

When worlds collide

Managing privacy in joined-up service & payment environments

Human Services Delivery & Payment Reform
29 June 2010, Canberra

Stephen Wilson
Lockstep Group



Is privacy dead?

“People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time”

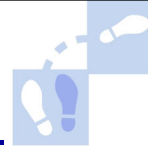
Mark Zuckerberg January 2010

Isn't it too early to draw reliable conclusions about changes in important societal norms like privacy?

Are the bosses of billion dollar dot-com businesses really authoritative in matters of social science?



Or are they selling something?



My considered view is that anyone who asserts that 'privacy is dead' is trying to sell something.

Zuck: Yeah so if you ever need info about anyone at Harvard, just ask. I have over 4,000 emails, pictures, addresses ...

[Friend]: What? How'd you manage that one?

Zuck: People just submitted it. I don't know why. They trust me. Dumb fks!**

Mark Zuckerberg 2004 (age 19)

This exchange between Mark Zuckerberg and a friend, very early in the development of Facebook, recently came to light, and has been cited by many commentators as evidence of contempt for members. But the more chilling aspect is the idea that Facebook data may be mined for the benefit of others unrelated to the members. This appears to be core to the Facebook business model.

Don't caricature the young



Is it true that young people have a more relaxed attitude to privacy? The operators of Social Networks make this claim often, and it suits their business purposes. Yet little research has actually been done on this point. This recent study suggests that we must not caricature young people.

***"The data show that [young adults] and older adults are more alike on many privacy topics than they are different ...
"Young-adult Americans have an aspiration for increased privacy even while they participate in an online reality optimized to increase revelation of personal data.
"Public policy agendas should therefore not start with the proposition that young adults do not care about privacy."***

HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES & POLICIES?
APRIL 14, 2010

"We suggest...that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data." (p. 144-145)

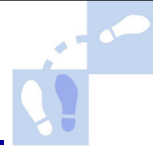
Chris Hoofnagle
UC Berkeley School of Law, Berkeley Center for Law and Technology

Jennifer King
UC Berkeley School of Information

Su Li
UC Berkeley School of Law, Center for the Study of Law and Society

Joseph Tunow
Annenberg School for Communication, University of Pennsylvania

Don't be simplistic about privacy



Privacy is too often casually derided. For example:

**“If you have something that you don't want anyone to know, maybe you should not be doing it in the first place”
Eric Schmidt (Google) December 2009.**

An excellent detailed rebuttal of that idea was written by academic lawyer Daniel Solove. He shows that privacy is more complex than wanting to hide one's embarrassments or mistakes. It's best not to be simplistic about why people value their privacy.

“I've Got Nothing to Hide” and Other Misunderstandings of Privacy

DANIEL J. SOLOVE*

TABLE OF CONTENTS

I. INTRODUCTION	745
II. THE “NOTHING TO HIDE” ARGUMENT	748
III. CONCEPTUALIZING PRIVACY	754
A. A Paralytic Conception of Privacy	754
B. The Social Value of Privacy	760
IV. THE PROBLEM WITH THE “NOTHING TO HIDE” ARGUMENT	764
A. Understanding the Many Dimensions of Privacy	764
B. Understanding Structural Problems	768
V. CONCLUSION	772

I. INTRODUCTION

Since the September 11 attacks, the government has been engaging in extensive surveillance and data mining. Regarding surveillance, in December 2005, the *New York Times* revealed that after September 11, the Bush Administration secretly authorized the National Security Administration (NSA) to engage in warrantless wiretapping of American citizens' telephone calls.¹ As for data mining, which involves analyzing

* © Daniel J. Solove 2007. Associate Professor, George Washington University Law School, J.D., Yale Law School. Thanks to Chris Hoofnagle, Adam Moore, and Michael Sullivan for helpful comments, and to my research assistant Shreem Shalkepoor. I develop some of the ideas in this essay in significantly more depth in my forthcoming book, *Understanding Privacy*, to be published by Harvard University Press in May 2008.

1. James Rosen & Eric Lipton, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, *N.Y. TIMES*, Dec. 16, 2005, at A1.

Privacy is frequently pitted as being at odds with ... utility (the usefulness of online systems is thought to be held back by privacy) or security or law enforcement. For example, Ed Giorgio, Office of the Director of National Intelligence, said “We have a saying in this business: Privacy and security are a zero-sum game” (*New Yorker*, 21 Jan 2008). This fatalism is politically expedient, intellectually lazy, and antagonistic to innovation, where there is real promise of attaining privacy and security at the same time.

Privacy



**Utility
Security
Counter-fraud**

What a wonderful joined up world

We use different digital identities (account numbers, user names, pseudonyms and handles) for different online services. Some of these are naturally amenable to being joined up, while most people would wish to keep some separate, such as role playing games, and personal health records.

A day in the digital life

- Internet banking
- E-commerce
- Employment
- Telecommuting
- Health information
- Education & Training
- E-Health Records
- Social security payments
- Tele consultation
- Medical OSN

Our digital lives are increasingly rich and important. Banking, commerce, travel and employment services were rapidly transformed by the Internet. There is strong evidence now that the ready availability of health information is impacting the relationship between patients and doctors (both positively and adversely). Tele consultation is joining patients and providers online, for better access and time management. One of the next frontiers in e-health is medical social networking and "apomediation" where patients access expertise in a more conversational setting. There are signs that online psychiatric counseling may sometimes be superior to traditional modes – but only if privacy is absolute.

Don't accept the premise!

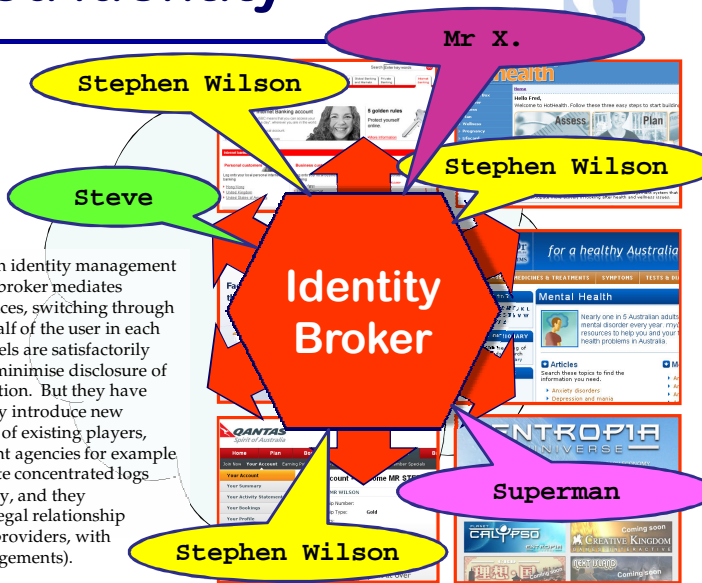


Innovative technologies mean that we don't need to accept the premise that privacy is at odds with security, utility and so on. Most people are familiar with the inherent privacy of their mobile devices, knowing that their data and transmissions are ordinarily protected (while there are well accepted and well regulated law enforcement related overrides). New smartcard implementations like the Queensland Driver License and smart student cards bring user-centric multiple applications. There is a lot to be said for a technology upgrade of the Medicare card, to open up online applications, and superior security and privacy.

Brokered identity



There are numerous modern identity management models where some sort of broker mediates connections to various services, switching through the right credentials on behalf of the user in each context. The brokered models are satisfactorily "user centric" and they do minimise disclosure of irrelevant personal information. But they have important downsides. They introduce new players (or change the roles of existing players, turning telcos or government agencies for example into ID brokers). They create concentrated logs (honeypots) of users' activity, and they fundamentally change the legal relationship between users and service providers, with complex new liability arrangements).



See also <http://lockstep.com.au/library/babysteps/babyste13-identity-silos>

Identity “in your pocket”

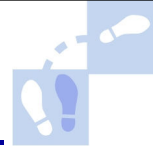
An even more powerful approach is to allow users to keep their diverse digital identities closer, exercising them independently via personal authentication services like smart phones and smartcards.

See also <http://lockstep.com.au/technologies/stepwise>

Progressive themes

- When did “silo” become a dirty word?
- Don’t accept the zero sum game default
- Drive service innovation for *utility* and not security per se
- Position technologies as agents of the individual – and not of the state

Respecting privacy



If authentication is what you
need to know about someone
to transact with them then ...

*What don't you need to know
about them?*

Discussion



www.lockstep.com.au

