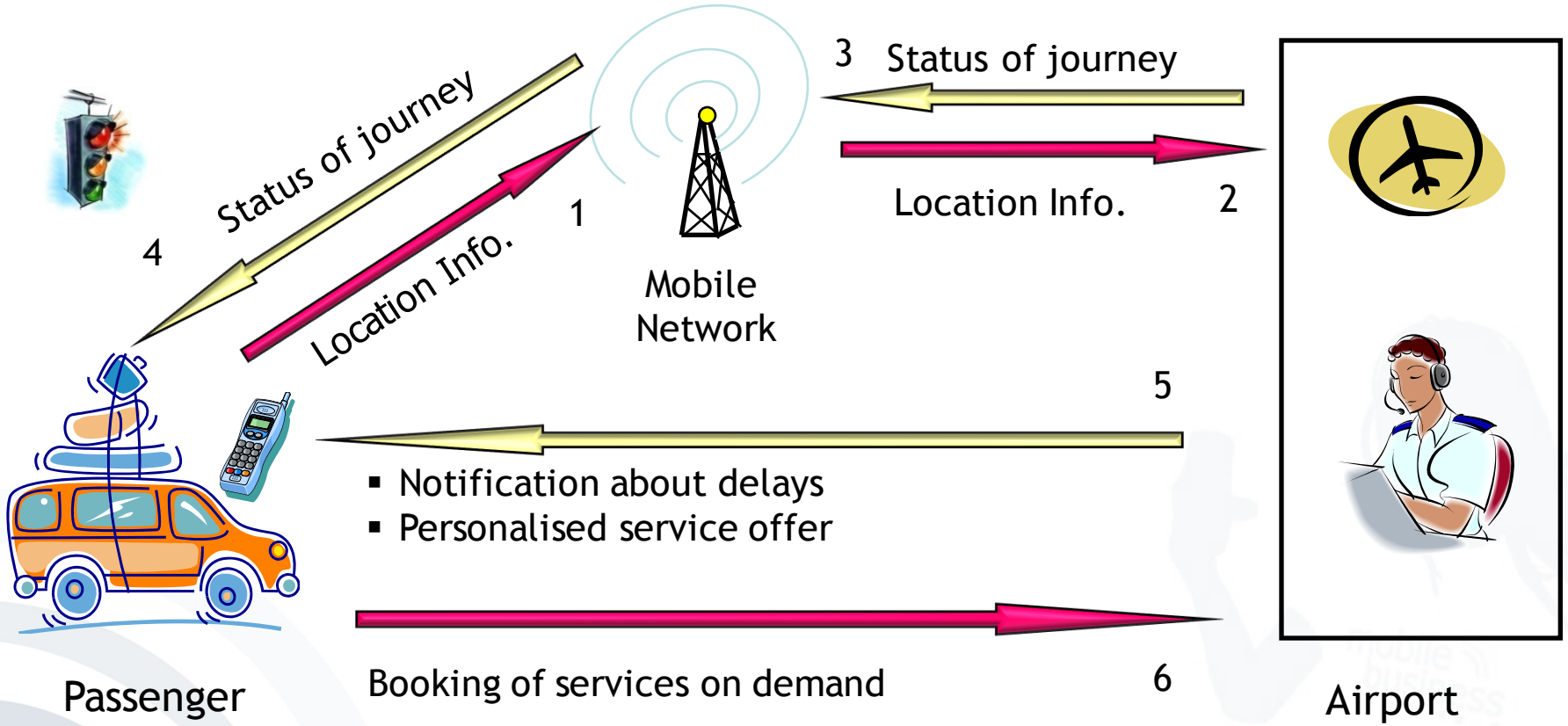
Source: Apple iTunes, 2012

Possible Future Information System Case: Travelling Assistance for Frequent Flyers

Mobile Customer Relationship Management System

- Passengers get assistance during their journey (e.g. by car) to the airport from their airline.
- If delays for the journey are detected (e.g. caused by traffic jam), the passengers are contacted by the airline.
- The passengers will be offered personalised services via their mobile device. (e.g. parking service at the airport)
- Depending on the delay, these services can reduce the risk of passengers actually missing their flight.

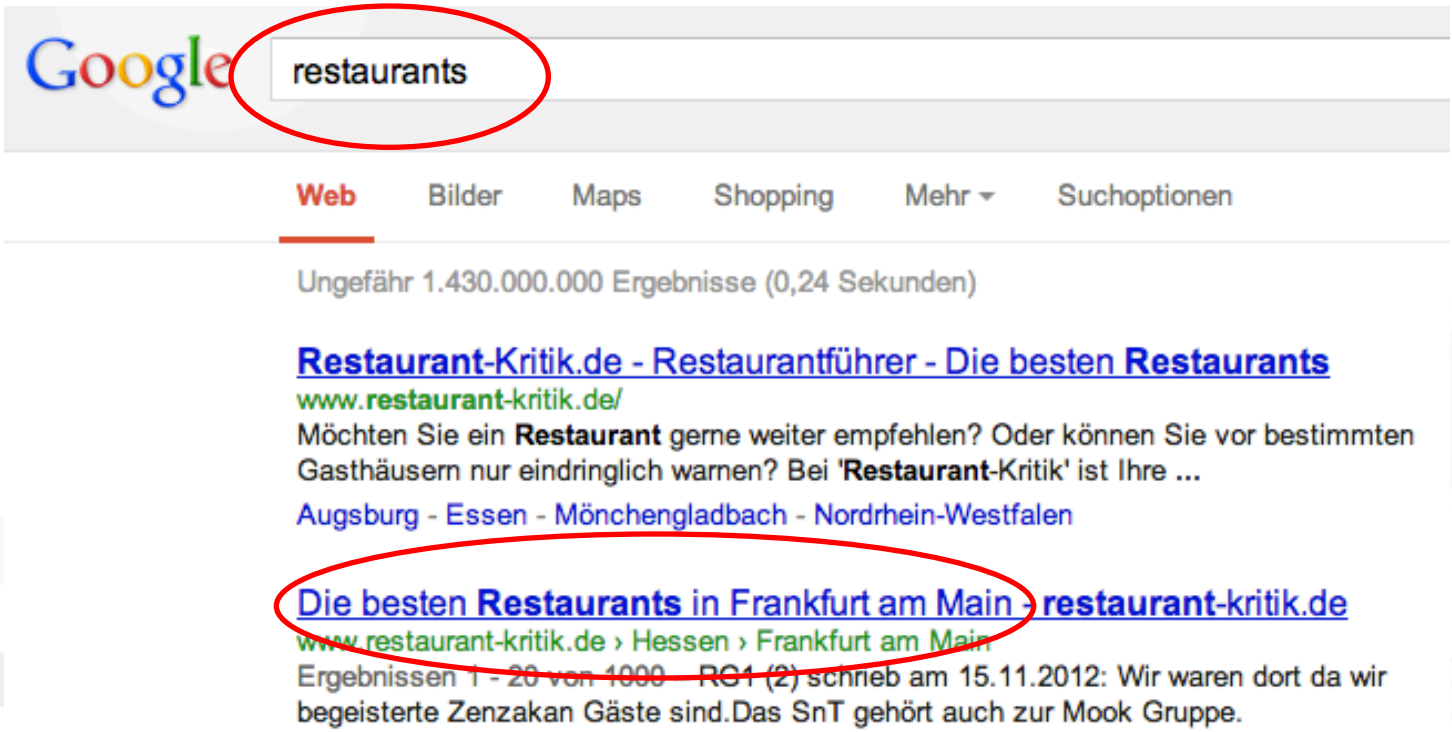
Travelling Assistance for Frequent Flyers: Support during Journey to the Airport



The airline monitors the location of the passenger's mobile device and thereby calculates their ETA.

“Somehow” Perceivable Benefits of Personal Data Disclosure

- Local Search

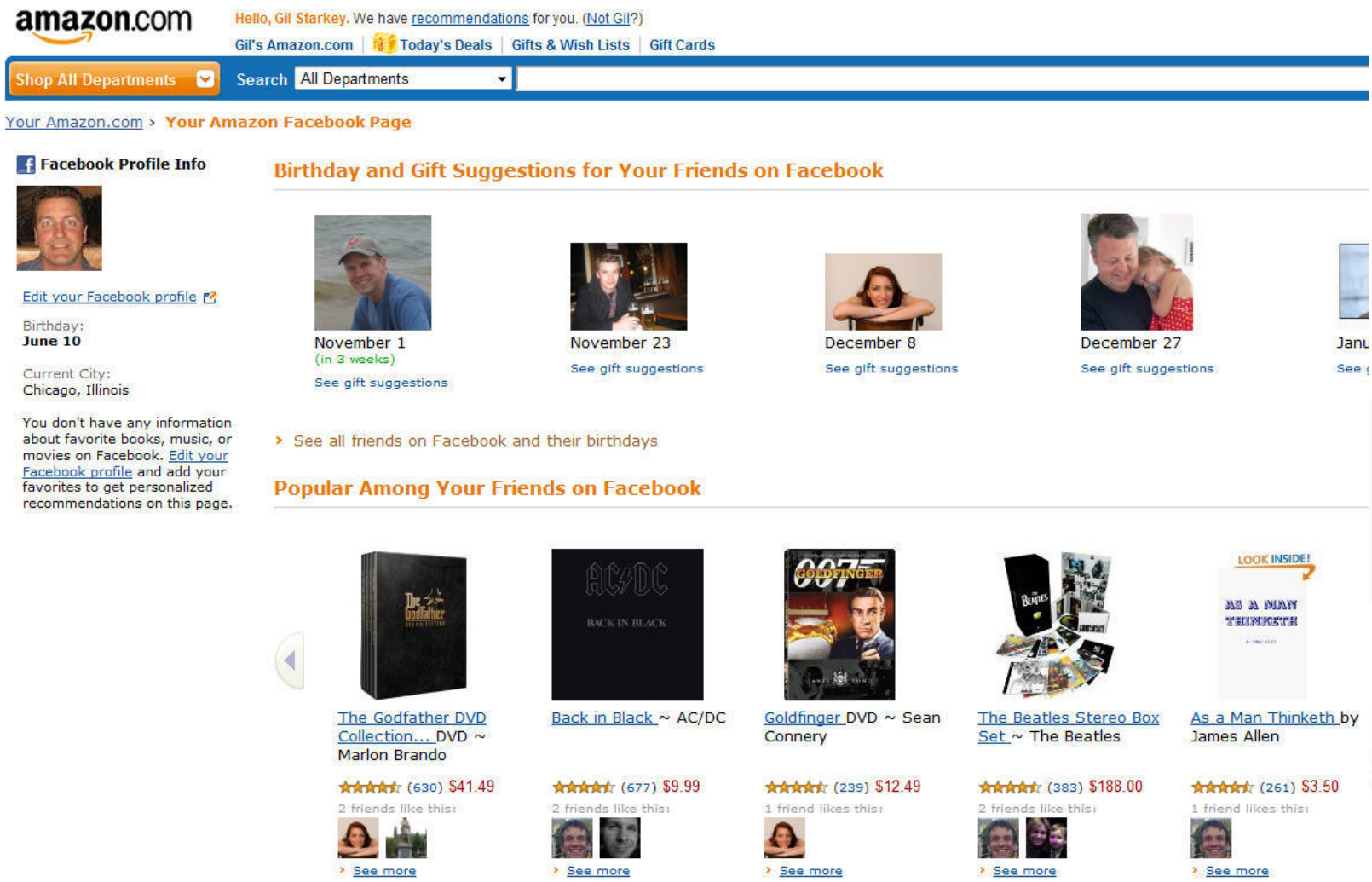


“Hardly” Perceivable Benefits of Personal Data Disclosure

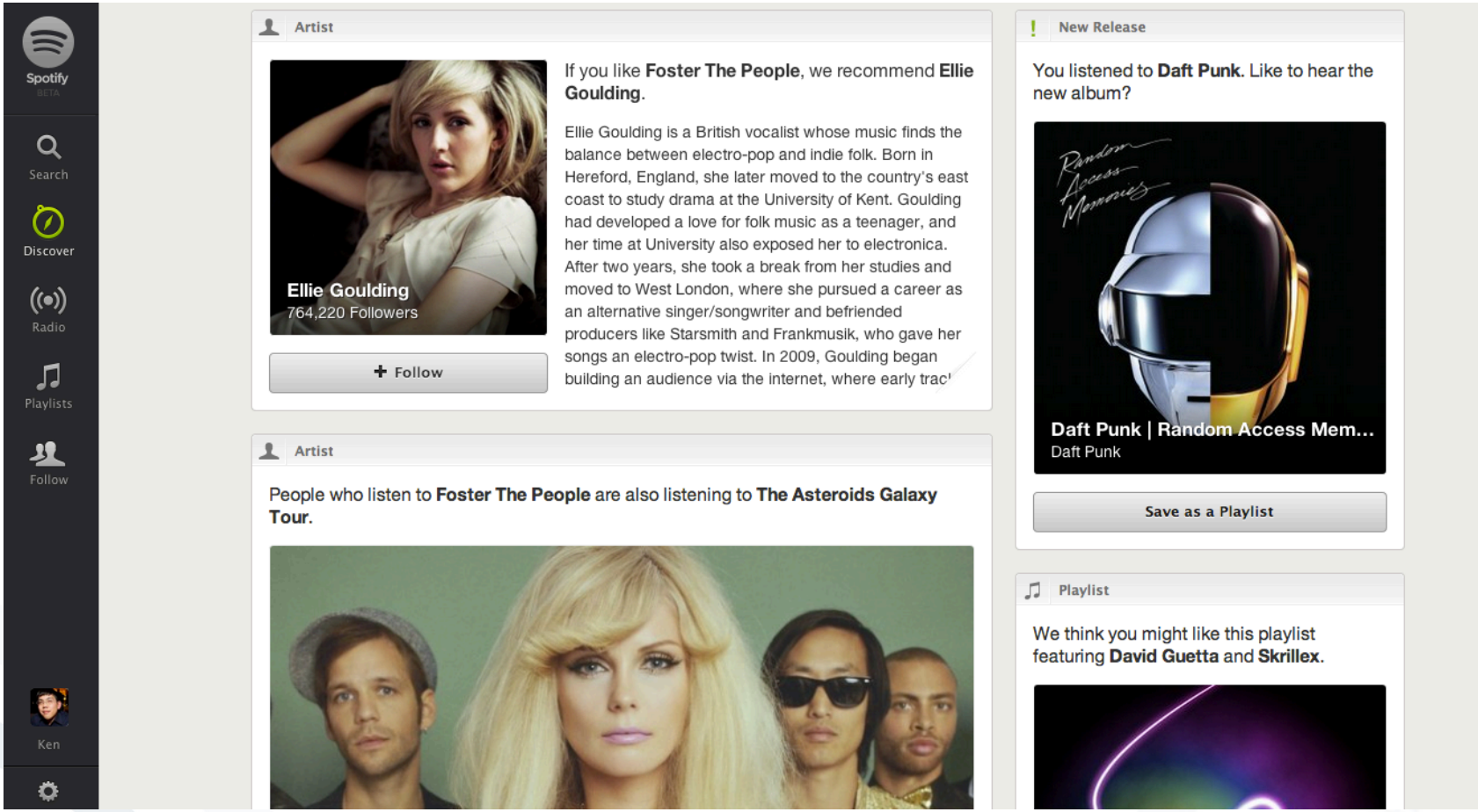
- Google Suggest & Spelling Correction

Facebook Newsfeed Personalisation

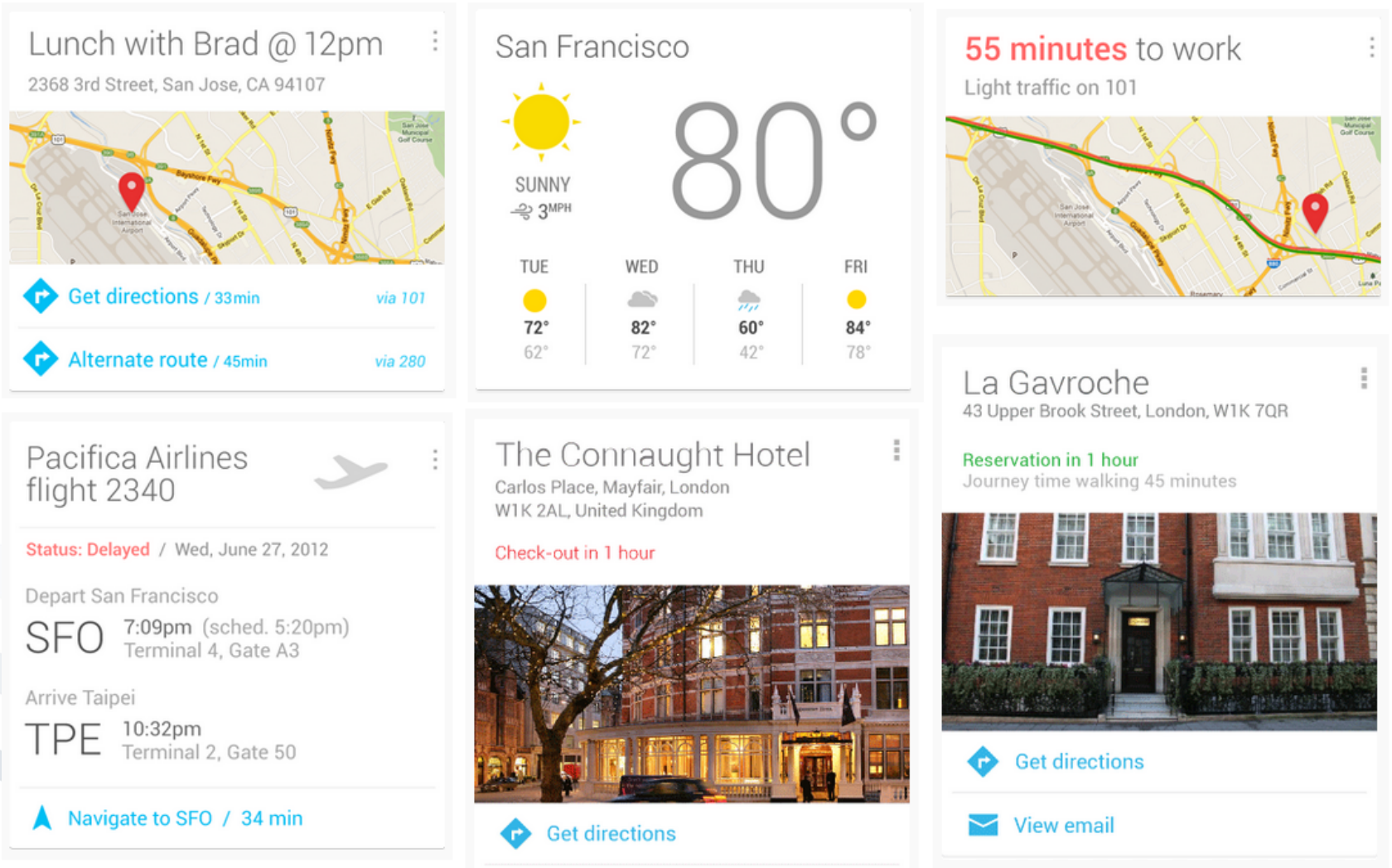
Amazon Recommendations based on Facebook



Spotify Recommendations



Google Now Predictions



Digital businesses better addressing User Needs/Demand

- Improving Web/Mobile UIs through user tracking
- Predicting demand for products/services based on tracking users on a website
- Predicting the spreading of diseases based on search queries
- Improving products/services based online/mobile user feedback/reactions
- …

Agenda

- Trade-off between Personal Data and Value Proposition
- Perceivable Benefits of Personal Data Disclosure
- Issues originating from Lack of Personal Data
- Privacy Issues / Challenges of Privacy Protection
- Privacy as Competitive Edge
- Business Cases driven by Privacy as USP

Targeted Advertising needs Personal Data

- Personal data allows to target online advertisements to the personal needs an individual in his current usage situation

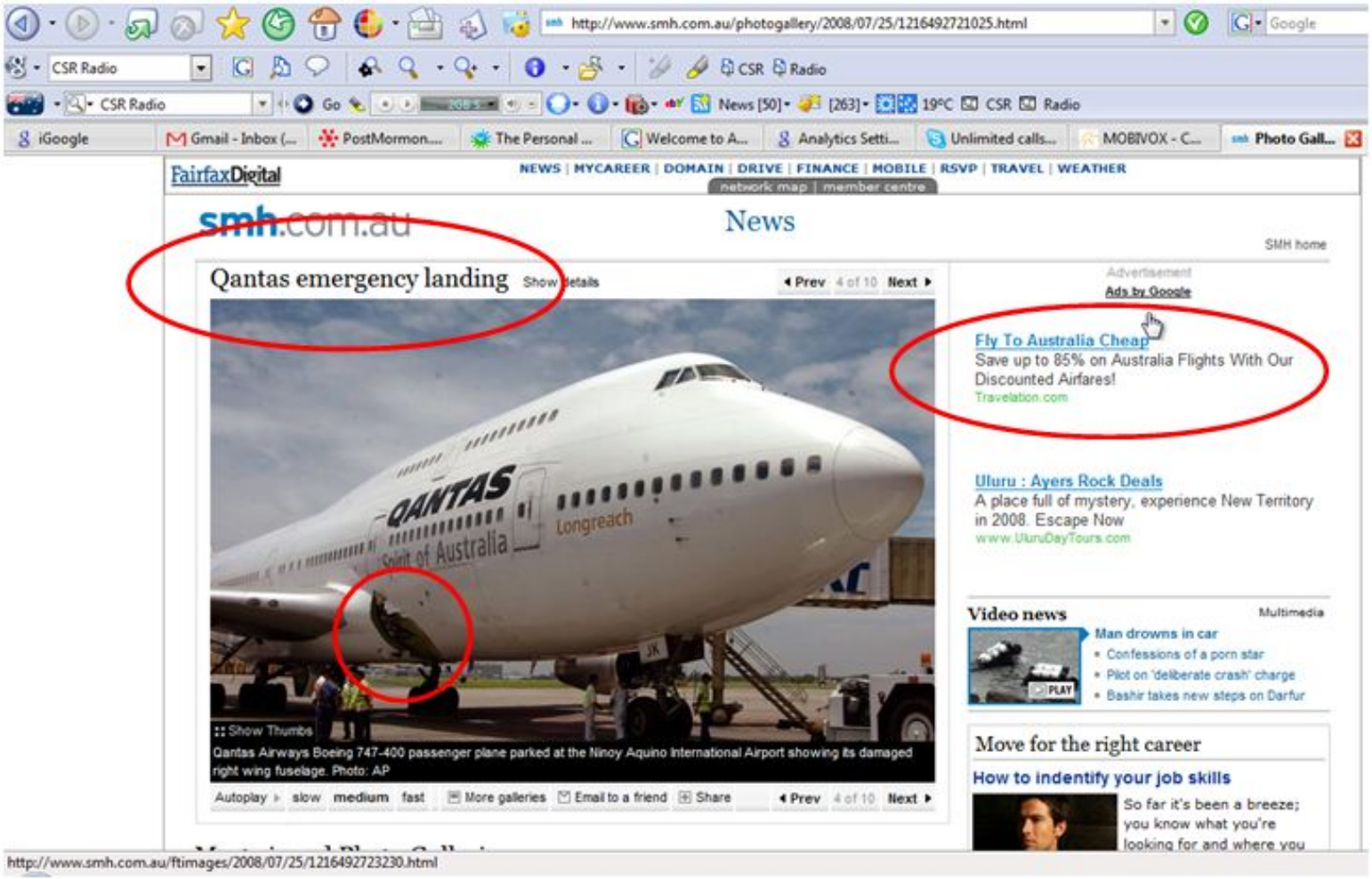
- In exchange, individuals benefit from free or subsidized online services or content as well as relevant ads

- **Problem 1:** Individuals often do not consider a free services or content as "payment" for their personal data and attention. This mental link is missing.

- **Problem 2:** Ad relevance is often not perceived as a benefit by individuals. Only if the ads are NOT relevant at all individuals may feel disturbed …

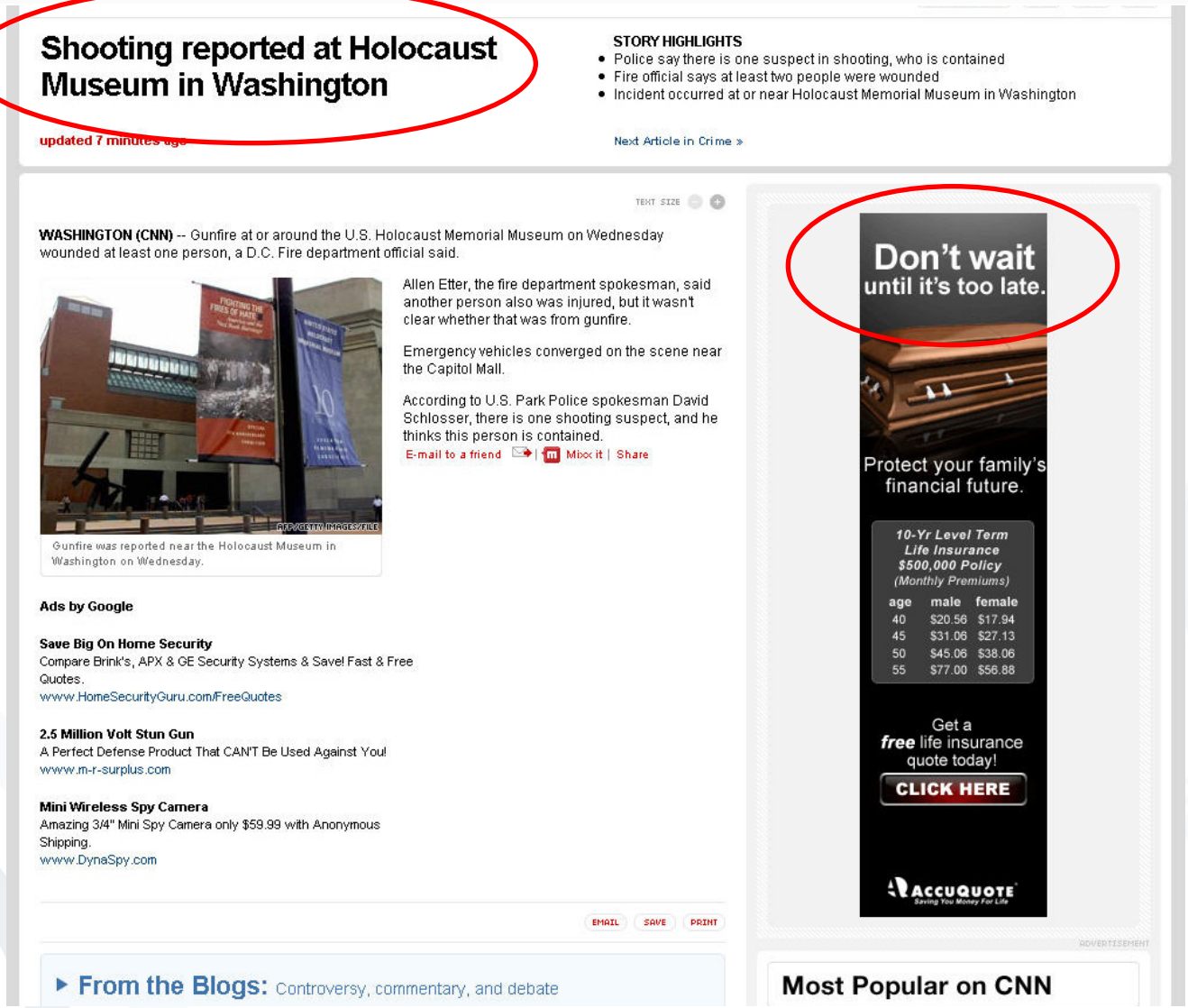
When Ads fail …

Targeted Ads gone wrong



http://propr.ca/wp-content/uploads/2009/01/qantas-090120.jpg

Targeted Ads gone wrong (2)



Shooting reported at Holocaust Museum in Washington

updated 7 minutes ago

STORY HIGHLIGHTS
- Police say there is one suspect in shooting, who is contained
- Fire official says at least two people were wounded
- Incident occurred at or near Holocaust Memorial Museum in Washington

Next Article in Crime »

TEXT SIZE

WASHINGTON (CNN) -- Gunfire at or around the U.S. Holocaust Memorial Museum on Wednesday wounded at least one person, a D.C. Fire department official said.

Gunfire was reported near the Holocaust Museum in Washington on Wednesday.

Allen Etter, the fire department spokesman, said another person also was injured, but it wasn't clear whether that was from gunfire.

Emergency vehicles converged on the scene near the Capitol Mall.

According to U.S. Park Police spokesman David Schlosser, there is one shooting suspect, and he thinks this person is contained.

E-mail to a friend | Mixx it | Share

Ads by Google

Save Big On Home Security
Compare Brink's, APX & GE Security Systems & Save! Fast & Free Quotes.
www.HomeSecurityGuru.com/FreeQuotes

2.5 Million Volt Stun Gun
A Perfect Defense Product That CAN'T Be Used Against You!
www.m-r-surplus.com

Mini Wireless Spy Camera
Amazing 3/4" Mini Spy Camera only $59.99 with Anonymous Shipping.
www.DynaSpy.com

EMAIL SAVE PRINT

▸ **From the Blogs:** Controversy, commentary, and debate

ADVERTISEMENT

Most Popular on CNN

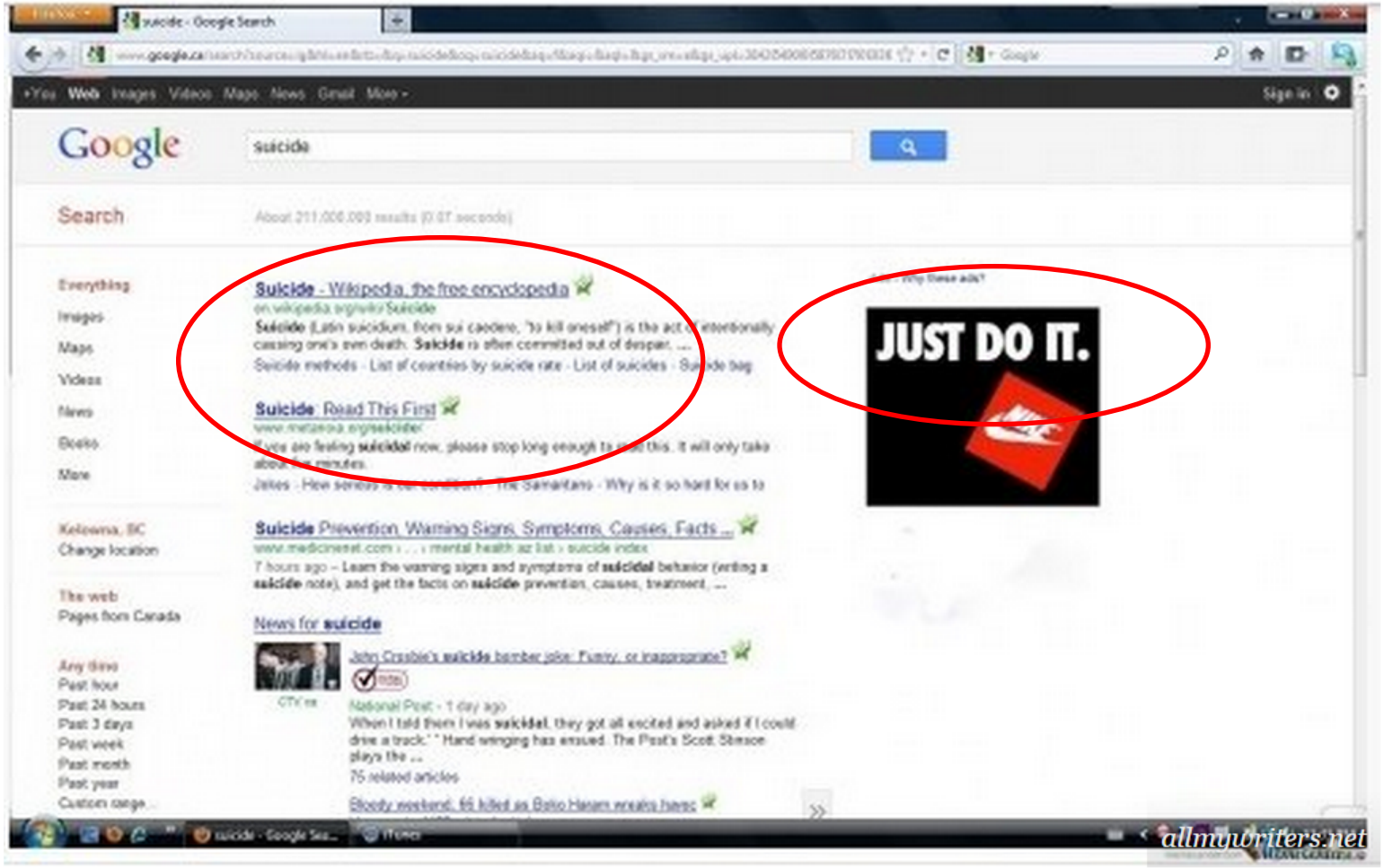
http://www.divinecaroline.com/

Targeted Ads gone wrong (3)

http://purethinking.typepad.com/pure_thinking_a_streamofc/2009/08/targeted-ads-gone-bad.html

Targeted Ads gone wrong (4)

Targeted Ads gone wrong (5)



And one more – Targeted Ads gone wrong (6)

http://www.chicagotribune.com/news/nationworld/chi-0504250109apr25,1,4214950.story?coll=chi-newsnatio

ACROSS THE NATION

Skydiver dies after legs severed in midair

Items compiled from Tribune news services
Published April 25, 2005

DeLAND, FLORIDA -- A skydiving cinematographer was killed after his legs were severed in a midair collision with the airplane he had jumped from, authorities said.

Albert "Gus" Wing III, 50, had deployed his parachute Saturday when he struck the left wing of the DHC-6 Twin Otter propeller plane at about 600 feet, a witness on the ground told police.

Both of Wing's legs were severed at the knees.

He was airlifted to a hospital, where he died, DeLand Police Cmdr. Randel Henderson said.

chicagotribune

Impacts of Less Personal Data on Advertising Business (due to regulation)

- Study on how privacy regulation might impact economic activity on the advertising-supported Internet:
  - Avi Goldfarb, Catherine E. Tucker (2011) Online Advertising, Behavioral Targeting, and Privacy, Communication of the ACM (54:5), New York, USA.
- Comparison of Online Advertising effectiveness on websites within the EU (under EU regulation) and outside the EU.
- Due to EU regulations, advertising networks are no longer allowed to collect and link certain information about online user behaviour.
- As a result, advertising effectiveness dropped by up to 66% on European websites.

Impacts of Less Personal Data on Advertising Business (due to regulation)

- Each advertiser is affected differently by the same regulation
- Advertisements on websites with a high diversity of content (e.g. news portals) are more affected by dropping advertising effectiveness than highly specialised websites (e.g. travelling portal), which focus only on a few topics.
- Why?

Impacts of Lack of Personal Data on Advertising Business (due to Default Tracking Protections)

- Theoretical issues of switching on Tracking Protection by Default
  - Online/mobile advertising businesses lose their data for targeting advertisements
  - Advertisers have to cope with incomplete, varying data which makes targeting more difficult
  - Increasing use of content-based targeting with lower targeting efficiency

- Possible consequences
  - Lower number of ad-financed online/mobile services
  - Users have to pay for digital services (“Bezahlschranke”)
  - Lower offered service quality
  - Unavailability of certain services

Agenda

- Trade-off between Personal Data and Value Proposition
- Perceivable Benefits of Personal Data Disclosure
- Issues originating from Lack of Personal Data
- Privacy Issues / Challenges of Privacy Protection
- Privacy as Competitive Edge
- Business Cases driven by Privacy as USP

Possible Consequences of Privacy Violations

- If users no longer feel in control of their personal data, they could …
  - … stop trusting online services and refrain from using them
  - … give up caring about their privacy and security because they feel helpless
  - … no longer behave in a natural way because they may feel "under surveillance"
  - …
- Consequently, this would affect negatively affect the digital economy as well as the society as a whole

Current Approaches for Privacy Protection

Personal data of users „can“ be protected by

- Regulation / Data Protection Law
- Technical Data Protection
- Privacy by Design

But what are the challenges / outcomes of these approaches for users and digital businesses?

Apropos, what is the role of *trust* by users in this context?

Issues of Regulating the Collection of Personal Data for Advertisers

- Regulation provides only a very basic protection because it needs to address the demands of as many as possible organisations within EU.
- Regulation is often unclear or interpreted in many different ways by authorities.
- Regulation has to be enforced, which is often slow or even sometimes too late.

Problems with Self-Regulation on Personal Data Collection

- Self-Regulation of an industry is better than regulation by law
- Self-Regulation is often difficult to audit and not transparent enough
- Self-Regulation as means to avoid regulation by law?

Conclusion on Regulation on Personal Data Collection

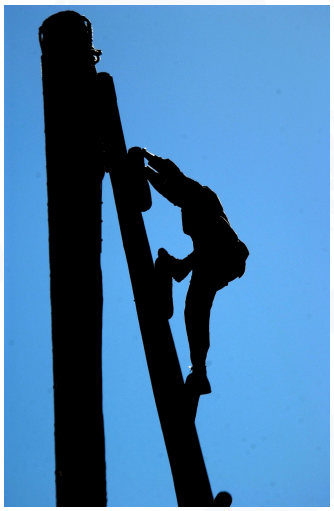
- Indicators that regulation affects Online business or at least the advertising industry exist
- Regulation has many issues, but regulation is necessary and also beneficial as it
  - provides enforceable basic data protection framework
  - provides data processing guidelines for organisations
  - generates awareness in the population about data protection

Issues with Technical Data Protection Means for Individuals

- Individuals have to be ***aware*** about privacy threats. However,
  - this often requires technical understanding
  - data flows exchanged with online services are often not transparent to a user
  - data flows transparent to users are often too complex for them to understand (e.g. logs files)

Issues with Technical Data Protection Means for Individuals

- Protection of personal data by individuals always **takes effort**, e.g.
  - installing and understanding technical solutions (e.g. browser plug-ins)
  - accepting lower service quality due to lack of data because of technical solutions (e.g. slow webpage loading time because used proxy servers)
  - maintaining privacy settings for online/mobile services
  - because data protection can currently not be centrally managed (availability of multiple devices, services, data flows which have to be managed)
  - consciously limiting data disclosure or service usage



Issues with Technical Data Protection Means for Individuals

- In order for individuals to take up this effort, they need to receive **directly perceivable benefits or incentives** in exchange, e.g.
  - Protection from possible data disclosure consequences
    - Disclosure of embarrassing pictures on social networks
  - Protection from manipulation of behaviour, e.g.
    - getting lured into buying certain products
    - influencing one's opinion on something

Issues with Privacy Settings on Social Network Sites

- Privacy settings of Social Network sites are often very complicated and hard to find.
- Users mostly stick with the default privacy settings. Thereby, users often simply do not post certain things instead of restricting their disclosure via configuration of privacy settings.
- Social Network sites often lack of real-time feedback for applied privacy protection settings.
- Note: Privacy settings do not apply for social network site providers, they have in general access to all posted personal data anyway.

Excursion: The Power of Default Settings

- Default settings hardly get changed by users. Therefore these settings are very powerful mechanism for those controlling the default settings.

- Examples: Consequences of
  - turning on tracking protection lists for the Internet Explorer by *default*?
  - Facebook changing of *default* privacy settings (http://mattmckeon.com/facebook-privacy)?

Technical Issues of Tracking Protection Means

- Web Tracking Protection is technically easy
  - Internet Explorer has build-in Tracking Protection
  - Tracking Protection is available via Browser Plug-Ins
  - Some browsers support the DoNotTrack flag

- ... but who is going to maintain the tracking protection lists used to block the trackers?

- In addition, Tracking Protection …
  - … does not really work on mobile devices for web apps
  - … mobile browsers typically don't support plug-ins
  - … mobile apps are more relevant than browser apps
    - Mobile apps have trackers directly integrated

Conclusion on Technical Data Protection

- Technical Data Protection takes effort and requires knowledge without users being able to perceive direct benefits

- **Missing mental link for users** between privacy protection and the availability of free services
  - For instance, a user blocking the tracking of his web online behaviour does not experience any direct disadvantages with regard to free services.

- **Mental link does exist** for privacy protection against other users of a Social Networking site,
  - For instance, a user posts a picture which was intended only for a limited audience but was leaked due to sloppy privacy settings.
  - But this constitutes only data protection towards other users and NOT towards the service provider as well.

Privacy by Design

- Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Ann Cavoukian,
Information & Privacy Commissioner Ontario, Canada

Privacy by (Re)design Principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

Ann Cavoukian,
Information & Privacy Commissioner Ontario, Canada

Conclusion on / Issues of Privacy by Design

- No incentives for online business to do Privacy by Design
  - Users are not demanding it
  - No competitive advantage for businesses
  - Regulatory does not directly demand it, yet
- Open Question: Which personal data is exactly required to run a service such as Google Search or Facebook?
- There is so far no real best practice/approach to develop online services based on Privacy by Design principles

Agenda

- Trade-off between Personal Data and Value Proposition
- Perceivable Benefits of Personal Data Disclosure
- Issues originating from Lack of Personal Data
- Privacy Issues / Challenges of Privacy Protection
- Privacy as Competitive Edge
- Business Cases driven by Privacy as USP

Privacy (Protection) Challenge

- Users demand privacy but the effort to protect this privacy is often to high.
  - How to reduce/minimize this effort?

- Digital Businesses have no actual incentive to protect the privacy of their users.
  - How to motivate them to do so?

User gives up Privacy very easily
Privacy Paradox and Privacy Calculus Examples

When disclosing personal data offers direct benefits or privacy protection takes to much effort, users give up on privacy very easily:

- Microsoft Study: Users willing to receive Targeted Ads (80%), to be tracked (30%)
- Privacy-aware users preferring Google Service Engine over privacy-friendly Search Engine **IxQuick** (ULD certified)
- Continuous media coverage of privacy issues of smart phones (e.g. leaked location data, usage tracking, cloud sync, forced user authentication or registration, etc.), but still increasing sales
- Privacy issues in mobile apps (e.g. WhatsApp is one of the most popular mobile messenger apps – but at the same the most unsecure and privacy invasive). Who cares?

Privacy Protection in Practice – What currently works (beyond regulation)

- Provider-driven
  - Apple
    - Tracking Protection in Safari, Device ID Prevention, One-Stop Tracking OO
  - Microsoft
    - DNT by Default in IE10, Tracking Protection Lists

- User-driven
  - Facebook Privacy Scanner (Transparency)
  - Ghostery (Transparency)
  - AdBlock Plus (Privacy-Enhancing)
  - Bitcoins (Privacy-Enhancing)

- Why does it work?

Digital Business and Privacy Protection (exaggerated picture)

- So far, offering privacy-friendly services does not constitute a competitive edge for Online Businesses
  - Selectively collecting personal data from users generates additional effort/costs
  - Privacy Protection leads to less personal data
  - Privacy Protection generates additional efforts for users
  - …
- Consequently, for Online Businesses *privacy protection* often equals *costs*
- From an economic perspective *costs* have to be minimized
- Minimizing *costs* equals minimizing *privacy protection*
- Minimum *privacy protection* equals *regulative requirements*

Towards Privacy as Competitive Edge for Online Businesses

- Competition on Privacy
  - does most likely not generate any additional revenues
  - but can drive Online Businesses to continuously offer and excel on privacy protection (beyond regulation)
- Approach
  - Minimize user effort through Identity Management at the heart of business models
  - Enabling Online Businesses
    - to offer perceivable privacy
    - Handle less personal data (if necessary)
- Why are some digital businesses (e.g. Apple) seem to protect the privacy of their users while others don't?

Use Case: Ad-Financed Online Editorial Content (e.g. SPON, FTD)

- Media industry on the verge of a radical change? Has ad-financing a future?
  - Ad-financing often allows not to produce high quality content
  - Ad-Blocker beginning to become main stream
  - No willingness to pay for trivial content (e.g. weather)
  - High quality content increasingly behind paywalls
  - Competition by non-media enterprises (e.g. individuals via blogs, youtube.com, etc.)
  - Increasing number of channels to consumers (e.g. mobile vs. fixed) may require different content formats (making reuse harder)
  - …

Agenda

- Trade-off between Personal Data and Value Proposition
- Perceivable Benefits of Personal Data Disclosure
- Issues originating from Lack of Personal Data
- Privacy Issues / Challenges of Privacy Protection
- Privacy as Competitive Edge
- Business Cases driven by Privacy as USP

Anonymous Payments via Bitcoin

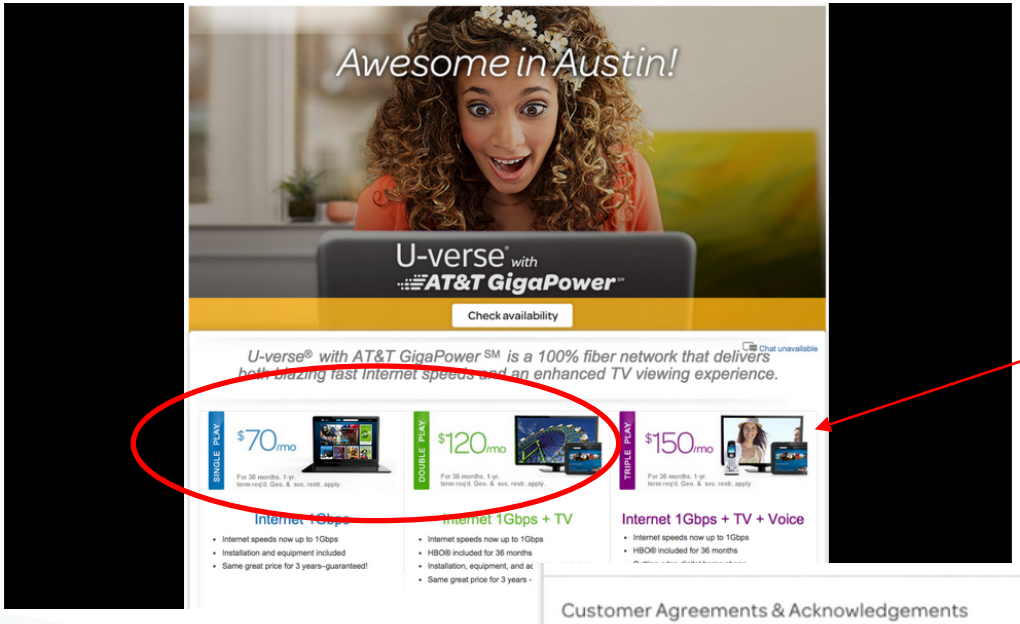
- Peer-to-Peer Payment System
  - Based on digital/virtual „crypto-currency“
  - All transactions are stored in public, decentralised database
  - No regulating/controlling authority
  - Users/transactions can only be identified by their unique addresses
  - For privacy, addresses should be renewed for each transaction

Browser „AdBlock“ Business Model

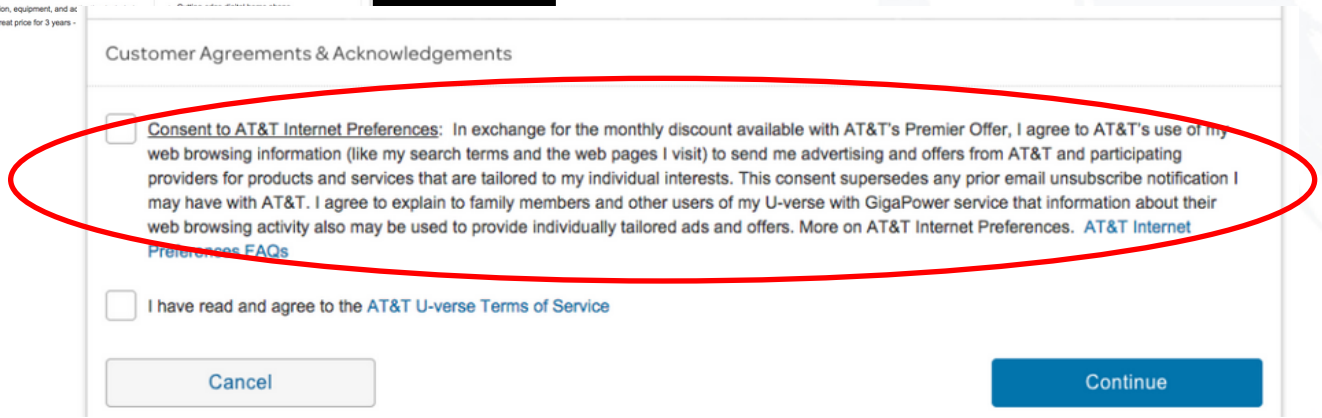
- AdBlock Plus
  - Offers browser add-on that blocks Web advertisements.
  - Free for users, highly effective

- *Controversial* two-sided Business Model
  - **Internet User:** Free browser add-on that blocks Web advertisements
  - **Ad Industry:** Has to pay to get their ads on the AdBlock Plus exception/white list

AT&T offers its customers to buy their Privacy (at a premium)



Privacy incl. in Service …



TelekomCLOUD

Cloud Services hosted in Germany under German data protection law

cloud.telekom.de

Apple Corp.

Apple's commitment to your privacy

[...] *„Our business model is very straightforward: We sell great products. We don't build a profile based on your email content or web browsing habits to sell to advertisers. We don't "monetize" the information you store on your iPhone or in iCloud. And we don't read your email or your messages to get information to market to you. Our software and services are designed to make our devices better. Plain and simple."* [...]

Source: http://www.apple.com/privacy/

Further Readings

Big Data vs. Privacy

- http://www.golem.de/news/alexander-dobrindt-grundsatz-der-datensparsamkeit-muss-weg-1511-117536.html
- http://www.heise.de/newsticker/meldung/Merkel-auf-dem-IT-Gipfel-Datenschutz-darf-Big-Data-nicht-verhindern-2980126.html
- http://www.computerwoche.de/a/analytics-und-big-data-software-der-markt-ist-reifer-geworden,3220141
- http://www.golem.de/news/neue-geschaeftsbedingungen-snapchat-moechte-bilder-veroeffentlichen-und-verkaufen-1511-117232.html

Future of Online/Mobile Marketing

- http://onlinemarketing.de/news/10-thesen-zukunft-online-marketing
- https://netzoekonom.de/2013/12/01/online-gesucht-offline-gekauft-wie-google-die-verbindung-herstellt/
- http://m.faz.net/aktuell/wissen/mensch-gene/online-reklame-wenn-werbung-nicht-mehr-wirkt-13850094.html
- http://www.technologyreview.com/review/544371/the-end-of-internet-advertising-as-weve-known-it/
- http://onlinemarketing.de/news/50-prozent-vorhersagbarkeit-online-shop-technologie

Last access: April 2016