Chapter 3
Interpreting “You” and “Me”: Personal Voices, PII, Biometrics, and Imperfect/Perfect Electronic Memory in a Democracy

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT
Over a billion people are said to use the WWW and Internet, with 1 in 6 humans on earth accessing these technological systems. Many of these users have created their own personal profiles online, and all also have “silent information” about them that may be accessed on a variety of connected databases (including many on the Deep, Hidden, or Invisible Web). People use the WWW and Internet with a semblance of anonymity, but in fact, most interactions online are trackable to Personally Identifiable Information (PII), which allows for the revealing of the individual behind the photo, the video, the information, or other elements. Internet profiles may be coalesced into actual identities, even with inaccuracies, and such information may be kept in perfect electronic memory into perpetuity. This current reality has implications for citizens’ peace-of-mind and degrees of freedom in decision-making. This chapter offers an approach that may serve as a “forcing function” to propose limitations to the sharing of private information in public spaces.

INTRODUCTION
“You know, there could have been privacy, but people sell it. People sell their own privacy at such a low price that it’s remarkable” (Markus Jakobsson (Show 020—An Interview with Markus Jakobsson, The Silver Bullet Security Podcast with Gary McGraw, at http://www.cigital.com/silverbullet/page/6/), arguing that the selling of privacy creates current and future vulnerabilities that may compromise the individual).

We are anonymous, we are legion (Anonymous).
A slogan of a high-profile international hacker group.

DOI: 10.4018/978-1-4666-3637-8.ch003
Transparency is not an unadulterated virtue to be preferred without reflection over discretion, modesty, privacy, and tact (Brenner, 2011).

In open and democratic societies, the default is to err on the side of information release into the public because accurate information enables citizens to engage ideas, collaborate, and contribute to a civil society. Information that is to be protected must be specially marked out against sharing and embargoed. Even protected information is regularly hacked and leaked around the world via the Internet. In societies where free speech rights are de rigueur, many share with an unthinking speed—through microblogs (think real-time “Tweets”), social networking sites, blogs, wikis, political sites, text messaging, and email.

Many individuals are not showing the necessary oversight or restraint, and personal and private information and images are flooding public spaces. Many use the affordances of the World Wide Web (WWW) and Internet with a feeling of relative safety, given the high numbers of interactions online (safety in numbers) and maybe given their false sense of anonymity and security. Intrusions into protected systems are often invisible to users, and identity compromises are not revealed often times until financial accounts or other aspects of people’s identities are compromised. Finally, all these various channels of imperfect information may be preserved into potential perpetuity and made constantly searchable into the future over a range of distributed networks given the relative minimal cost of digital hosting. This leaves people living in an electronic panopticon where everything that they have ever done (documented by themselves and others) is potentially accessible and knowable and interpretable by others. This current state of the world promotes some aspects of democracy such as free speech, but individual and personal privacy (an essential part of human rights and the degrees of freedom in decision-making) is short-changed. When people release information about themselves, that can be used in ways both intended and unintended. Further, over time, much information that is shared becomes “forgotten data” (Nolan & Levesque, 2005, p. 34), but its potency remains because given its findability, it may appear in any number of future contexts.

To use the various services and affordances of the WWW and Internet, people are using socio-technical infrastructures that track Personally Identifiable Information (PII), information that can show a tie to the actual individual. “Silent information,” personal individual data that is harvested by others, may be read into to extrapolate understandings about people—such as the reading of a credit score to extrapolate whether a person is a good insurance risk or will follow through on difficult drug regimens or may be an effective employee. Any information that is collected is theoretically (and often practically) subject to compromise, leak, misinterpretation, and misuse. Wide dispersion of private information means a greater potential for mischief and criminology. The electronic environment is open to virtually all information and has an eternal memory. These factors make for a challenging environment for individuals to maintain a sense of privacy and the degrees of freedom to live an unsurveilled life.

Information that the state considers sensitive—by statute—includes health information. What is considered sensitive personal information may vary between cultures and individuals, with one extreme being cultures without even terminology about privacy and others with clearly defined protections against privacy infringements in various manifestations.

In a democracy, citizens (and people everywhere) are assumed to have a presumptive and innate human right to certain freedoms. They are considered to have a right to solitude—or to control their access to a personal space. They have a right to anonymity and secrecy in social interactions, and the right to control the collection and onward distribution of sensitive personal information. They have a right to free speech that does not cause harm. They have personal liber-
16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product’s webpage: www.igi-global.com/chapter/interpreting-you-personal-voicespii/74567?camid=4v1


Related Content

Service, Security, Transparency & Trust: Government Online or Governance Renewal in Canada?

Analysing Open Data in Virtual Research Environments: New Collaboration Opportunities to Improve Policy Making

Motives, Strategic Approach, Objectives & Focal Areas in e-Gov-Induced Change

User Attitudes to E-Government Citizen Services in Europe