UNIVERSITÄT SIEGEN

Security of Online Social Networks

Access Control

Lehrstuhl IT-Sicherheitsmanagment

Universität Siegen

May 10, 2012

Overview Lesson 05

Access Control Principles

Social Graph based Access Control

RDF Access Control

Facebook Defaults

Objective

to control:

$$\underbrace{\text{Subject}}_{\text{Who?}} \xrightarrow[\text{What?}]{\text{Access Rights}} \underbrace{\text{Object}}_{\text{With?}}$$

Examples:

- "You may show my pictures to Alice."
- `-rw-r--r--  1 lars lars [...] 05-accesscontrol.pdf`

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)

Models

- Access Control Matrix
  - Capabilities
  - Access Control Lists
- Security Labels
  - Bell LaPadula
  - Chinese Wall Model (Brewer and Nash model)

Access Control Matrix

	o_1	$\ldots$	o_m	s_1	$\ldots$	o_n
s_1						
s_2						
$\vdots$						
s_m						

- Subjects: $S = \{s_1 \ldots s_m\}$
- Objects: $O = \{o_1 \ldots o_n\}$
- Rights: $R = \{r_1 \ldots r_k\}$

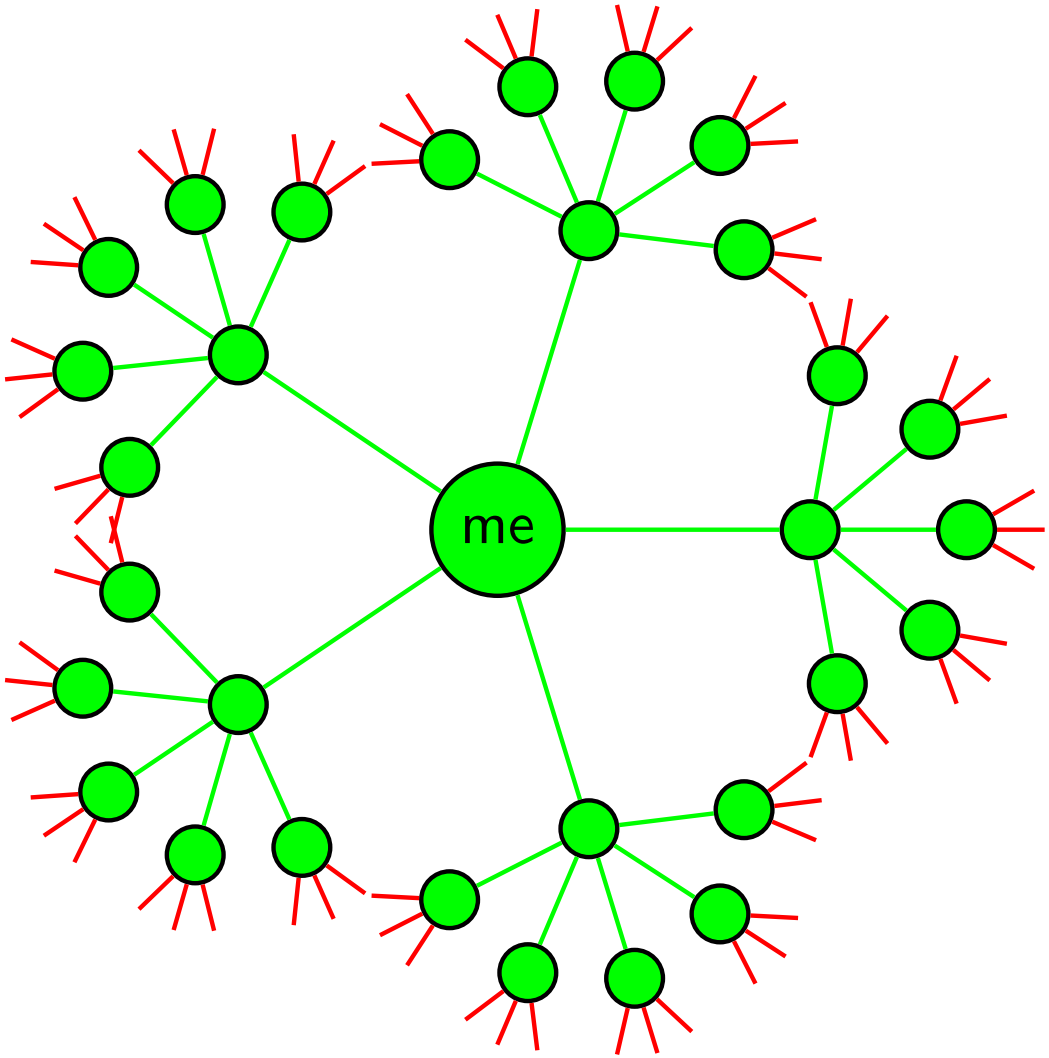
$A[s_i, o_j] = \{r_{ij_1}, \ldots, r_{ij_l}\}$:
Subject s_i has Rights $r_{ij_1}, \ldots, r_{ij_l}$ to Object o_j.

Social Graph based Access Control

Graph Attribute Access Rights

$$
\begin{aligned}
G &= (V, E, p, a) \\
& V: \text{ vertices} \\
& E: \text{ edges} \\
& p: V \rightarrow \text{ personal attribs} \\
& a: E \rightarrow \text{ link attribs}
\end{aligned}
$$

- Node Relation Attributes
- Distance $d : V \times V \rightarrow \mathbb{R}$
- Conditioned Path/WoT
- Labels
  - Similarity e.g. Group
  - Requirement
  - Streams/Aspects/Circles



Path Distance

Access Control:

max 2 hobs (FoaF)

RDF Access Control

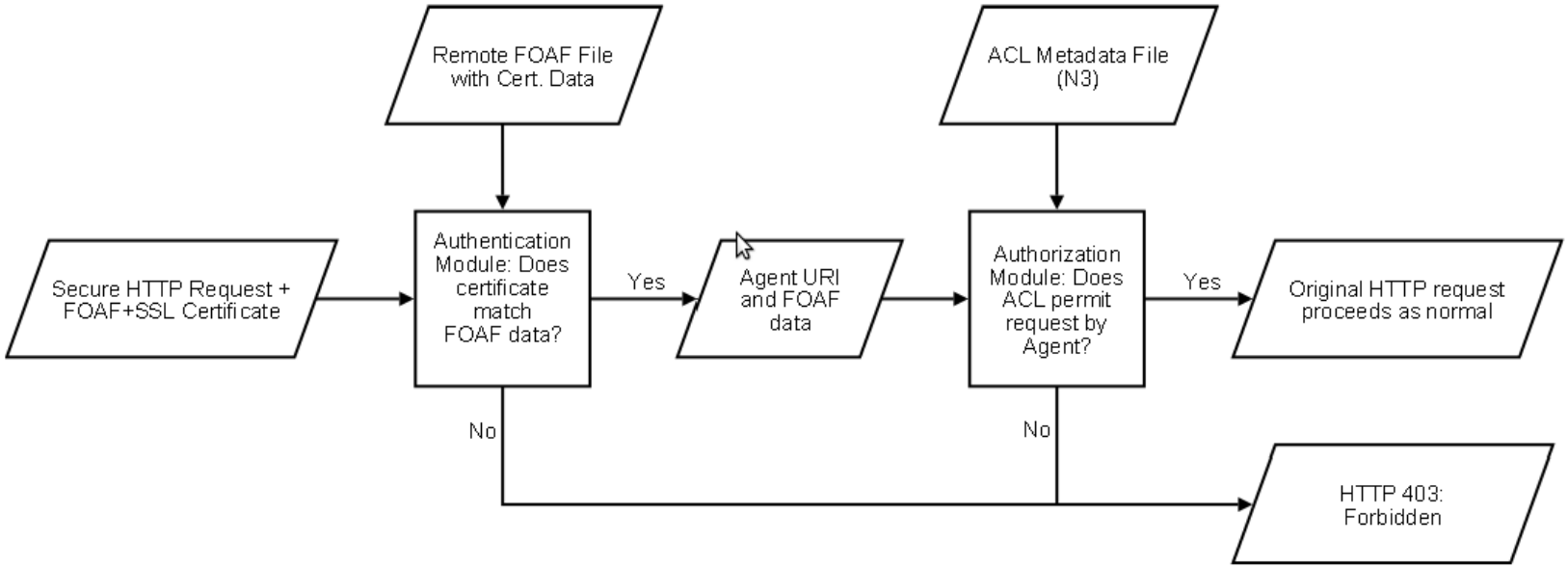
W3C ACL for FoaF

- Hollenbach, Presbrey, Berners-Lee: Using RDF Metadata To Enable Access Control on the Social Semantic Web, 2009
- Basic Access Control ontology
  `http://www.w3.org/ns/auth/acl`
- Apache mod authn webid
- Working Prototype for AC Managment GUI
  `http://dig.csail.mit.edu/2009/aclsidebar`

```
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
[]
  a acl:Authorization ;
  acl:defaultForNew <.> ;
  acl:accessTo <foaf.rdf> ;
  acl:agent <http://presbrey.mit.edu/foaf#presbrey> ;
  acl:mode acl:Control, acl:Read, acl:Write .
[]
  a acl:Authorization ;
  acl:accessTo <foaf.rdf> ;
  acl:agentClass <http://xmlns.com/foaf/0.1/Agent> ;
  acl:mode acl:Read.
```

[Hollenbach, Presbrey, Berners-Lee: Using RDF Metadata To Enable Access Control on the Social Semantic Web 2009]

Authentication Process



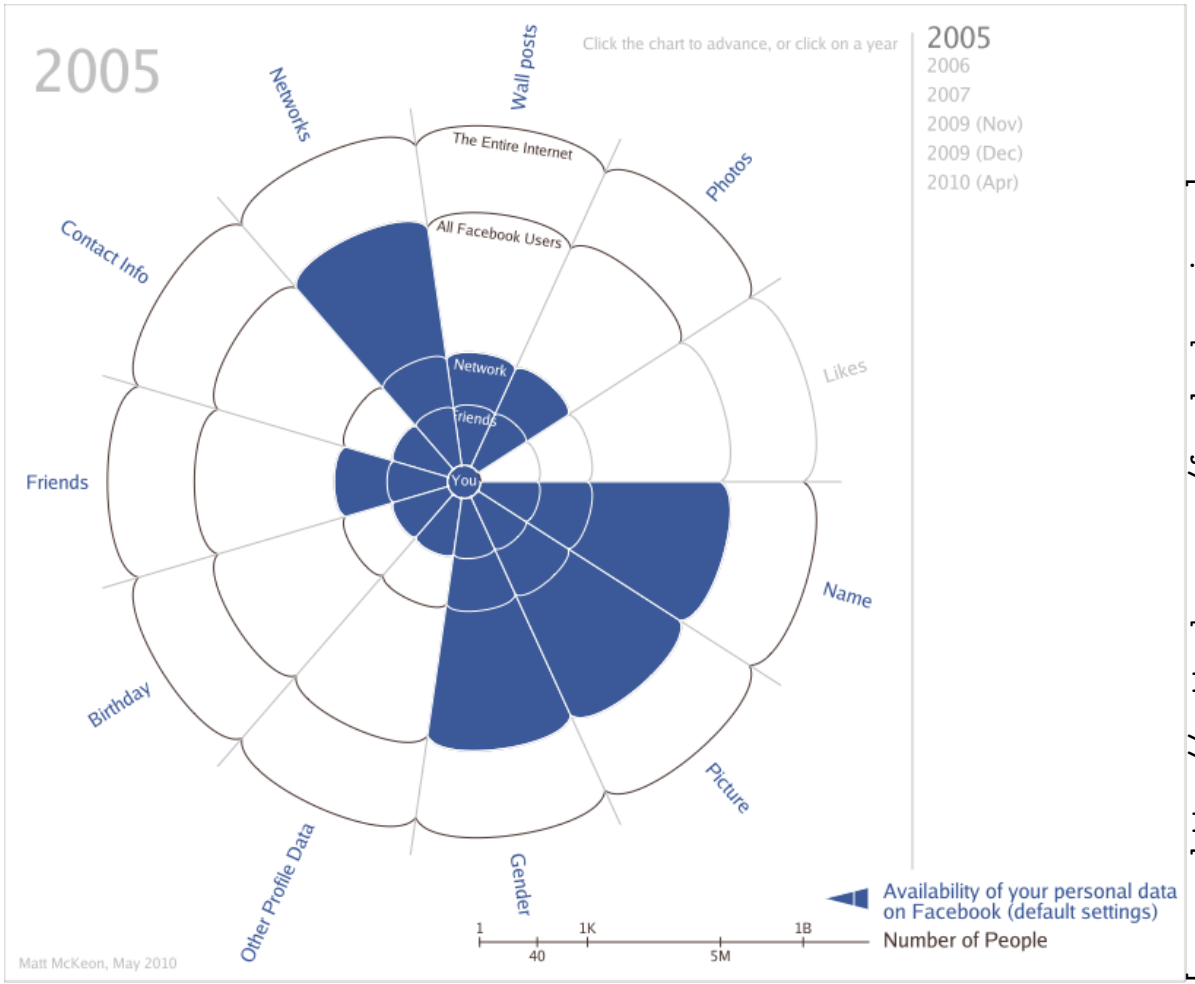
[Hollenbach, Presbrey, Berners-Lee: Using RDF Metadata To Enable Access Control on the Social Semantic Web 2009]

Discussion W3C ACL

- Group rights `agentClass`
- Express "Friend-distance read rights"?

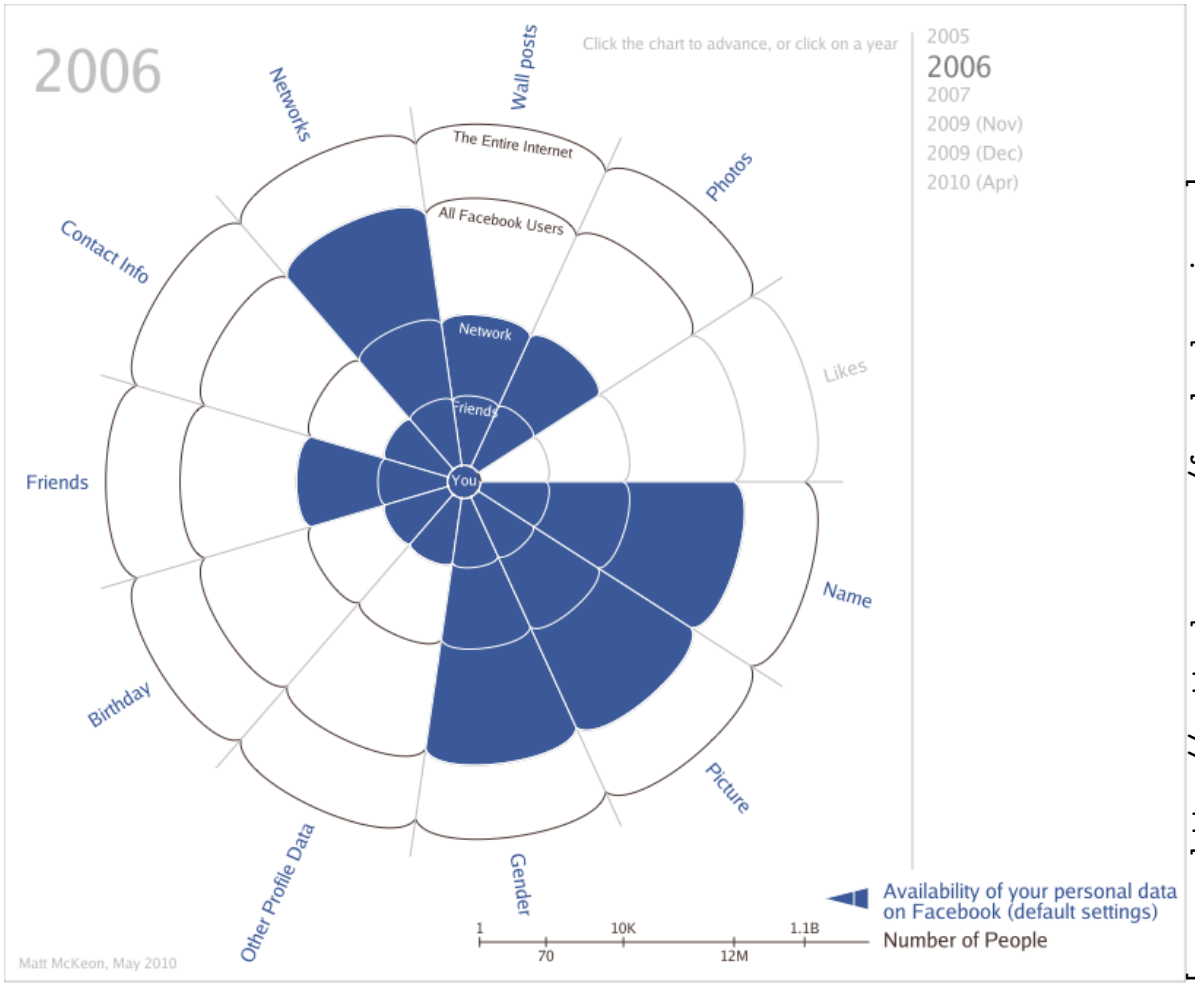
Facebook Defaults

Facebook Default View Rights



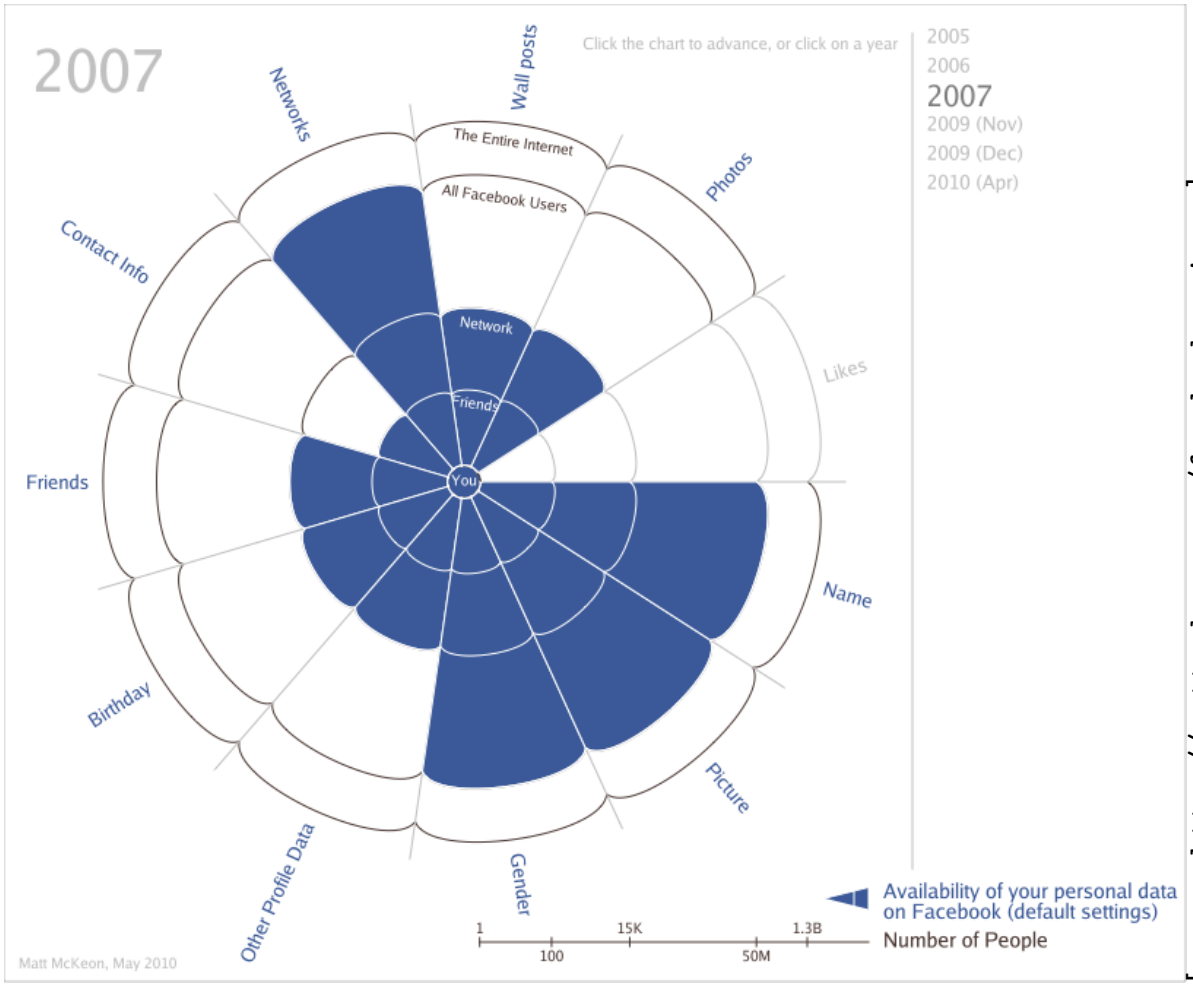
[source: http://mattmckeon.com/facebook-privacy]

Facebook Default View Rights



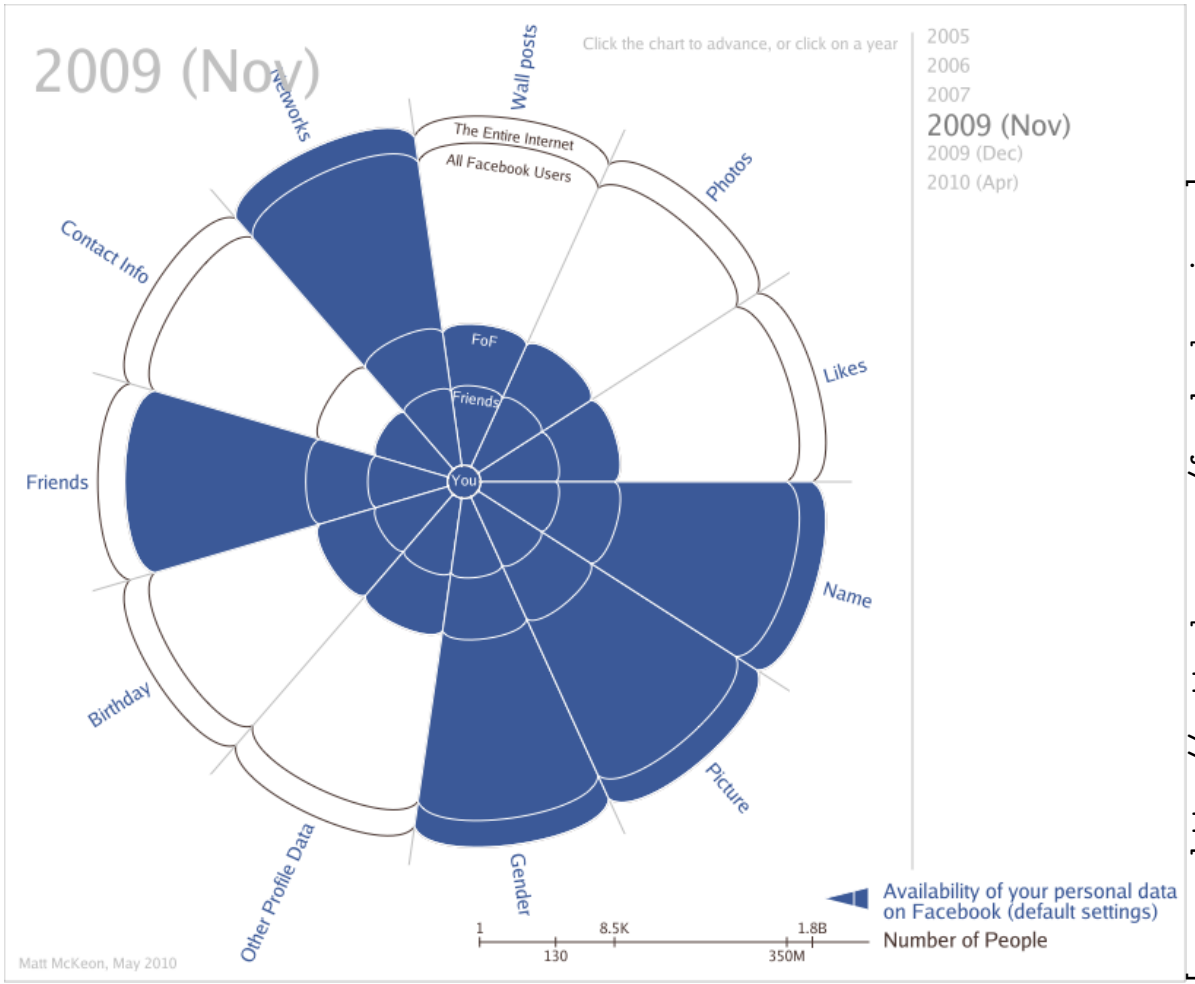
[source: http://mattmckeon.com/facebook-privacy]

Facebook Default View Rights



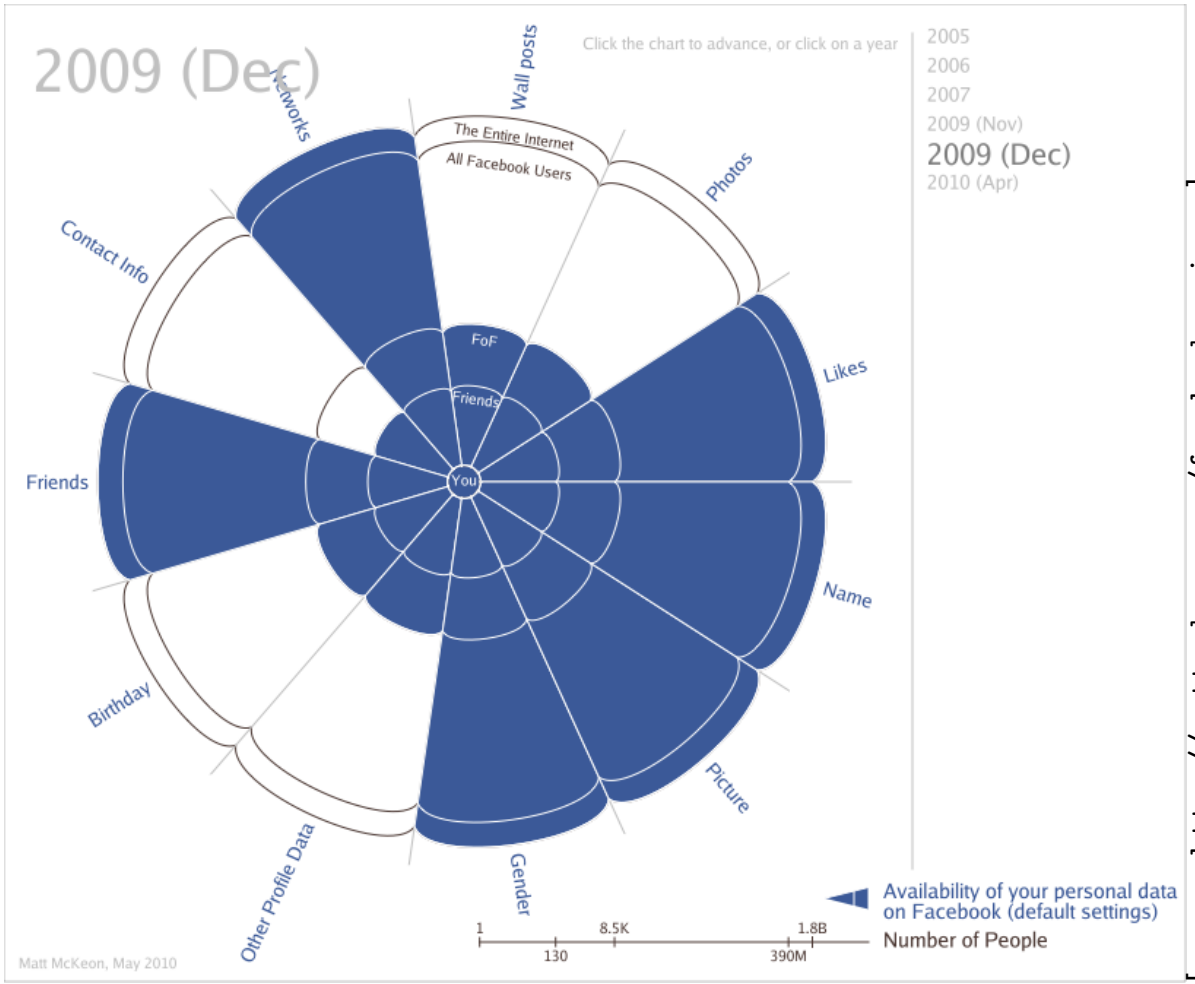
[source: http://mattmckeon.com/facebook-privacy]

Facebook Default View Rights



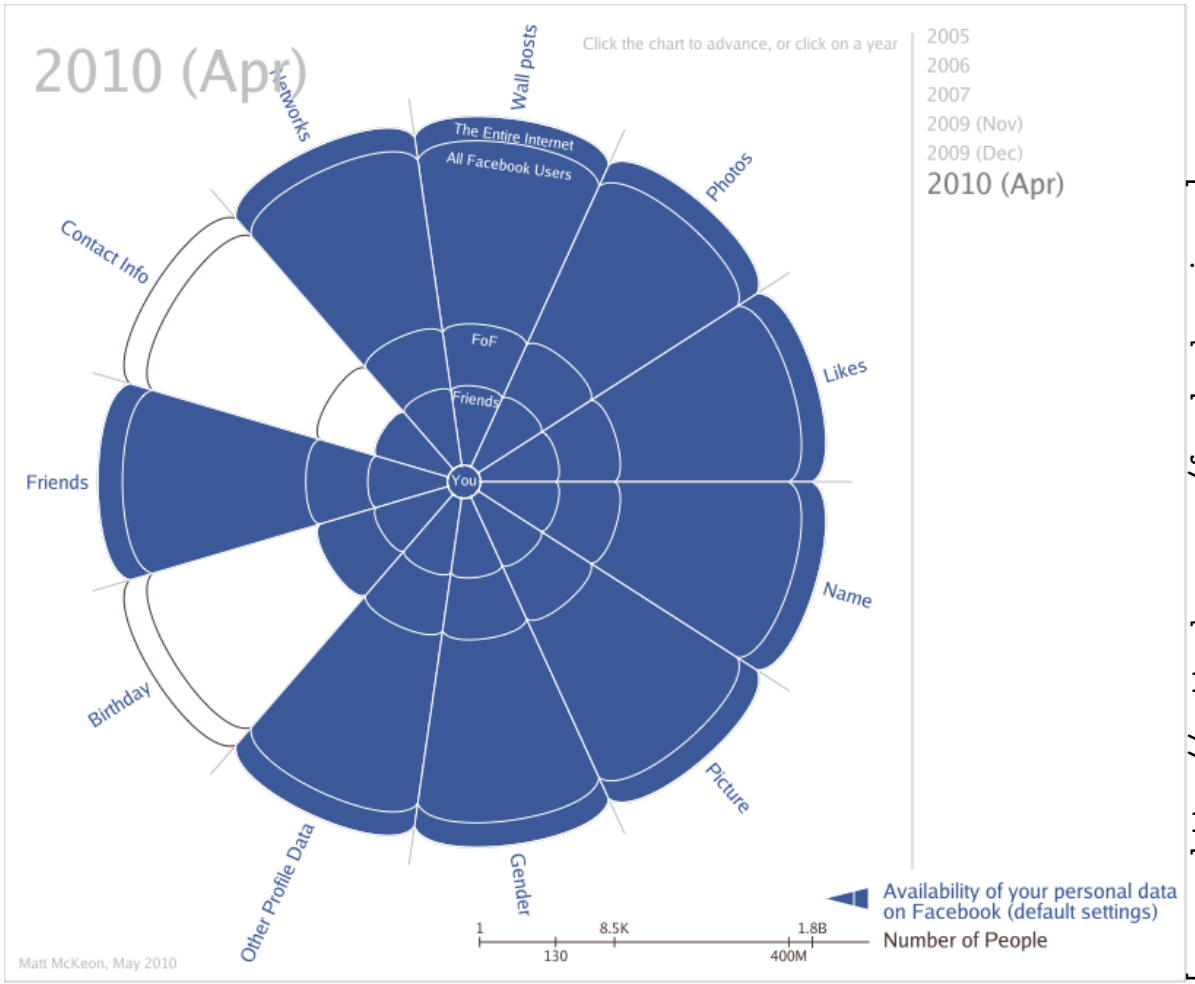
[source: http://mattmckeon.com/facebook-privacy]

Facebook Default View Rights



[source: http://mattmckeon.com/facebook-privacy]

Facebook Default View Rights



[source: http://mattmckeon.com/facebook-privacy]

Literatur I


D. D. F. Brewer and D. M. J. Nash, "The chinese wall security policy," *IEEE*, 1989. [Online]. Available: http://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/brewer_nash_89.pdf


J. Hollenbach, J. Presbrey, and T. Berners-Lee, "Using rdf metadata to enable access control on the social semantic web," 2009. [Online]. Available: dig.csail.mit.edu/2009/Papers/ISWC/rdf-access-control/paper.pdf