IDENTITY: THE HISTORIAN'S PERSPECTIVE

BY

TIMOTHY GRAYSON

History is not the same as the past is a truism revealed in a compulsory course during the honours year, well after dates and events have been dutifully memorized. This disenfranchised notion always comes as a shock. Every student eventually works through the calculus of time and accepts the impossibility of capturing the past fully and accurately in the limited space of historical narrative. Yet, to the devoted and dedicated, there is always the nagging desire to know everything and, as any historical biography will attest, eventually it is. In the fullness of time, everyone and everything is *outed*.

I bring forth this peculiarity of history not because of the first truism, but the second. The most extraordinarily well hidden parts of a life, including thoughts and plans, are no match for the forensic study of the diligent historian. Nor are those hidden treasures to be kept from the purposeful marketer. Today, the Internet environment has <permitted> masses of information to be

stockpiled, parsed, aggregated, cleansed, and minced – all to induce a bigger picture about the market. Most troubling to many is that it is being done to individuals specifically, a process called profiling. It creates a massive potential for privacy breech. It also has creates a need for valid and strong digital identity to provide certainty to digital transactions. These are not necessarily compatible issues.

Despite life being a continuum of risk, the choice of acceptable level in a circumstance being a personal (or corporate) matter weighed in a complex algebra of variables such as gain to be had, loss to be suffered, centrality and peripherality of the event, etc.), in this emerging digital identity space we are trying to invest what is essentially a sterile environment with personality. We are trying to do this because of the inherent impersonality of the virtual medium and our human need for contact and connection. We are attempting to inject an alternative to the very personal issue of judgment called trust that develops between two people. It is an essential substitute that will allow us collectively to have greater comfort with these impersonal interpersonal transactions, particularly as the risk profile of the transaction increases. That is obvious and, probably, valuable.

The problem is that the only way for the element of "trust" to develop is through *iteration* or *association*. The former mimics the physical world experience whereby one's comfort in another increases as a result of repeated interaction that creates a pattern upon which

we feel comfort basing a trust judgment. A trusting relationship is won over time. The latter is also a reflection of the real world experience we often refer to as referral or introduction. The aegis of comfort and trust between two parties is extended to a third by association. The new party begins the relationship with the presumption of trustworthiness and comfort by the party to whom (s)he is introduced. Even this latter relationship devolves to the iterative variety. But, because it starts at a higher plane, it has the effect of establishing that trust more rapidly – instantaneously, in some cases. In other words, the relationship is there to be lost not to be won.

In the digital identity space, the systemic problem with purely iterative approach (detached connection at best) is compounded by a transaction focus that typically can not wait for trust to develop. Or, stated another way, the problem is that online we expect to conduct a non-trivial transaction with an essentially unknown party in what is likely our first interaction without the benefit of temporal build-up of the relationship through iteration.[1] eBay, is an interesting proof of this premise: volume of activity, typically commencing with more trivial transactions, provide evidence of trustworthiness of the identity. Where the volume does not exist, alternate protections are often required for – larger – transactions (escrow, etc.). In other words, one buys respectability in small

[1] Certainty is also, of course, required as a means of validating or authenticating the person to be sure we are interacting with the person purported. There is a different set of complications here that we will address modestly herein, but which require their own larger space.

measures. As some have suggested, a similar, non-eBay means of addressing this problem is by providing a body of work, thought, activity, and information about oneself online and in a place/form available to others. Good but, still only a half-measure because there is the very real possibility that the published work is fiction.

The implication is then that surviving means for establishing identity and trust within the circumstances is by association in some form or another. Whether the association is with a credit provider (implying an additional financial protection for the other party), a credit bureau, an employer, government, or other corporate third party, digital identity provides value to the online transaction – at least initially – by association. The problem here, of course, is that in a broad, substantially unknown and unknowing, global environment, the value of the association is relevant if the third party is trusted and bears liability for the "introduction" and its association with the identity. For that to happen, the prudent organization will insist upon knowing who the person being identified is: conduct due diligence by proofing the person before issuing them a credential that the trusted third party will endorse. Of course, a paper trail develops.

But, despite the fact that there is *somebody* with more highly scrubbed information about the identity and the activities of the individual who is as susceptible to security compromise, even perfect protection of this digital identity has absolutely nothing to do with

privacy and protection of individual privacy. Remember, everyone is outed sooner or later.

The notion that digital identity programs will somehow protect and/or preserve privacy is spurious. At best, such mechanisms will afford the opportunity for non-trivial transactions conducted electronically to be informationally closed between the parties to the transaction: privity not privacy. The legal concept of privity is essentially that of having a "right to a closed interaction." For example, in a contractual dispute between you and me, your spouse will have no right to any claim. This concept may encompass some degree of privacy, <def'n>, but privacy is neither required nor assured. Again, by example, until the divorce and public relations attack, Jack Welch's parting bonus from GE was privacy, known only to those involved, and there is privity between GE and Welch. The privity remains; the privacy did not.

Privacy is the act of <description>. That can only be achieved by the actions and commitments of the parties involved. In an essentially open environment, such as the Internet and the information age in general, there are perhaps two small parts of the privacy issue addressable by digital identity. First, the certainty that in the creation of a "private" transaction, the "right" parties are participating and committing. Second, that after the information about the transaction exists, only those parties with legal right or authorization to become aware of it indeed gain access. Notably, both of these are measures which have less to do with privacy than

with authenticity. The post-fact value of digital identity relative to privacy then becomes the prevention of unauthorized access. While this is important, it is not the most significant part of privacy. It is, in fact, a simple security issue. (And, in this respect, digital identity is an essential element of the "open" networked world.)

[Note: anonymity is NOT privacy because where there is anonymity privacy exists solely within the "actor" so no breach that could be prevented by digital identity is relevant; only the actor can *actively* compromise the privacy. By extension any measure that seeks to emulate anonymity (i.e., pseudonymity, "real" id detached) falls into the same class. Privacy is about opacity: keeping information either hidden or separated so that knowledge can not be gained. It is a matter of degrees and context as well. Almost all information is distributed to someone; privacy is in the selectivity of the sharing.]

Digital identity tools, structures, and process have limited impact on privacy because they comprise such a minor part of the overall ____ of privacy, one that ultimately comes down to how well two parties keep a secret. It is obvious, in the general consideration of privacy, that we are concerned with keeping information secret. And secrets can be found out and deduced in a number of ways. The can be stolen, intercepted, coerced, induced, deduced, and hypothesized.

Historians, who are essentially investigators and information interpreters, eventually "get" the private goods by diligently hunting for scraps of data and correlating them into a coherent story. Historians have the luxury of the fullness of time to access sources that police and the information infiltrator do not have. Where there is information there is room for interpretation.

So much information is available – everywhere – that the notion of creating privacy about ourselves online becomes almost laughable. It would be a conceit as bold and unrealistic as the revolutionary idea of wiping clean the social slate and starting anew after the overthrow. The genie is out of the bottle. Much conspires to prevent the idealized notion of privacy (the "I am master of my information and none will breach my desires" idea) from being more than a false shadow. Consider the wealth of data already housed in the information stores of corporate CRM files, loyalty programs, credit bureaus, public record, and so forth. Will it disappear or be destroyed? Will its holders and users cease to use it?

[Privacy resides in the actions of those accessing the information. It's naïve to presume that some of these receivers will not use the data in a way that either compromises it or leads to its compromise. We – the "owners" of the private information – are unthinkingly responsible for the problem. How often do we distribute little slices of private information in innocuous ways – for some benefit – thinking, "I don't care if somebody knows that."? Individually information items *d*, *a*, *m*, and *n* cause us no fear, even

if we've distributed them fairly widely at different times. Only when they become *damn*-ing, together, do we become protective and concerned. And, digital identity will have only a minor decelerating effect on the privacy problem.

One of the many examples of the type of non-official (i.e., non-government activities and services that make a mockery of privacy is Siesent. This business's inexpensive online service prepares dossiers on subject persons rapidly and thoroughly. It sources and correlates data from multitudes of place, making inductive "conclusions" on certain combinations of or relations between data in disparate storehouses. It literally creates knowledge from information and raw data. That is scary. And, it will not go away with the implementation of digital identity programs. So, . . .

Dig ID addresses the matter of certainty – perhaps, and may go some way to contain the personal information used and provided in the context of the obtaining of the ID. It does not solve the privacy problem though. Everything is outed eventually, and in the case of ID that happens as a result of the spillage/slippage outside the ID context. No matter how hard one attempts to hold the information private and sacred, personal information can be inferred and is distributed to many places many times.

XXX

Timothy Grayson is part of the eBusiness group at Canada Post Corporation, in Ottawa. He is the author of "Every Canadian's Guide to Common Contracts" published by HarperCollins. grayson@templar.ca

©2003, Timothy Grayson