Michael Dumlao
Distribution Paper
CCTP 505

THE MARKET OF IDENTITY: FINDING THE AUTHENTIC SELF

In Jeffrey Rosen's post-9/11 world of the Omnipticon (as described in his book "The Naked Crowd"), the crowd subjects itself to perpetual scrutiny- drawing on a collective belief in the authentication of identity as the predication of trust and fundamental security.[1] Whether one considers physically invasive biometric technologies or the less tactile but globally accessible divulgence of self through online journals ("blogs") and dating profiles, in the "Age of Authenticity," there is great pressure to "Be Thyself."[2] However, while there is increasing pressure for Industries to meet Institutional demands for authenticity, Industries in turn confine an Institution's cultural evolution within codes of conduct instructed by the very *codes* of technology. As Rosen mentions, "technologies, left to their own devices, are indifferent about the balance between liberty and security" and therefore need a forum for a reciprocal exchange of influence between Industry (for example, biotech companies and software developers) and Institutions (cultural frameworks and government).[3]

Meeting this need is the Market of Identity, hereby defined as a system of trade (and trade-offs) that nurtures Industry to develop tools that govern how consumers verify identity while allowing governing Institutions and emerging cultural norms to dictate the architecture of security technology. Drawing parallels between the privacy/ security discussion surrounding biometrics and the ever-growing use of online networks such as

[1] Jeffrey Rosen, *The Naked Crowd* (New York: Random House, 2004) 162
[2] Rosen, 174
[3] Rosen, 101

"Friendster" and *"Match.com,"* I argue that through nurturing technological innovation, the Market of Identity helps consumers understand the ever-evolving nature of the representations of "self" in the Age of (In)Security.

As Rosen mentions, " …citizens in a risk society can no longer rely on tradition or fixed hierarchies to establish their identity or give them reliable guidance about whom to trust in a society of strangers."[4] While one can easily argue that today's consumers are empowered by a greater sense of agency and are not as inhibited by family or heredity in their social movements, as Johnson points out, "there has to be feedback between agents."[5] Much like cells of the human body, society functions through an intrinsic reciprocation of influence between neighbors who dictate how others behave through observation.[6] From the time of eighteenth-century class-based honor systems of social stratification to the Jacksonian age of the "cult of sincerity" where citizens were subject to a strict conduct code of disclosure, members of society often base their individual identities in relation to others in one way or another.[7] While Alexis de Tocqueville observed that the absence of hierarchy in egalitarian societies breeds anxieties about one's perpetually shifting status, even in the security-obsessed "Age of Code Orange," individuals are still seeking to connect with each other, however different the new rules for *how* to connect have become.[8]

Let us consider the behavioral requisites of this presumed "Age of Disclosure." From the aforementioned Jacksonian cult of sincerity, citizens (and later consumers) have managed a precarious balance between authentication and personal security. Reveal too

[4] Rosen, 162
[5] Steven Johnson, *Emergence* (New York: Touchstone, 2002) 96
[6] Johnson, 86
[7] Rosen, 172

little and a person is subject to dismissal or suspicion; reveal too much and they are vulnerable to chicanery; reveal the right amount and the person has proven that they are worthy of trust and not a threat. If trust is one of the base elements of trade in a Market forum, "people try to prove their trustworthiness by revealing details of their personal lives to prove that they have nothing to hide before a crowd whose gaze is turned increasingly on all the individuals that compose it"[9] From the tragedy of 9/11 society has learned that mere visual cues are not enough to discern reliability (terrorists, after all, have learned to adopt ubiquitous personas that blend-in and assimilate). Self-revelation now serves as a pass-key for connection with others, and Markets of Identity have allowed Industry to develop technologies as scientifically complex as face-recognition to ones as seemingly innocuous as online encrypted password protections to provide entry into society through that monolithic door of trust.

Verifying identity and passing through that door, however, is a function of how people can best represent themselves to ensure the aforementioned balance between disclosure and vulnerability. Rosen offers the concept of Personal Branding, which borrows from the advertising strategy of selling goods by embodying products with carefully crafted and consistently broadcasted emotive qualities of worth and salience in an effort to build consumer loyalty and ensure recurring patronage.[10] In the Market of Identity, the answer to the question of *who* one *is* is frequently answered by an abstraction of a more complex personal reality: credit histories reveal spending patterns, but not the motivation behind purchases; mileage points display the frequency of travel

[8] Rosen, 172
[9] Rosen, 163
[10] Rosen, 176

but can never narrate the experience of exploration; and online dating profiles, while becoming increasingly accommodating to the varying degrees of detail one can choose in revealing him or herself, still offer an abstract representation that can never supplant face-to-face interaction. Recalling Rosen's Omnipticon, members of the Market of Identity have become globally consumable consumers, able to and often willing to be scrutinized and judged by others to achieve connection and social validity.

The brand is a "trust mark" that connects the product (or person) with carefully pre-designed emotive associations.[11] To be effective, brands have to be simple and direct, acknowledging a peer's short attention span and the general public's inability to comprehend nor immediately embrace the full complexity of a stranger vying for their trust. Reincarnating the eighteenth century's rules of caste and social hierarchies, human beings eschew considerations for "product ingredients" for a more convenient and efficient system of codes of representation that allow for a greater immediacy in consumption. Buyers imbue brands with a trust based on favorable prior experiences, and are often willing to forego reviewing content labels as long as the experience remains constant. Hence the governing law that brands must remain consistent and direct; maintenance of this brand "requires a degree of self-discipline rather than unregulated self-exposure." [12]

Online dating services and "hook-up" sites such as "*Match.com"* or "*E-Harmony"* flourish because they create a more efficient Market of exchange between prospective partners. By eliminating profiles with irrelevant characteristics and allowing users to focus only on those with mutually desirable traits, internet dating offers the

[11] Rosen, 178

potential for a more effective method of pursuit. However, in building one's online avatar, the laws of branding still apply: even with the inclusion of photos (which are never fully indicative of how a user actually appears in person) and a cacophony of disclosure that can reveal anything from career histories, musical preferences to sexual proclivities, it is consistency, simplification and honesty that ensure brand loyalty and return patronage (i.e., the second date).

"*Friendster,"* arguably one of the most successful online social networks in recent memory, functions on the belief that strangers with existing interpersonal connections (however detached) make better partners and associates based on the trust that existing peers have already afforded them. One cannot be included in a "social circle" unless the primary member of that community verifies that the newcomer is indeed a friend. By limiting membership and offering rigid parameters of control, *"Friendster"* becomes a system of verification. It eases, for example, the issue of validating what are often dubious claims of "slim, athletic figures" or "interests in the arts and romantic walks on the beach" by giving users pre-existing social networks with which to check such assertions. The ubiquity of this "six-degrees-of-separation" system of networking proves that trust still predicates social interaction, even if friendships are tenuous at best and our assumptions are based on online profiles that are still carefully selected abstractions of self.

Biometric technologies function on this very notion of authentication through selective representations of identity. Voice recognition systems, closed-circuit television, facial scans and fingerprint verification technologies all promise to provide credible

[12] Rosen, 181

though context-free authentication of identity upon which is based pre-conditioned criteria for determining whether one is a threat or friend to society. West Coast code (as embodied by HNC Software and other internet development companies), bereft of capital and resources after the dot-com plummet, answered the East Coast code's (government's) claims of increased security threat and produced a portfolio of protective devices that have proven to help citizens *feel* more secure despite trade-offs in civil liberties and personal privacy.[13]

The rewards for meeting consumer needs for enhanced security are as palpable as the consequences for not doing so (as demonstrated by Mad Cow's effects on the eleven percent drop in beef consumption across the European Union and the subsequent four billion pound loss to the British economy).[14] This is clearly demonstrated by the Oracle Corporation's meteoric rise in profit value; in battling urban gang war-fare in Chicago, Oracle consolidated disparate databases and networked previously disconnected information patterns (such as crime, weather, property value and gun ownership), to create adequate abstractions of identity that could predict behavior.[15] By focusing on patterns rather than individuals, one can argue that privacy remained intact; however, because law enforcement is primarily interested in apprehension rather than mere prediction, convictions based on select elements rather than the full circumstances of an individual still leads to a violation of liberties.

In the context of a culture of security, the Market of Identity produces technology that answers said cultural concerns; however, as demonstrated by the proliferation of

[13] Rosen, 102
[14] Rosen, 86
[15] Rosen, 111

public surveillance in England, there also lies a very possible scenario where technology (and the Industry of Security that produces it) demonstrates the power to modify culture and therefore affect identity.[16] "The crowd's unrealistic demand for a zero-risk society is related to its anxieties about identity," and as such has made itself willing to alter behaviors and identities to suit subsequent losses in privacy and liberty.[17] Under a culture of perpetual scrutiny, communities in Britain have willingly succumbed to a near-omnipotent system of closed-circuit cameras, thereby assuming that "if you've got nothing to hide, you've got nothing to fear."[18] But while terrorists themselves have not been apprehended, nor have their plans been ascertained or thwarted, low-level criminals have been caught, creating a public illusion that surveillance breeds security where in actuality in merely forces greater threats into more hidden methods of operation. With the proposed inclusion of universal face recognition systems that can connect all citizens with databases of past criminal activity (however trivial), increased erroneous connection between say, unpaid parking tickets and complicity in terrorist acts indicates the dangers of exclusive reliance on abstractions of identity rather than interpersonal affiliation.

According to Oracle, "at one corner is privacy, at one corner is assurance of security… and at another corner is usability. It's all a matter of trade-offs."[19] In the parable of the Blog and Naked Machine, Rosen offers a choice between technologies that offer a balance between ensuring security while protecting privacy (the Blog Machine, which obscures physical traits while scanning for specific, suspicious articles) or that disregard privacy altogether in the interest of unwavering assurance of safety (the Naked

[16] Rosen, 32
[17] Rosen, 31
[18] Rosen, 36
[19] Rosen, 111

Machine, which obscures nothing and reveals everything).[20] While it may appear at first that the Blog machine would be the preferable choice, Rosen asserts that, in actuality, it is the Naked Machine that captures the majority vote. Confronted by the prospect of another 9/11, consumers have opted for the no-excuses approach, offering their identities in full context to undergo scrutiny. Perhaps it is "the reluctance of the public to make nuanced judgments in the face of remote threat (that) has made it hard to find a market for well-design technologies that protect liberty and security at the same time."[21] Or, in considering the constraints offered by the Personal Brand, the public has opted for the ultimate convenience of full disclosure.

Similar to our online chat profiles, the Blog Machine is a Personal Brand that protects flaws but forces us to select a consistent arsenal of traits to display to obtain that ever-desired verification of trust. There is a measure of personal constraint, especially if one *does* have something to hide, to make sure undesirable traits are concealed and only select elements of self are disclosed. The Naked Machine, however, implies open divulgence. It is easier and desirable because it absolves people from the pressures of "self-branding" and (when everyone is "naked") offers immediate connection without compromise of security or threat of "exposure." Like the British CCTV, the Naked Machine offers an illusion of egalitarian security because everyone is being watched.

Like the sidewalks described by Steven Johnson in "Emergence," the Market of Identity facilitates interpersonal communication, knowledge sharing and collective interdependence amongst its consumers and vendors. Underlying this forum for exchange is a level of trust, the acquisition of which, in the post-9/11 Age of Security, Authenticity

[20] Rosen, 4

and Disclosure, is governed by a set of rules that lie on the precarious balance between security and civil liberty. However, navigating these rules is a function of an inherent social need to connect with others despite the risks - a task that requires problematic considerations for how one should represent "self" in a time when that vital access to community is predicated on maintaining the right Personal Brand. When identity is based on market abstractions, the question of "who am I?" becomes "who should I be online" or "what *don't* I take to the airport?" In the battle between security and privacy, it is an offered hope that in the dialogue between technology and consumer behavior (between Industry and "I") the self will be regained.

BIBLIOGRAPHY

1) Steven Johnson, *Emergence: The Connected Lives of Ants, Brains Cities and Software*, New York: Touchstone Books, 2002
2) Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, New York: Random House, 2004

[21] Rosen, 91