Designing for Privacy

Human factors and system’s engineering

Privacy

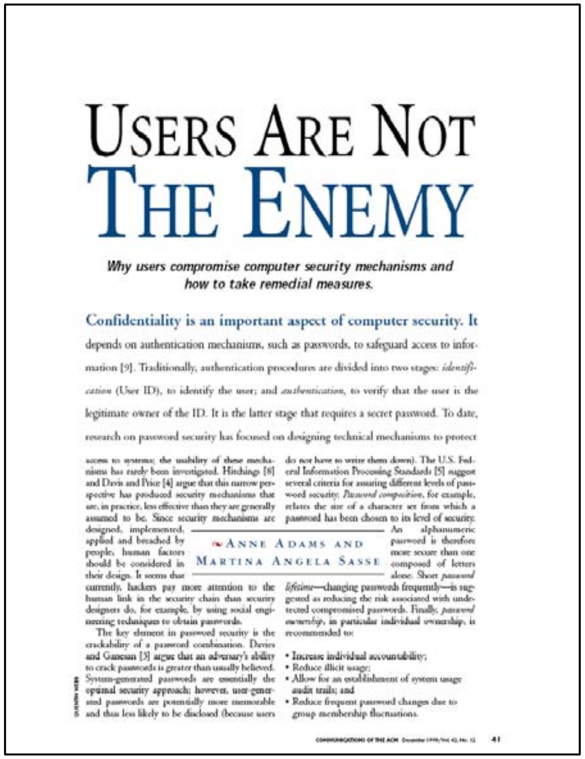
- Non-electronic situations
  - A “boundary regulation process” of accessibility depending on “context” (Altman)
  - A “personal adjustment process” (Westin) balancing the desire for privacy against the desire to interact in the context of social norms and their environment
- Electronic systems
  - A distinction (Solove) between *access control* (regulating access to information about oneself) and *risk management* (reducing likelihood of unintended/undesired usage)

Personal attitudes

- Behavior does not always coincide with expressed attitudes
  - Economic perspective (“privacy economics”)
    - efficiency of transactions aided by disclosure or
    - value of short-term disclosure weighed more heavily than long-term effects)
  - Psychological perspective
    - the temptation to reveal
    - more concerned about disclosing information perceived to be varying from the norm
- Highly variable from person to person
  - “Unconcerned” or “marginally concerned” (20-25% of the population)
  - “fundamentalists”
  - “pragmatists”
    - “identity aware” (concerned with specific personally identifiable information)
    - “profile aware” (concerned with characterizing information)

Human factors

- Importance of human factors ("Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design.")
- Studies show that users do not employ recommended practices in password management (e.g., short passwords kept for long periods)
- A study:
  - Web survey (139 responses)
    - Half of respondents from Company A
    - Remainder from global community
  - In depth interview (30 subjects)
    - Equal numbers from Company A and B
    - Semi-structured, allowed open-ended suggestion of new issues
  - Findings in four areas
- Theme: user-centered design and user training are central to good security



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

ANNE ADAMS AND MARTINA ANGELA SASSE

The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary's ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password lifetime*—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

COMMUNICATIONS OF THE ACM December 1999/Vol. 42, No. 12 41

Finding 1: Multiple Passwords

- Multiple passwords
  - required by different applications/systems
  - Mandatory expiration often enforced
- These factors encourage users to employ unsafe practices
  - write down the passwords (50% of survey respondents)
  - poor password design
    - Repeated use of same password
    - Short/easily cracked passwords
    - password linking (name1, name2, name3,…) (50% of respondents)
- The dilemma: users "perceive their behavior to be caused by a mechanism designed to increase security."

Finding 2: Password Content

- In selecting passwords
  - Users have inadequate knowledge of how to select passwords (dictionary words and names were often used)
  - Users did not understand how cracking works
- Dilemma:
  - “restrictions introduced to create more secure password content may produce less memorable passwords, leading to increased password disclosure”
  - “having to circumvent security procedures lowers users’ regard for the overall security arrangements in the organization, which, in turn, increases password disclosure.”

Finding 3: Work Practices

- Passwords must (be perceived to) be compatible with work practices
  - Users in Organization A found individual passwords for group work to be undesirable (individual passwords were seen by Organization A as allowing better accountability/audits)
  - Users rejected Organization B’s practice of having group passwords for individual personal information (email)

Finding 4: User's perceptions

- Lack of information on security threats and security goals lead users to develop their own ("often wildly inaccurate") models that guide their behavior
  - Users considered personnel files and email as sensitive but customer information was seen as less sensitive (was this in line with the organization's interests?)
  - Users considered their password safety less important because their role in the organization was not important.
  - Users had confusion about authentication (believing that user IDs were similar to passwords and had to be constructed and secured in the same manner).

The downward spiral

- Security departments, motivated by the *need-to-know* principle, insufficient inform users of treats and security procedures
- Security mechanism/policies are developed that are not based on user-centered design and, therefore, have lower usability
- Users perceive that the security mechanisms/policies interfere with work practice and, lacking better information, develop behaviors based on incorrect models of threats and information sensitivities
- Security departments perceive users' behavior as "inherently insecure," which reinforces their reluctance to share information with users

Recommendations

- Inform users
  - Good practices on password design; provide feedback during password construction process.
  - Existing and potential threats
  - Which systems/information is sensitive and why.
- Security should be visible
  - Detect and challenge in a constructive manner insecure user behaviors
- Employ a user-centered design philosophy to ensure that security mechanisms align with user practice.

Engineering for privacy

- Three technical "spheres"
  - User (person's device)
  - Recipient (organization to which user's information is disclosed)
  - Joint (data hosting and related service, aka the "cloud)
- Privacy concerns
  - (see table)

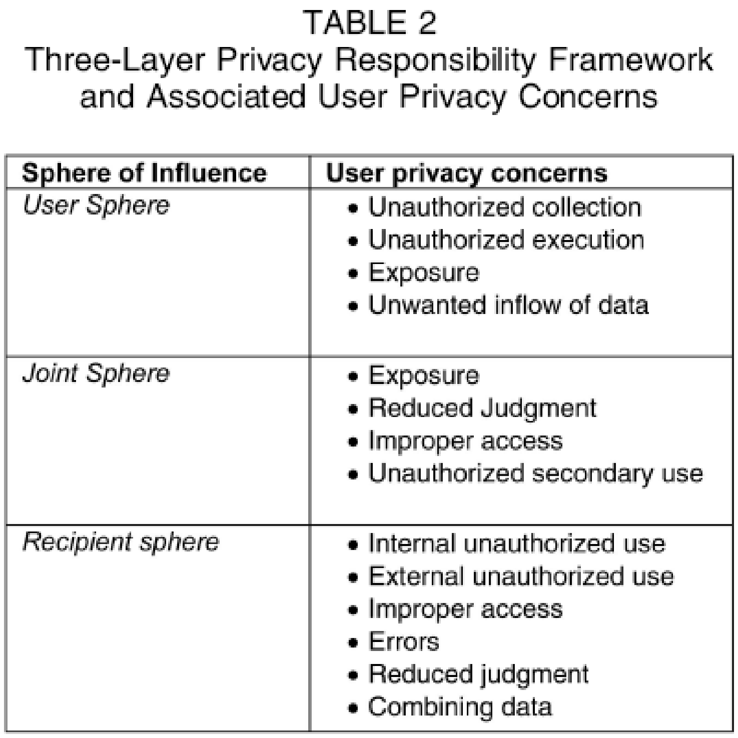
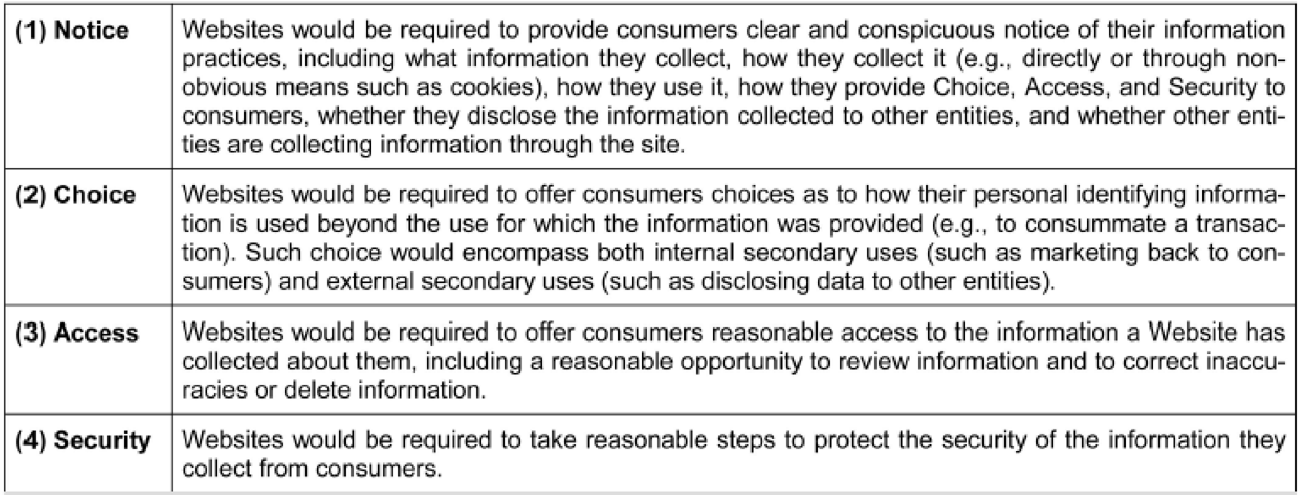


TABLE 2
Three-Layer Privacy Responsibility Framework
and Associated User Privacy Concerns

Sphere of Influence	**User privacy concerns**
User Sphere	• Unauthorized collection • Unauthorized execution • Exposure • Unwanted inflow of data
Joint Sphere	• Exposure • Reduced Judgment • Improper access • Unauthorized secondary use
Recipient sphere	• Internal unauthorized use • External unauthorized use • Improper access • Errors • Reduced judgment • Combining data

Fair Information Practices

TABLE 3
The Fair Information Practices Proposed by the US Federal Trade Commission in Their 2000 Report to Congress [79]



(1) Notice	Websites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
(2) Choice	Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
(3) Access	Websites would be required to offer consumers reasonable access to the information a Website has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.
(4) Security	Websites would be required to take reasonable steps to protect the security of the information they collect from consumers.

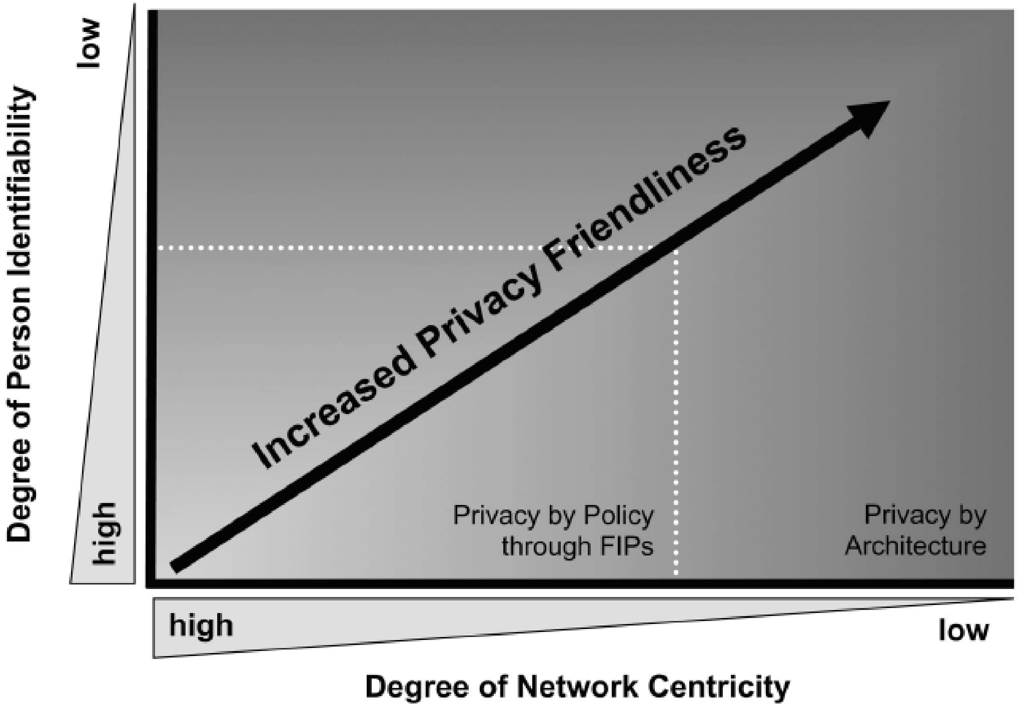
- Focuses on “notice” and “choice”
- Tailored to e-commerce

Design factors

- Network centricity (e.g., a location aware system in which the user does not have to disclose their location to a central server vs. one where the central server knows (and can possibly share with others) their location)

- Identifiability (a (pseudo) anonymous identity or providing attributes (role, right) rather than identity to accomplish a transaction

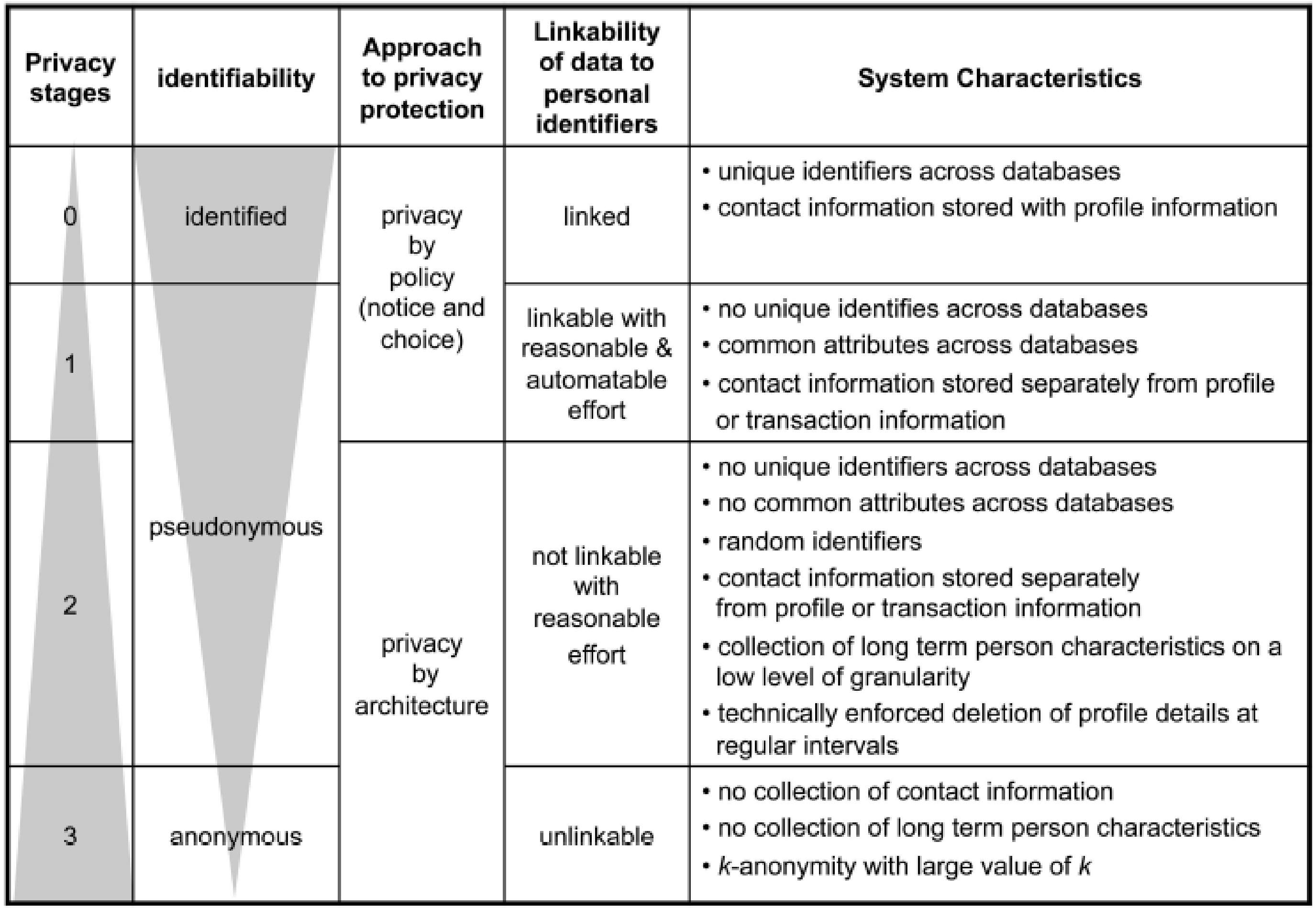
Architecture types


Degree of Person Identifiability
low
high
Increased Privacy Friendliness
Privacy by Policy through FIPs
Privacy by Architecture
high
low
Degree of Network Centricity

- Privacy-by-architecture (the way the system is built)
- Privacy-by-policy (the rules which control the system)

Degrees of Identifiability

TABLE 4
Framework for Privacy-Friendly System Design



Privacy stages	identifiability	Approach to privacy protection	Linkability of data to personal identifiers	System Characteristics
0	identified	privacy by policy (notice and choice)	linked	• unique identifiers across databases • contact information stored with profile information
1	pseudonymous		linkable with reasonable & automatable effort	• no unique identifies across databases • common attributes across databases • contact information stored separately from profile or transaction information
2		privacy by architecture	not linkable with reasonable effort	• no unique identifiers across databases • no common attributes across databases • random identifiers • contact information stored separately from profile or transaction information • collection of long term person characteristics on a low level of granularity • technically enforced deletion of profile details at regular intervals
3	anonymous		unlinkable	• no collection of contact information • no collection of long term person characteristics • *k*-anonymity with large value of *k*

Implementing Privacy-by-policy

- A site can instill trust by revealing:
  - type of information collected
  - use of information
  - conditions for sharing this information with others
    - and restriction upon or policies of such third parties
  - security of the information
  - how users access information about themselves
    - access to full individual profile should be accessible
  - how to provide/withhold consent

- Notification of collection/consent
  - judicious interruption of user
  - user Preference policies can minimize interruptions

- Enforcing compliance
  - Compliance engines (validates access against privacy policy)
  - Auditing mechanisms (reveals possible breaches leading to sanctions)