Economics of Identity Theft

Economics of Identity Theft:
Avoidance, Causes and Possible Cures

L. Jean Camp

Springer

L. Jean Camp
Indiana University
901 E. 10th St.
Bloomington, IN, USA
ljean@ljean.com

Library of Congress Control Number: 2007926498

Economics of Identity Theft by L. Jean Camp

ISBN-13: 978-0-387-68614-1 e-ISBN-13: 978-0-387-34589

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

To my parents, who contributed significantly to this identity.

List of Figures & Tables

List of Contributors

Elaine Newton, RAND

Bennet Yee, Google

Barbara Fox, Microsoft

Allan Friedman, Harvard University

Ari Schwartz, Center for Democracy and Technology

Preface

Anyone who has ever bought a car, rented an apartment, had a job or conversation that they would rather not see in their employee review may find this book of interest.

There is a collision occurring in identity management. Identity technologies are problematic, and many see light at the end of the identity theft tunnel. Yet the innovation is driven by individual tendencies to seek convenience and business imperatives to minimize risk with maximized profit. The light is an oncoming identity train wreck of maximum individual exposure, social risk and minimal privacy.

The primary debate over identity technologies is happening on the issue of centralization. RealID is effectively a centralized standard with a slightly distributed back-end (e.g., fifty servers). RealID is a national ID card. Many mechanisms for federated identities, such as OpenID or the Liberty Alliance, imagine a network of identifiers shared on an as-needed or ad-hoc process. These systems accept the limits of human information processing, and thus use models that work on paper. Using models that work on paper results in systematic risk of identity theft in this information economy.

There are alternatives to erosions of privacy and increasing fraud. There is an ideal where individuals have multiple devices, including computers, smart cards, and cell phones. Smart cards are credit card devices that are cryptographically secure. This may be shared and misused, or secure and privacy enhancing. Yet such a system requires coordinated investment.

There are strong near term incentives for low-privacy, cheap and thus technically flawed identity systems. The expense is now, and the risk of fraud is in the future. The immediate loss of privacy becomes a systematic loss in security over time. Just as convenient credit cards have become even more convenient for criminals with the advent on e-commerce, the foreseeable diffusion of mobile commerce and pervasive computing will break many of the proposed Federated or centralized identity systems. There are better choices.

This book is organized with four major components, each more focused than the last.

The book begins with a discussion about how the digital networked environment is critically different from the world of paper, eyeballs and pens. Many of the actual effective identity protections are embedded behind the eyeballs, where the presumably passive observer is actually a fairly keen student of human behavior. Even a passive clerk notices when a two hundred and fifty pound man presents Emily Sue's credit card.

The second section takes the observations about the profound divide between ink and bits, and applies that to the immediate problem of identity theft. Identity theft best practices are included; but the core observation is that the average person can do nothing to avoid exposure to this risk.

The third section looks at defining the problem of security in the context of identity. What is the problem? That question is followed by a view at the proposed answers.

After the overview of the technology and proposals for identity management comes a series of possible futures. Examination of these futures indicates that there are two choices: surveillance, near term profits, and long term fraud versus near term expense, private secure credentials, and long term stability.

Acknowledgments

I would like to acknowledge my excellent doctoral students, first and foremost: Allan Friedman, Warigia Bowman, Camilo Viecco, Debin Liu, and post doctoral fellow Alex Tsow.

I would like to acknowledge all the participants of that early identity workshop, where the idea for this book was born. The two-day workshop included public servants, technologists, policy analysts, and civil libertarians. The early publication from that workshop provided the clearest set of definitions, and thus clear thinking, that I have yet to see on this issue.

Also, Dave Farber whose *ip* list provided pointers to many of the anecdotes included in this book.

I would like to acknowledge my spouse, Shaun McDermott, the one without who so much would be infeasible, including finishing any bit of work. I would like to acknowledge my children, who are the joy and light of my life, just because.

Finally, I would like to thank my colleagues at Indiana University School of Informatics. While there remains debate about how to define an Informaticist, we can only hope that any who fit the final definition are such fine colleagues and coworkers.

Table of Contents