End-User Privacy in Human–Computer Interaction
End-User Privacy in Human–Computer Interaction

Giovanni Iachello

Georgia Institute of Technology
USA
giac@cc.gatech.edu

Jason Hong

Carnegie Mellon University
USA
jasonh@cs.cmu.edu

now
the essence of knowledge

Boston – Delft
Foundations and Trends® in Human–Computer Interaction
Volume 1 Issue 1, 2007
Editorial Board

Editor-in-Chief:
Ben Bederson
Human–Computer Interaction Lab
University of Maryland
3171 A. V. Williams Bldg
20742, College Park, MD
USA
bederson@cs.umd.edu

Editors
Gregory Abowd (Georgia Institute of Technology)
Jonathan Grudin (Microsoft Research)
Clayton Lewis (University of Colorado)
Jakob Nielsen (Nielsen Norman Group)
Don Norman (Nielsen Norman Group and Northwestern University)
Dan Olsen (Brigham Young University)
Gary Olson (University of Michigan)
Sharon Oviatt (Oregon Health and Science University)
Editorial Scope

Foundations and Trends® in Human–Computer Interaction will publish survey and tutorial articles in the following topics:

- History of the research Community
- Design and Evaluation
  - Ergonomics/Human Factors
  - Cognitive engineering and performance models
  - Predictive models of interaction
  - User-centered design processes
  - Participatory design
  - Graphic design
  - Discount evaluation techniques
  - Design and interaction
  - Ethnography
- Theory
  - Models of cognition
  - Empirical methods of evaluation
  - Qualitative methods of design and evaluation
- Technology
  - Programming the graphical user interface
  - Input technologies
  - Output technologies
- Computer supported cooperative work
  - History of CSCW in HCI
  - Organizational issues
  - Online communities
- Games
- Communication technologies
- Interdisciplinary influence
  - The role of the social sciences in HCI
  - MIS and HCI
  - Graphic design
  - Artificial intelligence and the user interface
  - Architecture and the role of the physical environment
- Advanced topics and trends
  - Information visualization
  - Web design
  - Assistive technologies
  - Multimodal interaction
  - Perception and the user interface
  - Specific user groups (children, elders, etc.)
  - Sensor-based or tangible interaction
  - Ubiquitous computing
  - Virtual reality
  - Augmented reality
  - Wearable computing
  - Design and fashion
  - Privacy and social implications

Information for Librarians

Foundations and Trends® in Human–Computer Interaction, 2007, Volume 1, 4 issues. ISSN paper version 1551-3955. ISSN online version 1551-3963. Also available as a combined paper and online subscription.
End-User Privacy in Human–Computer Interaction

Giovanni Iachello¹ and Jason Hong²

¹ Georgia Institute of Technology, USA, giac@cc.gatech.edu
² Carnegie Mellon University, USA, jasonh@cs.cmu.edu

Abstract

The purpose of this article is twofold. First, we summarize research on the topic of privacy in Human–Computer Interaction (HCI), outlining current approaches, results, and trends. Practitioners and researchers can draw upon this review when working on topics related to privacy in the context of HCI and CSCW. The second purpose is that of charting future research trends and of pointing out areas of research that are timely but lagging. This work is based on a comprehensive analysis of published academic and industrial literature spanning three decades, and on the experience of both ourselves and of many of our colleagues.
# Contents

1 Introduction 1  
1.1 Why Should HCI Researchers Care About Privacy? 2  
1.2 Sources Used and Limitations of this Survey 5  

2 The Privacy Landscape 7  
2.1 Often-Cited Legal Foundations 7  
2.2 Philosophical Perspectives on Privacy 9  
2.3 An Historic Perspective on Privacy 13  

3 Understanding, Building and Evaluating Privacy in Interactive Systems 17  
3.1 Understanding Users’ Privacy Preferences 19  
3.2 Methodological Issues 33  
3.3 Prototyping, Building, and Deploying Privacy-Sensitive Applications 41  
3.4 Evaluation 65  
3.5 Privacy Frameworks 74  

4 Trends and Challenges in Privacy HCI Research 95  
4.1 Better Ways of Helping End-Users Manage Their Personal Privacy 96  
4.2 Understanding of People’s Attitude and Behavior 98
4.3 Developing a “Privacy HCI Toolbox” 100
4.4 Better Organizational Practices 102
4.5 Understanding Adoption 105

5 Conclusions 113

Acknowledgments 115

References 117
Privacy is emerging as a critical design element for interactive systems in areas as diverse as e-commerce [63], health care [287], office work [156], and personal communications. These systems face the same fundamental tension. On the one hand, personal information can be used to streamline interactions, facilitate communication, and improve services. On the other hand, this same information introduces risks, ranging from mere distractions to extreme threats.

Government reports [239, 283], essays [223], books [17, 93, 196, 303], and media coverage [252, 295, 312] testify on peoples’ concerns regarding the potential for abuse and general unease over the lack of control over a variety of computer systems. Similarly, application developers worry that privacy concerns can impair the acceptance and adoption of their systems.

No end-to-end solutions exist to design privacy-respecting systems that cater to user concerns. Lessig provided a very high level framework for structuring the protection of individuals’ privacy, which leverages four forces: laws, social norms, the market, and technical mechanisms [195]. However, the challenge is in turning these broad guidelines into actionable design solutions. Our thesis is that
researchers in Human–Computer Interaction (HCI) and Computer-Supported Cooperative Work (CSCW) can greatly improve the protection of individual’s personal information, because many of the threats and vulnerabilities associated with privacy originate from the interactions between the people using information systems, rather than the actual systems themselves.

Approaching the topic of privacy can be daunting for the HCI practitioner, because the research literature on privacy is dispersed across multiple communities, including computer networking, systems, HCI, requirements engineering, management information systems (MIS), marketing, jurisprudence, and the social sciences. Even within HCI, the privacy literature is fairly spread out. Furthermore, many IT professionals have common-sense notions about privacy that can turn out to be inaccurate.

Hence, the goal of this article is to provide a unified overview of privacy research in HCI, focusing specifically on issues related to the design and evaluation of end-user systems that have privacy implications. In Section 2, we present two philosophical outlooks on privacy that will help the practitioner frame research questions and design issues. We also show how privacy research has evolved in parallel with HCI over the past 30 years. Section 3 presents an overview of the research literature, structured along an ideal inquiry-build-evaluate development cycle. Finally, in Section 4, we outline key research challenges, where we think that HCI methods and research approaches can make a significant impact in furthering our knowledge about information privacy and personal data protection.

In the remainder of this section, we explain why we think privacy research is challenging and interesting for HCI, and map out relevant literature published in HCI conferences and journals, and in neighboring fields such as MIS and CSCW.

1.1 Why Should HCI Researchers Care About Privacy?

Human–computer interaction is uniquely suited to help design teams manage the challenges brought by the need of protecting privacy and personal information. First, HCI can help understand the many notions
1.1 Why Should HCI Researchers Care About Privacy?

of privacy that people have. For example, Westin describes four states of privacy: solitude, intimacy, anonymity, and reserve [302]. Similarly, Murphy lists the following as expressions of privacy: “to be free from physical invasion of one’s home or person,” “the right to make certain personal and intimate decisions free from government interference,” “the right to prevent commercial publicity of one’s own name and image,” and “the control of information concerning an individual’s person” [212]. These perspectives represent different and sometimes conflicting worldviews on privacy. For example, while some scholars argue that privacy is a fundamental right, Moor claims that privacy is not a “core value” on par with life, security, and freedom, and asserts that privacy is just instrumental for protecting personal security [209].

Second, a concept of tradeoff is implicit in most discussions about privacy. In 1890, Warren and Brandeis pointed out that privacy should be limited by the public interest, a position that has been supported by a long history of court rulings and legal analysis [296]. Tradeoffs must also be made between competing interests in system design. For example, the developer of a retail web site may have security or business requirements that compete with the end-user privacy requirements, thus creating a tension that must be resolved through tradeoffs. Because HCI practitioners possess an holistic view of the interaction of the user with the technology, they are ideally positioned to optimally work through and solve these tradeoffs.

Third, privacy interacts with other social concerns, such as control, authority, appropriateness, and appearance. For example, while parents may view location-tracking phones as a way of ensuring safety and maintaining peace of mind, their children may perceive the same technology as smothering and an obstacle to establishing their identity. These relationships are compellingly exemplified in Goffman’s description of the behavior of individuals in small social groups [120]. For instance, closing one’s office door not only protects an individual’s privacy, but asserts his ability to do so and emphasizes the difference from other colleagues who do not own an individual office. Here, the discriminating application of HCI tools can vastly improve the accuracy and quality of the assumptions and requirements feeding into system design.
Fourth, privacy can be hard to rationalize. Multiple studies have demonstrated that there is a difference between privacy preferences and actual behavior [8, 39]. Many people are also unable to accurately evaluate low probability but high impact risks [250], especially related to events that may be far removed from the time and place of the initial cause [130]. For example, a hastily written blog entry or impulsive photograph on MySpace may cause unintentional embarrassment several years down the road. Furthermore, privacy is fraught with exceptions, due to contingent situations and historical context. The need for flexibility in these constructs is reflected by all the exceptions present in data protection legislation and by social science literature that describes privacy as a continuous interpersonal “boundary-definition process” rather than a static condition [17]. The use of modern “behavioral” inquiry techniques in HCI can help explicate these behaviors and exceptions.

Finally, it is often difficult to evaluate the effects of technology on privacy. There are few well-defined methods for anticipating what privacy features are necessary for a system to gain wide-scale adoption by consumers. Similarly, there is little guidance for measuring what level of privacy a system effectively offers or what its overall return on investment is. Like “usability” and “security,” privacy is a holistic property of interactive systems, which include the people using them. An entire system may be ruined by a single poorly implemented component that leaks personal information, or a poor interface that users cannot understand.

In our opinion, HCI is uniquely suited to help design teams manage these challenges. HCI provides a rich set of tools that can be used to probe how people perceive privacy threats, understand how people share personal information with others, and evaluate how well a given system facilitates (or inhibits) desired privacy practices. Indeed, the bulk of this paper examines past work that has shed light on these issues of privacy.

As much as we have progressed our understanding of privacy within HCI in the last 30 years, we also recognize that there are major research challenges remaining. Hence, we close this article by identifying five
“grand challenges” in HCI and privacy:

— Developing standard privacy-enhancing interaction techniques.
— Developing analysis techniques and survey tools.
— Documenting the effectiveness of design tools, and creating a “privacy toolbox.”
— Furthering organizational support for managing personal data.
— Developing a theory of technological acceptance, specifically related to privacy.

These are only few of the challenges facing the field. We believe that focusing research efforts on these issues will lead to bountiful, timely and relevant results that will positively affect all users of information technology.

1.2 Sources Used and Limitations of this Survey

In this survey paper, we primarily draw on the research literature in HCI, CSCW, and other branches of Computer Science. However, readers should be aware that there is a great deal of literature on privacy in the MIS, advertising and marketing, human factors, and legal communities.

The MIS community has focused primarily on corporate organizations, where privacy perceptions and preferences have a strong impact on the adoption of technologies by customers and on relationships between employees. The advertising and marketing communities have examined privacy issues in reference to privacy policies, and the effects that these have on consumers (e.g., work by Sheehan [257]).

The legal community has long focused on the implications of specific technologies on existing balances, such as court rulings and the constitutional status quo. We did not include legal literature in this article because much scholarly work in this area is difficult to use in practice during IT design. However, this work has some bearing on HCI and researchers may find some analyses inspiring, including articles on data protection [249], the relation between legislation and technology
Introduction

As one specific example, Strahilevitz outlines a methodology for helping courts decide on whether an individual has a reasonable expectation of privacy based on the social networking literature [272]. As another example, Murphy discusses whether or not the default privacy rule should allow disclosure or protection of personal information [212].

Privacy research is closely intertwined with security research. However, we will not refer HCI work in the security field. Instead, we direct readers to the books *Security and Usability* [67] and *Multilateral Security in Communications* [210] for more information.

We also only tangentially mention IT management. Management is becoming increasingly important in connection to privacy, especially after the enactment of data protection legislation [178]. However, academia largely ignores these issues and industry does not publish on these topics because specialists perceive knowledge in this area as a strategic and confidential asset. Governments occasionally publish reports on privacy management. However, the reader should be aware that there is much unpublished knowledge in the privacy management field, especially in CSCW and e-commerce contexts.

This survey paper also focuses primarily on end-users who employ personal applications, such as those used in telecommunications and e-commerce. We only partially consider applications in workplaces. However, perceived control of information is one of the elements of acceptance models such as Venkatesh et al.’s extension [289] of the Technology Acceptance Model [74]. Kraut et al. discuss similar acceptance issues in a CSCW context [183], pointing out that in addition to usefulness, critical mass and social influences affect the adoption of novel technologies.
References


References


References

References


References


References


References


[111] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, Design Patterns: Elements of Reusable Object-Oriented Software. p. 395, Addison-Wesley, 1995.


References


References


References


128 References


References


Full text available at: http://dx.doi.org/10.1561/1100000004
References


References


References


M/S Ilich and ashore at St. Petersburg, Russia: North-Holland, Amsterdam, August 12–17 1993.


References


References


[310] G. Wolf and A. Pfitzmann, “Empowering users to set their security goals,” in Multilateral Security in Communications Technology, Infrastructure, Econ-
References


