6. Secrecy, Privacy, Identity

Phishing attacks are so profitable because they enable cascading failures. Online identity systems that are built upon concepts of papers and identification enable these cascading failures in part because such systems do not protect privacy.

Privacy, confidence and trust are about the distribution of power. Privacy offers me the ability to act freely, as a citizen, in my own home without my government or employer watching me. Privacy offers me the power to protect myself. Privacy also allows me to use illegal drugs or commit acts of violence in my home, despite government prohibition and employer chagrin. Privacy can enable harming others.

Privacy is violated only when identifying information is associated with other data. There are no privacy issues with anonymous grocery cards, not because with work and determination the shopper cannot be identified. There are not privacy concerns because the work required is so much higher than the value of the identifying information. There are not privacy concerns in inventory or tracking purchase correlations (e.g., giving out cat litter coupons upon the purchase of cat food). Privacy is only an issue when there is identity in a record, or when identity can be easily extracted from the record.

Yet privacy is double-edged sword. One person's privacy can reduce another person's autonomy. A classic use of privacy to control is described in "The Unwanted Gaze" where Rosen discusses the dual problems of privacy in sexual harassment. Sexual harassment investigations allow for intrusive investigations, against both claimants and those charged. Yet the lack of sexual harassment laws created a sphere of privacy that was used for abuse of power. The pundit O'Reilly had his secret sexual fantasies exposed when his producer played the tapes of his obscene phone calls. Powerful men demanded women's bodies for the women to keep their jobs. Exploitation of this type, called quid pro quo, is now not only illegal but widely socially condemned. Bragging about sleeping with a secretary is as contemptible as driving drunk – another change in social mores based on the balance between individual autonomy and the good of others. Yet the practices of exploitive sex in the workplace was an element of the existence of privacy, just like domestic violence and child abuse. The relationship between my privacy and your security is complex.

Indeed it was the sanctity of the family that prevented child abuse laws to the point where the first successful child abuse prosecution was under laws against cruelty to animals. (In 1874 animals were legally protected but children were not. In the case of the horribly abused Mary Ellen McCormack, the first successful child abuse prosecution in the United States, the judge

depended on cruelty to animal laws to sentence the mother to 1 year of prison. The next year the New York Society for the Prevention of Cruelty to Children was founded based on the model of the NY Society for the Prevention of Cruelty to Animals.) Child abuse laws were seen as invasions into the privacy of the family. Privacy can be the opposite of accountability. For example, Rosen defends a concept of privacy that is brutal. A perfectly private world risks being one where violence is never investigated, where identities can be snuffed out. Privacy that prevents a person from bearing witness to her own experiences does not create freedom. But privacy that makes every interaction recorded merchandise creates its own threats to freedom.

This balance in autonomy, the downside to privacy is widely heralded and embraced in discussions about security. No doubt children, though lacking full legal protection until age eighteen, are better off with child abuse laws than without them. No doubt the family that is wrongly accused might disagree, so the ability to accuse and investigate is tightly constrained.

Yet the balance between security and privacy is not so absolute. A lack of privacy can weaken security. Privacy cuts both ways in terms of security.

A lack of privacy can mean no autonomy. A life lived under surveillance is not a free life.

A lack of secrecy can mean a lack of security. Without privacy there is no secrecy. When all is exposed there are no secrets. Identity theft, phishing, and much computer crime, is enabled because there is no secrecy for the supposed private information. Indeed, an Illinois Appellate court has determined that sharing information, including names, addresses, and social security is not an invasion of privacy. The basis for the decision that cell phone companies can use subscriber information was that none of information shared (including - names, cell phone numbers, billing addresses, and social security numbers) were private facts. In this case, no privacy means no security. (Busse v. Motorola, Inc., 2004 Ill. App. LEXIS 738 (1st Dist. June 22, 2004))

Yet unlike secrecy (we all agree on the nature of a secret) there is great divide in people's perceptions of privacy. Age, gender, employment, and generally the person's place in the overall hierarchy effect their beliefs about the value and nature of privacy (Wilfords, 2002). Individual politics and belief systems alter our conceptions of privacy – a libertarian and a liberal have different views about government limits on business use of personal data. Yet both have the same understanding (albeit possibly different opinions) about classified or secret data.

The loss of privacy in the cases where security is decreased is deeply intertwined with identity and identity management.

On the surface, there is a seemingly inherent tradeoff between identity and privacy. Privacy-enhancing identity management is not an oxymoron. Privacy and ubiquitous ID systems can, together, serve to enhance individual autonomy. Of course, there is a conflict between the designer's desire to have