Chapter 1
Individual Privacy and Security in Virtual Worlds

Malu Roldan
San Jose State University, USA

Alan Rea
Western Michigan University, USA

ABSTRACT
The rapid growth in online usage has resulted in greater concerns about the privacy and security of users. These concerns are no less pertinent in virtual worlds where users often undertake virtual identities that stretch the boundaries of their real-world identities. These in-world personas may be detrimental to users’ careers and reputations should their in-world activities be linked to their real-world identities in digital dossiers. This chapter reviews and classifies privacy transgressions in virtual worlds and provides an overview of technological, behavioral and policy solutions to address these transgressions. The authors conclude with a discussion of the future research and multi-sector collaboration required to integrate disparate, emerging solutions into a federated security infrastructure for the Internet and virtual worlds. The current state of privacy solutions presents an opportunity for virtual worlds to attract more mainstream users as part of the ecosystem of organizations providing security services to online users.

INTRODUCTION
As with most other prominent platforms on the web, Virtual Worlds have become spaces where users face threats to their security and privacy. Recent high profile breaches underscore the poorly evolved nature of security and privacy technologies for use on the Internet and more specifically the virtual worlds that are hosted on it:

- In August 2009, a New York trial court granted a model an order that forced Google to reveal the identity of a person who was anonymously destroying her reputation via a blog. The model has reportedly forgiven the blogger but is considering filing suit for defamation (Reputation Whiz, 2009).
- In August 2009, users of top social media services like Twitter, Livejournal and Facebook experienced major service delays and interruptions as attackers sent
millions of junk messages to the services. These messages were sent to discredit and silence a blogger who was providing a controversial account of the territorial war between Russia and the Republic of Georgia. The attack surfaced deficiencies in the security infrastructure of the popular and relative newcomer Twitter service (Wortham & Kramer, 2009).

- Nearly half of all password-stealing Trojan software detected in 2008 targeted massive multiplayer online games like World of Warcraft, Everquest, and Lineage. The goal of such attacks is to steal in-game property and currency for resale on auction sites. A potentially lucrative activity as estimates in 2008 note a total in-game supply of cash and property in Asia at $4 billion! In response Blizzard Entertainment, Inc. (host of World and Warcraft) introduced an authenticator system in 2008 to allow its players to opt-in for stronger authentication protection.

- In September 2006, Linden Lab (the Second Life operator) reported on a data breach estimated to affect data associated with 650,000 accounts. Although Linden labs stated that the suspected hacker was after source code and currency used in Second Life, the breach exposed users’ personal data. In response, Linden Lab reset all user passwords, sent email notices of the change to all users, and moved more customer personal information (e.g. passwords, hashed credit card numbers, linden dollar balances) into a secure back-end vault (Lo, 2008).

- A “griefer” disrupted a presentation by one of second life’s top entrepreneurs in 2006. Ailin Graef’s presentation in CNET’s second life theatre by spamming the proceedings with bothersome virtual images (Terdiman, 2006).

These breaches are especially troubling in the Virtual World arena because many users consider these worlds as spaces where they can experiment and stretch definitions of their identities (Yee, n.d.). Hence, many users’ in world activities may be construed as exceeding the norms of acceptability in their everyday lives. Breaches could potentially expose these activities and cause damage to users’ reputations (among other things) across all arenas where they participate (Lo, 2008). Exacerbating these issues is the fact that Second Life’s Terms of Service require users establishing accounts to provide true and accurate information, to ensure that the user is a real person with legitimate, age-appropriate access to Second Life. However, this requirement prevents users from using pseudonyms and other methods for obscuring their real identities and breaking the link between their in world behaviors and their more traditional identities. This requirement facilitates the linkage of potentially non-traditional in world activities to real world identities (Lo, 2008). Second Life also does not allow users to tie multiple identities to a single login profile, thus preventing users from tailoring different avatars to various situations according to criteria such as privacy levels.

Classification of Privacy Violations

For this chapter, we are using the following definitions of privacy and security based on the work of Nath and King (2009)

Privacy transgressions include identity theft, unauthorized secondary use of data, physical and virtual stalking, and attacks, and IP Theft. Security constitutes the protections that an individual and/or organizations puts in place to prevent and remedy such transgressions.

Privacy researchers have proposed several classification schemes. There are several excellent listings of threats in the online space (Hogben, 2007) on which to base a classification scheme.