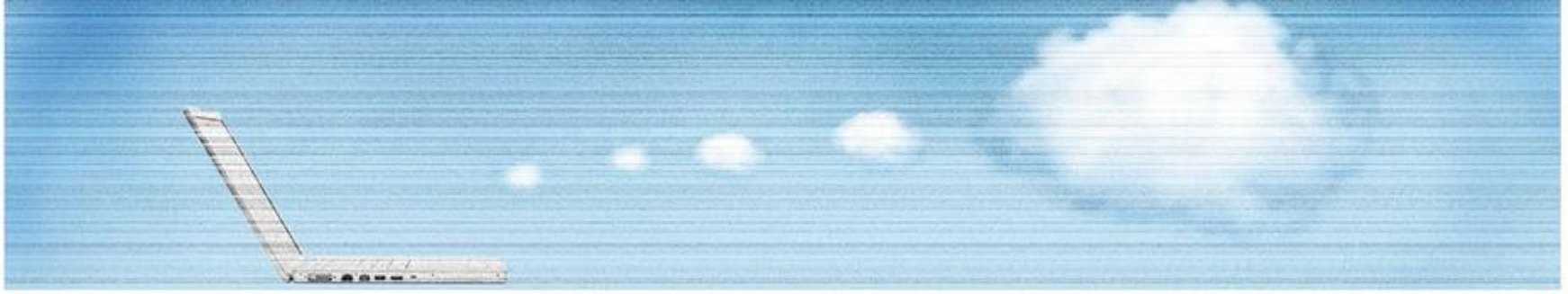


UiO : Department of Media and Communication
University of Oslo

The End of Privacy? New research apps, new research ethics

Dr. Charles Ess
<c.m.ess@media.uio.no>

NordMedia'13

9. August 2013

Overview

1. Device Analyzer: what it collects – and what its acceptance suggests regarding changing conceptions of "privacy"

2. Internet Studies: from *individual* "privacy" to *relational* "privacies"

3. Nissenbaum: privacy as contextual integrity

4. The shift towards relational privacies and research ethics guidelines: *privatlivet*, the *intimsfære*, and the NESH (2006) guidelines

5. Concluding remarks: more apps, new research ethics?

1. Device Analyzer: what it collects – and what its acceptance suggests regarding changing conceptions of "privacy"

In the electric age, we wear all mankind as our skin.

M. McLuhan, *Understanding Media: The Extensions of Man*

Initial reflection exercise:

would you install "Device Analyzer"

on your mobile device?

(C. Ess and H. Fossheim. 2013.

Personal Data: Changing Selves, Changing Privacies. In M. Hildebrandt, K. O'Hara, & M. Waidner, eds. *Digital Enlightenment Forum Yearbook, The Value of Personal Data.*

recent apps for smartphones allow researchers into "private" / *privatlivet* domains previously inaccessible, e.g.

"Device Analyzer"

Device Analyzer

UNIVERSITY OF CAMBRIDGE

Get statistics about your phone use and contribute to scientific research!
Device Analyzer works on Android devices running Android 2.1 or higher.

Device Analyzer collects usage statistics in the background while you use your phone.
This data is stripped of personally identifying information as best as possible while preserving useful information. Periodically the recorded data is uploaded to our server at the University of Cambridge, where we will aggregate it with other people's data and draw inferences from the patterns that emerge.

This is a real-time map of devices as they upload data to the university's server:

Already created a website login from inside the app?
Click here to log in securely.

The example of “Device Analyzer”

Basic Data

This data will usually be shared online after you had three months to inspect your data on the website. If you prefer, you can specify easily and directly within the application that you'd like your data stream to be used only within the University of Cambridge.

when you turn your phone on and off
the version of the operating system and the type of device
the system's local time
the amount of free internal and external storage
when the external storage card is inserted or removed
which parts of Device Analyzer you use as well as internal logging and crash reporting (yes, it analyzes itself!)
whether your phone is ringing normally, is silent or on vibrate
the volume of the different audio streams (ringer, media volume, etc.)
the times at which the phone is charging
the battery level and voltage
the times when you take pictures and how many pictures you have
the times when the screen is turned on and off
the brightness level of the screen and whether brightness is dynamically adjusted
when you enable and disable airplane mode …

The example of “Device Analyzer”

Basic Data

when which mode of network connectivity is available
the **hashed identifier** of the inserted SIM card
whether the phone is roaming or not
cellular signal strength
the amount of data transferred over 3G and wifi
the times when phone calls are made and text messages are sent and received as well as the number of characters per text message
hashed values for the phone numbers involved
when you enable and disable Bluetooth and wifi
hashed data about wifi networks that are in range
hashed data about Bluetooth devices (hashed) in the vicinity if another application initiates a Bluetooth scan (Device Analyzer will not initiate a scan by itself)
when you enable tethering or the mobile hotspot
…

Applications

We will collect the following data about applications on your device:

the list of markets where at least one application was installed from

We will also collect the following data for applications. This data will be shared without revealing the names of the applications unless you have given us express permission to publicly share the names from within the application.

the list of installed applications and which market they were installed from

updates and removals of applications

when you clear the data of an application

the running processes and their memory and CPU usage as well as their importance

the 10 most recently started tasks

how much data each application transferred

<http://deviceanalyzer.cl.cam.ac.uk/collected.htm>

The example of "Device Analyzer"

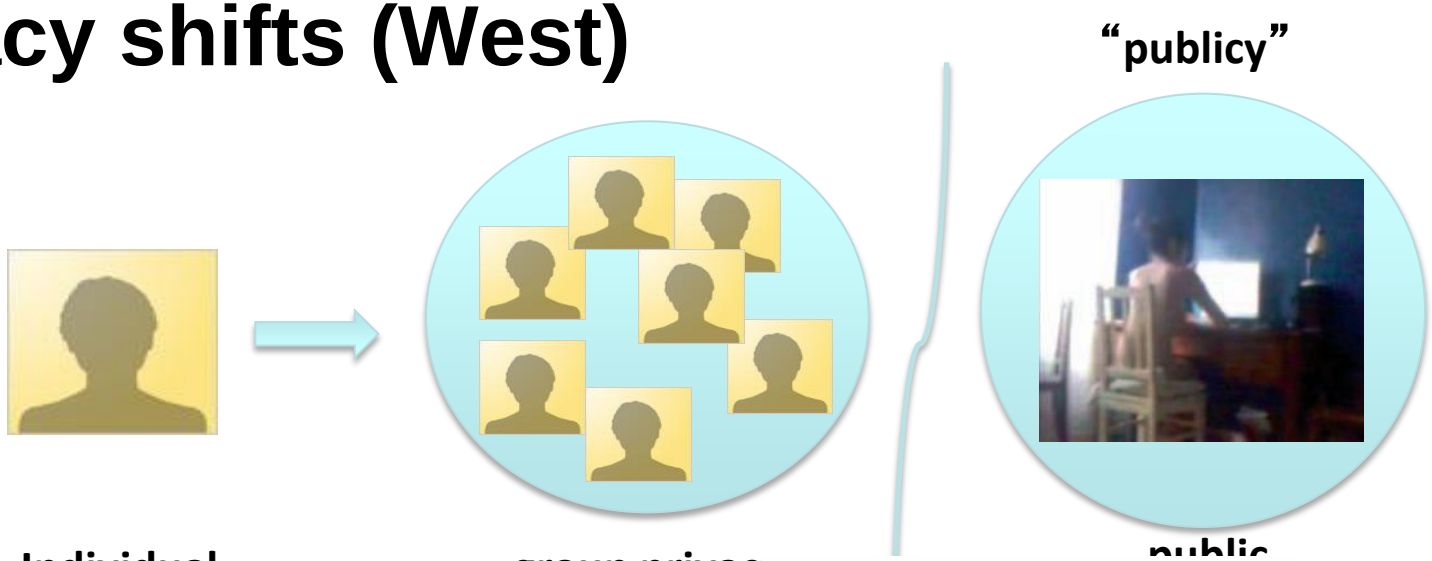
Questions for consideration, discussion

1) Who would voluntarily share this sort of data with researchers?
→ *utilitarian* considerations: benefits to both
the individual participant (more information about one's own phone)
+ larger society (as research results will lead to …)

2) What sorts of privacy protections are at work?
Reasonably good ones? (hashed identities, locations, etc.)
+ individual user has control over application (pause, stop, what data is collected, etc.)

3) BUT:
A) → changing conceptions of "privacy"?
B) → what sort of *selfhood / identity* assumptions are at work?

Privacy shifts (West)



"pub te" ←→

close friend s - videos be "hidden" by t em so that only friends and relatives would know how to find them

highly

ntities, sexual orientation, but <u>not</u>, e.g., home address

(Patricia Lange (2007) in McKee & Porter 2009, 78)

3. Nissenbaum: privacy as contextual integrity

Nissenbaum builds her account on **James Rachel's** theory of privacy – a *relational* (or, alternatively, *social*) understanding of selfhood.

Rachels demarcates a defining connection between **privacy expectations**, on the one hand, and **specific social roles**, on the other, such as "businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child, and so on" (Rachels 1975: 328, cited in Nissenbaum 2010: 65, 123).

Nissenbaum builds on Rachels' account:

> privacy rights defined in terms of flows of information as "appropriate" to a given **context**:

a **context**, in turn, is defined by three parameters **– beginning precisely with the *actors* and thereby, at least implicitly, the *relationships* between actors. Example: medical information shared between doctor / patient**

(remaining parameters are the attributes (types of information) and "transmission principles" of a given context (Nissenbaum 2011: 33).

4. The shift towards relational privacies and research ethics guidelines: *privatlivet*, the *intimsfære*, and the NESH (2006) guidelines

G.H. Mead ([1934] 1967); G. Simmel (1955, 1971); and E. Goffman (1959) → **S. Lomborg** (2012):

"personal space" emerging through a negotiation process between the author of *Huskebloggen* and her readers;

such a space preserves *individual* privacy while simultaneously constituting a *group* or *shared privacy* –
what Lomborg describes as neither simply individual nor solely public, but specifically ***relational*** (2012: 428).

→ **notions of *privatlivet* and *intimsfære* as *relational* terms**

4. The shift towards relational privacies and research ethics guidelines: *privatlivet*, the *intimsfære*, and the NESH (2006) guidelines

// notions of ”the mature human being” in Article 100 of the Norwegian Constitution:

This is **neither the collectivist concept** of the individual, which states that the individual is subordinate to the community, **nor the individualistic view**, which states that regard for the individual takes precedence over regard for the community. The conception of ”the mature human being” can be said to embody **a third standpoint that transcends the other two and assumes that a certain competence (socialization or education) is required in order to function as an autonomous individual in the open society**. (*There Shall Be Freedom of Expression* 2005, 18).

cf. “The Onlife Manifesto”: the self as an inherently **relational** [and] **free [individual]** self. (2013, 7)

4. The shift towards relational privacies and research ethics guidelines: *privatlivet*, the *intimsfære*, and the NESH (2006) guidelines

Contra prevailing research ethics codes – especially U.S. – that build on ***individual*** conceptions of privacy rights and expectations –

NESH guidelines include attention to *relational* conceptions of privacy (as underlain by relational notions of *privatlivet*, the *intimsfære*?):

13. The obligation to respect individuals' privacy **[privatlivet] and *close relationships***

13. The obligation to respect individuals' privacy [privatlivet] and *close relationships*

Researchers shall show due respect for **an individual's privacy**. Informants are entitled to be able to check whether confidential information about them is accessible to others.

Respect for privacy aims at protecting individuals against unwanted interference and exposure. This applies not only to emotional issues, but also to questions that involve sickness and health, political and religious opinions, and sexual orientation.

Researchers should be especially compassionate when they ask questions that involve intimate issues and they should avoid placing informants under pressure. **What is perceived as sensitive information can vary from one individual or group to the next.**

Distinguishing between the private and public spheres can sometimes be difficult when it comes to information about behaviour that is communicated and stored on the Internet. When using material from such interactions, researchers must pay sufficient attention to the fact that **people's understanding of what is private and what is public in such media can vary**. (NESH 2006 B.13, p. 17)

5. Concluding remarks: more apps, new research ethics?

A. Not the end of individual privacy →

”privacies” / *privatlivet* + *intimsfære* become more **complex**: **both** continuing *individual* privacy expectations **and** growing, relationally-oriented ”contextual integrity”

***B. Can* be done** – e.g., “Telenor smartphone undersøgelse” <http://www.wilke.dk/telenorpanel/>, which offers strong individual privacy protections.

C. *Can* also *fail*: example from Sweden.

D. Future developments?

From ”publicly private” / ”privately public”: ”personal space”

→ shift to *hybrid: individual* **and** *relational* selfhood **+**

→ **Nissenbaum**: privacy as ”contextual Integrity” **+**
NESH guidelines as first example **+**

Contemporary theoretical discussions, including:

emerging *philosophical* accounts of ”relational autonomy” (Mackenzie 2008) / ”distributed morality” and ”distributed responsibility (Floridi 2012)

C. Ess and H. Fossheim. 2013. Personal Data: Changing Selves, Changing Privacies. In M. Hildebrandt, K. O'Hara, & M. Waidner, eds. *Digital Enlightenment Forum Yearbook, The Value of Personal Data*. Amsterdam: IOS Press.

A. Markham (2012) Fabrication as Ethical Practice, *Information, Communication & Society*, 15:3, 334-353, DOI: 10.1080/1369118X.2011.641993

→ **new research ethics / codes**