

Chapter L

Emerging Technologies, Emerging Privacy Issues

Sue Conger
University of Dallas, USA

ABSTRACT

With each new technology, new ethical issues emerge that threaten both individual and household privacy. This chapter investigates issues relating to three emerging technologies—RFID chips, GPS, and smart motes—and the current and future impacts these technologies will have on society. The outcome will be issues for social discussion and resolution in the coming decades relating to use of these technologies.

BACKGROUND

New data losses of millions of individuals' personal information occur almost daily (Albrecht, 2002; Clarke, 1999; CNet, 2006). As losses amass, the realization grows that personal information privacy (PIP) is no longer managed by either individuals or the companies that collect the data. Research to date proposes that PIP is the responsibility of individuals' forging contracts with corporations for protection of their data (Smith, 2004), that it is the responsibility of government to protect the individual from corporate abuses (OECD, 2000, 2003, 2006; Swire, 1997), or the responsibility of corporations to manage internal use (Cheung et al., 2005; Culnan, 1993; Culnan & Armstrong, 1999; Smith et al. 1996). These

views are all corporate-centric but threats have expanded beyond the corporation to its data-sharing partners, resulting in data aggregation and sales that are largely unregulated and uncontrolled (Conger, 2006; Conger et al., 2005).

Dictionary.com has several definitions of privacy as shown in Table 1.

These definitions leave one with a clear expectation that individuals control their own physical visibility to the world. The legal definition further includes privacy in "personal matters."

Privacy can be thought of from several points of view (cf., OECD 1998; Smith 2004). On the one hand, the question is how the individual's inherent *right* to privacy can be protected, for example, by legislation. On the other hand, the individual has a *contractual* right of privacy, to

Table 1.

pri·va·cy (http://www.dictionary.com based on <i>Random House Unabridged Dictionary</i> , 2006)	<ol style="list-style-type: none"> 1. the state of being private; retirement or seclusion. 2. The state of being free from intrusion or disturbance in one's private life or affairs: <i>the right to privacy</i>. 3. SECRECY. 4. <i>Archaic</i>. a private place.
pri·va·cy <i>The American Heritage® Dictionary of the English Language, Fourth Edition</i> Copyright © 2000	<ol style="list-style-type: none"> 1. a. The quality or condition of being secluded from the presence or view of others. b. The state of being free from unsanctioned intrusion: <i>a person's right to privacy</i>. 2. The state of being concealed; secrecy.
pri·va·cy <i>WordNet® 2.1, © 2005 Princeton University</i>	<ol style="list-style-type: none"> 1. The quality of being secluded from the presence or view of others 2. The condition of being concealed or hidden
pri·va·cy <i>Merriam-Webster's Dictionary of Law, © 1996</i>	Freedom from unauthorized intrusion : state of being let alone and able to keep certain esp. personal matters to oneself—see also EXPECTATION OF PRIVACY, INVASION OF PRIVACY <i>privacy interest</i> at INTEREST 3b, RIGHT OF PRIVACY <i>Griswold v. Connecticut</i> and <i>Roe v. Wade</i> in the IMPORTANT CASES section
Privacy <i>Kernerman English Multilingual Dictionary, 2006</i>	The state of being away from other people's sight or interest Example: <i>in the privacy of your own home</i>

control interactions with the world, including the release of private information such as address and social security number.

In the past, privacy concerns were limited to protecting one's credit card, home, or mailbox from theft. Privacy research in the past focused on collection, unauthorized secondary use, ownership, accuracy, and access (Conger & Loch, 1995; Culnan, 1993; Culnan & Armstrong, 1999; Loch & Conger, 1996; Smith et al., 1996). Most research never stated what data was collected, or described a limited domain of data relating to a given transaction and demographics that oversimplifies breadth of data that might be collected (cf. Chen & Barnes, 2007; Cheung et al., 2005; Cheung & Lee, 2004/2005; Culnan and Armstrong, 1999; Doolin et al., 2005; Drennan et al., 2006).

Now, users of the Internet, worry that "personally revealing information about them is automatically generated, collected, stored, interconnected and put to a variety of uses." (OECD 1998, p. 11). To accommodate the changes enabled by Internet technologies, a more complete view of

the current state of PIP in business to consumer (B2C) transactions (see Figure 1) describes how an individual, the 1st party, comes to transact with a company, the 2nd party vendor/provider (Cheung, 2005, Conger et al., 2006).

Each unshaded box in Figure 1 and the arrows depicting the relationships between them represent areas in which significant research has already been conducted and incorporates the bodies of work summarized in Culnan and Armstrong (1999) and Cheung et al. (2005). Part of the individual's decision includes what data to provide to the 2nd party based on the expected life and use of that data, perceived reasonableness of the data collected, expected benefits, and expectations of corporate use of the collected data (Conger et al., 2005).

A decision to transact is based on an idiosyncratic evaluation of risk versus reward versus trust (Chen & Barnes, 2007; Dinev & Hart, 2006; Gallivan & Depledge, 2003; Geffen et al., 2003; Malhotra et al., 2004). Violate, or appear to violate, any of the decision factors and transactions will

25 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/emerging-technologies-emerging-privacy-issues/21617

Related Content

Giving Voice to Values: A New Perspective on Ethics in Globalised Organisational Environments

Mark G. Edwards, David A. Webb, Stacie Chappell and Mary C. Gentile (2012). *Ethical Models and Applications of Globalization: Cultural, Socio-Political and Economic Perspectives* (pp. 160-185).

www.irma-international.org/chapter/giving-voice-values/60426

Development and Psychometric Analysis of Cyber Ethics Instrument (CEI)

Winfred Yaokumah (2021). *International Journal of Technoethics* (pp. 54-74).

www.irma-international.org/article/development-and-psychometric-analysis-of-cyber-ethics-instrument-cei/269435

Improving the Ethical Dimension in the Innovation Process: Proposal for an Ethical Engineering Design Method

Robin Lecomte and Camille Jean (2022). *International Journal of Technoethics* (pp. 1-18).

www.irma-international.org/article/improving-the-ethical-dimension-in-the-innovation-process/302628

Moral Psychology and Information Ethics: Psychological Distance and the Components of Moral Behavior in a Digital World

Charles R. Crowell, Darcia Narvaez and Anna Gomberg (2005). *Information Ethics: Privacy and Intellectual Property* (pp. 19-37).

www.irma-international.org/chapter/moral-psychology-information-ethics/22937

The Ethics of Cyberweapons in Warfare

Neil C. Rowe (2010). *International Journal of Technoethics* (pp. 20-31).

www.irma-international.org/article/ethics-cyberweapons-warfare/39122