The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web

Daniel A. Caeton

*Bulletin of Science Technology Society* 2007; 27; 11
DOI: 10.1177/0270467606297624

The online version of this article can be found at:
http://bst.sagepub.com/cgi/content/abstract/27/1/11

Published by:

http://www.sagepublications.com

On behalf of:

National Association for Science, Technology & Society

Additional services and information for *Bulletin of Science, Technology & Society* can be found at:

Email Alerts: http://bst.sagepub.com/cgi/alerts

Subscriptions: http://bst.sagepub.com/subscriptions

Reprints: http://www.sagepub.com/journalsReprints.nav

Permissions: http://www.sagepub.com/journalsPermissions.nav

Citations http://bst.sagepub.com/cgi/content/refs/27/1/11
The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web

Daniel A. Caeton
Fresno State University, USA

Through a critique of the rhetorical configurations of identity theft, this article contributes to the emerging body of theory contending with the social effects of digital information technologies (DIT). It demonstrates how the politics of fear manipulate technosocial matrices in order to derive consent for radical changes such as the domestication of the Web and the instrumentalization of identity. Specifically, this critique attends to these tasks by performing a rhetorical reading of three recent television commercials that were heavily circulated by the international financial conglomerate, Citigroup Incorporated. Based on this reading, which is heavily indebted to Foucauldian theories of power and discipline, a distinction is drawn between identity theft as it is configured in juridico-political discourse and the cultural phenomenon of identity theft, which functions as a technosocial myth.

Keywords: identity theft; myth; World Wide Web; cultural phenomenon; technosocial; digital information technologies

In a terrific amount of academic and popular analyses during the past two decades, the rise of new media such as digital information technologies (DIT) has been acclaimed for exhibiting the potential to transcend the political and social constraints that stymie industrialized societies. Indeed, an astonishing array of technologists and cultural critics alike have seized on the contemporary kairotic moment as an episode in social history when, owing to the advent of DIT resources such as the World Wide Web (hereafter referred to simply as the Web), boundaries, fetters, and borders will be reconfigured and notions of progress will no longer be tainted with irony. This conviction has led Miller (1991), a deconstructionist literary theorist, to note that “these technologies are inherently democratic and transnational. They will help create new and hitherto unimagined forms of democracy, political involvement, obligation, and power” (p. 20). Thus, for many the proliferation and integration of DIT into the experiences of daily life has kindled new hope for the possible amelioration of the stratifying inequities existent in industrial and postindustrial societies. At the same time, though, other far less halcyon visions of DIT have circulated in academic and public discourse. These alarming versions typically depict DIT’s effects as hostile to democratic values such as the ethics of the free market and the insolubility of the rational individual.

From this perspective, the Web is a lawless domain hostile to the both the rule of law and bourgeois morality. This dichotomy is indicative of the ways that DIT continues to unsettle and disturb established technosocial relationships. The meanings of these developments are still being contested so that decades after the emergence of DIT, we have yet to satisfactorily answer the question, “What should we make of computers, and what will they make of us?”

Thus, this critique seeks to contribute to the growing corpus of scholarship dealing with the social impacts of DIT by contending that the cultural role of identity theft along with the ubiquity of advertisements from companies assuring protection against identity theft are indicative of a shift in the cultural position of the Web. Although many might initially be tempted to dismiss identity theft as a tangential issue, I hold that an exploration of the rhetorical potency of identity theft is paramount to an understanding of how DIT resources can reconfigure technosocial relations. Through an analysis of identity theft, we can come to appreciate how the politics of fear manipulate the technosocial matrix to derive consent for radical changes such as the domestication of the Web and the instrumentalization of identity. In particular, I attend to these tasks by performing
a rhetorical reading of three recent television commercials that were commissioned and heavily circulated by the international financial conglomerate Citigroup Incorporated. In doing so, I adhere to the premise that if, as Citigroup’s commercials would have it, the Web is a contested zone, then the scrimmage occurring is not one between thieves and consumers, but rather, it is between the hegemony of late capitalism and the radical possibilities engendered by DIT.

What follows then is not an argument against the recognition of identity theft by governing bodies as a legitimate criminal activity. This critique, rather, demonstrates how the creation of identity theft in juridico-political discourse establishes a foundation for the instrumentalization of individuals by translating them from citizens into consumers, while simultaneously promoting consumer confidence in the security of the commercial aspects of DIT resources such as the Web. Moreover, commercial bureaucrats such as Citigroup embellish on the legal foundation of identity theft to translate it into a cultural phenomenon. By drawing on the work of Barthes (1982) and others, this critique demonstrates how the cultural phenomenon of identity theft operates mythically. It is important to clarify at this point that by claiming identity theft is mythical, this critique is not equating it with a fairy tale or some other type of fabrication. Identity theft assumes mythical status in the technical sense, which is to say that it is based on material relationships that are themselves rhetorically distorted so that they become obscured. Thus, the cultural phenomenon of identity theft—which is related to, yet distinct from, the legal codification of identity theft—can, like any myth, be deployed to promote ideological ends and contour technosocial relations. Working in conjunction, then, the legal codification of identity theft and the cultural phenomenon of identity theft transform cyberspace into what Foucault (1979) has termed to be “disciplinary space” and “analytical space” (p. 143). The specific purposes of these manufactured spaces, according to Foucault, were to ascertain “where and how to locate individuals, to set up useful communications, to interrupt others, to be at each moment to supervise the conduct of each individual, to assess it, to judge it, [and] to calculate its qualities or merits” (p. 143).

Based on that premise, this critique demonstrates how three of Citigroup’s commercials—Saddlebags, Babe Magnet, and Geek—are illustrative of how identity theft is deployed as a means of both domesticating DIT resources such as the Web so that they become more efficient virtual markets and instrumentalizing individuals into reliable consumers by reducing their online identities to easily manipulable data. Citigroup’s advertisements are, to be sure, very clever, but this cleverness belies their rhetorical efficacy to transform identity as it is enacted on the Web into an index of quantifiable data such as social security numbers, birth dates, credit ratings, and purchasing habits. The cultural phenomenon of identity theft improves the ability of corporate bureaucracies such as Citigroup to successfully “make people accessible to computers” (Porter, 2000, p. 44, emphasis original). This process is largely occluded, however, by the underlying message of the advertising campaign, which erroneously perpetuates the idea that crime on the Web results from individual deviance rather than from the enormous corporate and government bureaucracies that themselves promote the quantifiability of identity. In this way, the myth of identity theft serves to rearrange power dynamics by creating a threat while simultaneously promoting a spurious solution to the threat.

**Threat Assessment**

For many, the threat posed to both liberal democracies and market economies by unregulated DIT has come to be realized in the form of identity theft. Curiously, the scope of identity theft is both great and narrow, for it involves equally the massive institutions of multinational capitalism and the comparably smaller affairs of individual citizens. This danger, the argument goes, occurs when criminality and technology intersect; it is a larceny of selfhood enabled, and perhaps encouraged by, a growing cultural dependence on DIT. So because of the advanced DIT resources that power the Web, what was once classified as fraud has been transformed into the pernicious crime of identity theft. Although crimes involving unlawful impersonation and credit fraud have been committed and prosecuted for some time, it has only been in the past few years that identity theft has attained its current meaning. As the phrase *identity theft* indicates, what is at stake is not merely property but rather the intimate information that qualifies an individual for recognition by the institutional infrastructure that undergirds the public and private realms of contemporary society. In this way, identity theft reveals the twin impulses to reduce individuals to easily stored collections of data and to streamline DIT into an efficient means for storing, synthesizing, and monitoring these data.

Of course, this is not a nightmarish science fiction scenario, nor is it a paranoid conspiracy theory. It is instead the reality of how commercial activity and
information management cohabitate on the Web, because unlike in the terrestrial world where nearly every object can be commodified, the only thing that is subject to commodification in the virtual world is information. Hayles (1999) pointed out that these shifts disrupt the means through which commodities are defined and regulated. Accordingly, Hayles surmised that information is not a materially conserved quantity. When I copy information from my disk to yours, we both have it. The crucial issue with information is thus not possession but access. Access has already become a focal point for questions about how information as a commodity is going to be integrated into existing capitalist structures. (p. 78)

Put another way, information, by virtue of its instantaneous reproducibility, its intangibility, and its inability to be consumed, disrupts the methods for commodification that are practiced on material objects. Poster (2001) has corroborated the problematic of the commodification of information:

The issue of commodification also affords a narrow focus, often restricting the discussion of the politics of the Internet to the question of which corporation or which type of corporation will be able to obtain what amount of income from which configuration of the Internet. (p. 172)

Clearly, what is entailed by the shift in emphasis from materiality to information is an incompatibility with the organizational schemes of the State and the business as usual of corporate entities. Moreover, depending on how information is construed, it can allow for new forms of identity formation liberated from material constraints, or it can instrumentalize identity by reducing it to easily quantified sets of data.

To this end, the formulation of crimes such as identity theft in juridico-political discourse can foreclose the novel opportunities for liberation that DIT offers. For Lessig (1999, 2004), an accomplished legal theorist whose work has dealt with intellectual property law and cyberlaw, the Web is not inherently liberating or democratizing, though if configured properly, it can promote those effects. The pivotal point for Lessig is not what DIT is in and of itself but instead how DIT is administered by the rule of law in a given society. Borrowing a trope from Adam Smith, Lessig (1999) wrote that the “invisible hand of cyberspace” is currently molding a version of the Web “that is quite the opposite of what it was at cyberspace’s birth” (p. 6). He proceeded to claim that this “invisible hand, through commerce, is constructing an architecture that perfects control—an architecture that makes possible highly efficient regulation” (p. 6). According to Lessig (2004), institutions whose dominance is jeopardized by DIT’s potential “to change the way both commercial and noncommercial culture are made and shared have united to induce lawmakers to use the law to protect them” (p. 9). “They are,” he wrote, “succeeding in their plans to remake the Internet before the Internet remakes them” (p. 9). Although Lessig might have oversimplified things a bit by assigning such clear motives and agendas to those entities that feel threatened, his point that juridico-political discourse has been used to promote a specific version of the Web is an important addition to our understanding of the role that identity theft plays in reconfiguring technosocial relations. For the issue has never been whether DIT should exist but rather how it should exist and for what purpose. Identity theft legislation, as we shall see, lays the foundation for the cultural phenomenon of identity theft—or what I have elsewhere called the myth of identity theft—which itself acts as a robust instrument for both rationalizing the Web and operationalizing identity.

Ostensibly meaning to protect the stability of established institutions as well as the agency of individual citizens, the Congress of the United States passed Public Law 105-318, known informally as the Identity Theft and Assumption Deterrence Act of 1998, on October 30, 1998. Six years later, on April 10, 2003, the Identity Theft Penalty Enhancement Act, an amendment meant to strengthen Public Law 105-318, was introduced to the American House of Representatives. The bill, which had been sponsored by Rep. John R. Carter, was subsequently passed by the Senate and became Public Law 108-275 on July 15, 2004. Among the many important aspects of identity theft codified and criminalized in Public Law 105-318, perhaps the most salient for this critique is the definition that it provided for “means of identification.” In addition to routine pieces of data such as social security numbers, taxpayer identification numbers, and date of birth, which are used to authenticate an individual’s identity, the law also detailed less conventional means of identification. For example in subsection (d) of Section 003, the means of identification are also extended to include “unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation.” Clearly, this demonstrates the level of discipline that is possible with advanced DIT systems, for unlike social security numbers, taxpayer identification numbers, and birth dates, which are all numerical
designations that emanate from information systems, forms of biometric data represent a push to transform the whole body into information. It may be easy for skeptics to question how a social security number truly relates to an individual’s identity, but it is more difficult to question how the reduction of corporeality to a data set does not entail the erosion of identity.

Taken together, then, this legislation demonstrates the intimate connections between power and information and how these connections exacerbate the climate of fear surrounding DIT. Although it might be argued that Public Laws 105-318 and 108-275 were passed with the intention of deterring identity theft, it is equally important to consider that this legislation promoted the idea of identity theft. In other words, they grouped together and gave a singular name to a host of crimes that had already been criminalized. And although the phrase identity theft certainly preceded the enactment of Public Law 105-318, this phrase was elevated to a new stature once it had been acknowledged and its name had been sanctioned by an official body of governance. By criminalizing identity theft, the emphasis shifted from whether the commodification of information was reasonable to whether the public was reasonably protected against infractions against this new form of commodification. To put a finer point on things, the juridico-political discourse surrounding identity theft reinforced a climate of fear that made the smooth functioning of the reductive system of information seem all the more dear.

Furthermore, the juridico-political conceptions of identity theft act as discursive legerdemain whereby perpetrators of identity theft are believed to be predatory, deviant individuals rather than the clumsy bureaucracies that store and manipulate vast quantities of consumer data. The image created is of a lone criminal who paradoxically has the expertise to navigate and manipulate advanced DIT resources for illicit gain but who is still willing to dig through an individual’s trash to obtain personal information. So citizens who might otherwise question the wisdom of reducing identity to quantifiable information, which then is concentrated in the hands of a few massive bureaucracies, are instead preoccupied with shredding their paper waste before disposing of it. Through this paradox, it becomes possible to understand how the juridico-political discourse promotes specific ideological conceptions of identity theft. For as Althusser (1972) noted,

It is not their real conditions of existence, their real world, that “men” “represent to themselves” in ideology, but above all it is their relation to those conditions of existence which is represented to them there. It is this relation which is at the centre of every ideological, i.e. imaginary, representation of the real world. (p. 164)

Thus, the codification of identity theft in juridico-political discourse occludes the sum total of material and social dynamics that converge in identity theft. Instead, it represents a specific version of identity theft, one that ignores the system of identity instrumentalization and DIT operationalization in favor of a one-to-one interaction between criminals and victims. Despite this image of identity theft in American law, there are countless examples of identity theft that undermine such an ideological representation. In fact, three of the most egregious examples of identity theft or potential identity theft in the United States have occurred because of bureaucratic negligence. Even more telling, two of the three instances occurred after the passage of both Public Law 105-318 and Public Law 108-275.

The first case, which happened in December 2004, involved the loss of data tapes by Bank of America Corporation containing the personal account information of more than 1.2 million U.S. federal employees. Among those affected were hundreds of thousands of civilian and military employees of the Department of Defense, as well as many members of the U.S. Senate. Compounding the problem even further, the corporation did not publicly acknowledge the loss or notify all of the individuals affected until February 25, 2005.

The second example involved the theft of a laptop from a University of California, Berkeley, employee. The crime took place on March 11, 2005, and it exposed the personal details of more than 98,000 students and alumni. In this case, the stolen laptop was recovered after it had been purchased on an eBay auction, but forensic analysis revealed that the hard drive had been reformatted at some point during the laptop’s disappearance. It came to light during the investigation that the laptop had been through a network of criminal hands, as it had been sold to the eBay bidder by someone other than the person who originally stole it from the university’s campus.

Like the instance at the University of California, Berkeley, the third instance also involved the theft of a laptop. On May 3, 2006, a data analyst employed by the U.S. Department of Veteran’s Affairs (VA) breached security protocols by removing a laptop containing the sensitive information of 26.5 million veterans from the VA offices to his or her home. The employee’s home was subsequently robbed and the laptop containing the personal data was stolen. Unlike the first incident involving Bank of America
Corporation, but similar to the second incident at the University of California, Berkeley, the hardware and the data were recovered. However, forensic analysis of the stolen laptop could not confirm with absolute certainty that the veterans’ information had not been viewed or corrupted.

None of the three examples detailed above conform to the image of identity theft that was meant to be combated by the passage of Public Laws 105-318 and 108-275. In each case, the crime was not perpetrated by a single criminal against a single victim. Of course, one might complain that, for example, although the case involving Bank of America Corporation clearly implicates a bureaucratic institution, the objection can be raised that in the case of the University of California, Berkeley, theft and in the case of the VA theft, there appeared to be a single criminal and a single victim. But to raise this objection is to mistake the real crime for a tangential issue. The theft of the laptops in the first two examples was not the true crime. The laptops themselves were merely pieces of hardware, though they were no doubt expensive pieces of hardware, but the true crime in each case was the theft of the information contained on the laptops. Therefore, to assign culpability in such a crime involves examining not just individual thieves but also the technosocial system that both domesticates DIT and concentrates personal data in only a few institutions.

To this end, it is necessary to move beyond the legal codification of identity theft and toward an exploration of identity theft as a cultural phenomenon, because as Foucault (1990) noted, we now inhabit “a type of society in which the juridical is increasingly incapable of coding power, of serving as its system of representation” (p. 89). The preceding explication of the criminalization of identity theft remains important, however, because it serves as a foundation for the development of the myth of identity theft. Of course, foundation in this case should be taken loosely and not be understood in terms of base and superstructure. Rather, the formulation of identity theft in juridico-political discourse is foundational in the sense that it develops a prohibition against a set of actions, but prohibition itself cannot be deployed as a disciplinary mode of power. That is the function of myth. Another way of stating this relationship would be to say that legal prohibitions delimit possible actions, but phenomena that are mythologized supervise and direct actions. This understanding of power and discipline are consonant with the imperative that Foucault (1990) issued when he analyzed sexuality. After refuting the accepted understandings of sexuality and replacing them with incidences of discourse and power, Foucault claimed that “if we wish to analyze power within the concrete and historical framework of its operation,” then critics must be willing to “break free of . . . the theoretical privilege of law and sovereignty” (p. 90). Although Foucault’s study was clearly concerned with human sexuality and its various conceptions, he took many pains to clarify that his methods for analyzing power and discourse were applicable to a host of subjects. Therefore, to understand how identity theft operates as a locus of power that shapes and warps technosocial relations, attention must be given to the means through which identity theft attains cultural resonance beyond legal apparatuses. As such, the remainder of this critique will be devoted to performing an exegesis of Citigroup’s Citi Identity Theft Solutions advertising campaign.

Security Against Saddlebags, the Babe Magnet, and a Geek

The Citigroup campaign was selected for analysis because of two factors: (a) the high volume and notoriety of its advertisements and (b) the presence of Citigroup as the most profitable financial institution in the global marketplace. In October 2003, Citigroup launched a new service referred to as Citi Identity Theft Solutions. Subsequently, in 2004, Citigroup commissioned an advertising campaign from the Minneapolis-based firm Fallon Worldwide; the advertisements proved to be incredibly successful for both Citigroup and Fallon. Evidence of this success came in the form of a 2004 Emmy award that was bestowed on the television advertisement titled Outfit. To date, the campaign has yielded numerous print advertisements, which generally follow the format of a photograph situated next to a sidebar of text. Typically, the photograph depicts an individual who has been dubiously mismatched with a particular product or service. Two notable examples include a petite, smartly dressed Asian woman standing in front of a monster truck and an elderly woman with a bouffant sitting for a tattoo. The text accompanying the photographs developed the theme of the campaign, which was Citigroup’s vigilance against uncharacteristic charges on their customer’s credit and debit cards. In essence, they were demonstrating their attention to the nature of their customer’s identities and their ability to perceive whether any purchases seemed out of character.

In addition to print advertisements, Fallon also produced an initial run of four television commercials for Citigroup. These were titled Geek, Mudflaps, Outfit, and Saddlebags. In the wake of their popularity, four
additional commercials were released: *Babe Magnet*, *Ooh La La*, *Stirrup Pants*, and *Underpants On*. Like the print advertisements created by Fallon, the eight television commercials dramatized the threat of identity theft by confounding viewer expectations. For the commercials, Fallon capitalized on the affordances of the medium of television by overlaying a monologue performed by a voice actor onto the performance of a live actor who mouthed the words. Both the qualities of the voices, including gender, as well as the content of the monologues themselves contrasted with the expectations that viewers formed based on the appearances of the live actors. So, for example, in the case of *Stirrup Pants*, a middle-aged man in a sleeveless T-shirt sits atop a riding lawnmower while enunciating words being spoken by a young woman with a heavy Southern drawl. The man—a victim of identity theft—is possessed by the voice of the woman who exploited him, causing him to gesticulate and mug wildly. All the while he rhapsodizes about purchasing items like “a set of those press-on nails with diamonds built right in” and “ankle bracelets” from “the ritziest shopping channel on T.V.”

Clearly, the commercial is meant to amuse the viewer while at the same time establish that Citigroup pays careful attention to their customer’s spending practices. Of course, this is just a superficial reading and one that masks the robust rhetorical effects of the Citi Identity Theft Solutions program. Moving beyond aesthetic appreciation, it will be demonstrated that the rhetoric of identity theft manipulates the role that DIT plays in relation to the commercial bureaucracies and individuals. Moreover, this manipulation takes the form of a rehabilitation or rationalization of DIT that blunts its potentially critical edge. Rather than perform a perfunctory analysis of all of Citigroup’s television commercials, though, the scope of the ensuing analysis will be restricted to three of the eight: *Saddlebags*, *Babe Magnet*, and *Geek*. This decision may sacrifice breadth for the sake of depth, but it should be noted that in terms of thematic content, these three commercials are representative of the entire campaign. For the sake of clarity, each advertisement will be summarized separately, and the monologue delivered in each will be excerpted in its entirety.

**Commercial 1: Saddlebags**

*Saddlebags* features a thin, young man stylishly dressed in a black Western-style shirt and black cowboy boots that peak out from under the hem of his dark stovepipe jeans. He slumps on a car’s bench seat that has been removed from the car itself and now sits alone in the foreground of a carwash parking lot. In the background, attendants go about their work of spraying and wiping a vehicle. The man, who with his dark hair, dark eyes, olive skin, and facial stubble is ethnically ambiguous, makes friendly eye contact with the viewer while mouthing words delivered by a gravely, nasal female voice:

> With his info I got a bank loan and immediately called Larry, my plastic surgeon and said Honey, bikini season was coming. So I wanted to liposuck my saddlebags, fix my hammertoes, new nose, new teeth, hike up the twins and finally, [cackling laughter] add a little juice to the caboose [cackling laughter that breaks into a violent smoker’s cough].

After delivering this statement, text appears on the screen that says “Eric Nguyen Identity Theft Victim.” The commercial then cuts to a rotating Citi credit card that is rendered against a sterile, white background. The Citicard bears a sample account number and name on the front and the words “Citi Identity Theft Solutions” on the back. While the image is displayed, a kind-sounding female announcer speaks the phrase “Introducing Citi Identity Theft Solutions—free with any Citicard. Help getting your life back: that’s using your card wisely.” The commercial closes by cutting back to the young man at the carwash, who asks in the same nasal female voice as before, “How can you put a price tag on beauty?”

**Commercial 2: Babe Magnet**

In this commercial, the viewer is shown an Asian woman dressed in a dental hygienist’s smock and blue scrubs. The woman is perched on a round stool situated before a reclining dentist’s chair that has an overweight, bespectacled boy laying in it. Throughout the commercial, the drone of a suction hose stuck in the drowsing boy’s mouth can be faintly heard. The office itself is drab and the faux-wood counters, fading forest-themed wallpaper, and giant novelty toothbrush leaning against the wall give the impression that it has been left unremodeled since the late 1970s. The dental hygienist in the foreground sits with her rubber glove–protected hands in her lap while synchronizing her performance with words spoken in a man’s lascivious baritone:

> I used her credit card to treat myself to a little chunk of heaven, Baby. That single’s weekend in Tijuana—freaky-deaky. But, first I needed to power up my
babe magnet: self-tanning creme, hair plugs, and a complete wax job on the old chassis. Ouch [breathy chuckling]. Slow down ladies, there’s enough Larry for everyone [eruption of moaning laughter].

While delivering the last line, text appears over the image that reads “Helen D. Identity Theft Victim.” Following the general format of the advertisements, the sequence featuring the victim gives way to a gray Citicard that has “Fraud Early Warning” printed on the back. The slogan spoken by the female announcer in *Babe Magnet* varies slightly from that which was spoken in *Saddlebags*. In this case, the announcer says, “Fraud early warning. When we see suspicious spending, we’ll alert you and stop it. Citi identity theft solutions: that’s using your card wisely.” Unlike in *Saddlebags*, however, *Babe Magnet* does not return to the victim/perpetrator hybrid for a closing remark. Rather, it ends simply with the Citi logo, telephone number, and Web site address displayed against a white background.

**Commercial 3: Geek**

*Geek* opens with an attractive, young Black woman seated at what appears to be either a hair salon or a day spa. She is dressed in a simple, fashionable pink top and dark jeans. Bird-of-paradise flowers stand erect in a vase directly adjacent to her, and an elderly woman sits thumbing intently through a magazine in the background. As the victim reclines, the sound of bubbling water can be heard from the footbath in which her feet are submerged. Above the babble of the water, she speaks in what sounds to be the awkward cadence of an adolescent boy:

Firewall, like that could stop me [high-pitched snicker]. Once I got her account number I couldn’t spend fast enough: sixty four inch plasma screen monitor, ten 4.2 megahertz wireless routers, and twenty-thousand bucks to complete my robot. My girl robot [high-pitched snicker]. This is gonna be the best prom ever [creaking laughter].

As with *Babe Magnet*, *Geek* superimposes text displaying the victim’s name, “Sandra T. Identity Theft Victim,” over the last few lines of the monologue. It also follows the standardized pattern of cutting away from the actress to an image of a rotating Citicard. In this commercial, however, the back of the credit card reads “Citi Identity Theft Solutions,” and the front of the card advertises that Citibank offers interest rates that are “as low as 3.99% fixed APR.” *Geek* is similar to *Saddlebags* in that the slogan spoken by the female announcer is exactly the same. However, unlike *Saddlebags*, *Geek* does not return to the woman in the salon; instead, it ends as *Babe Magnet* does, with Citi’s logo and contact information prominently depicted on the screen.

**Citigroup and the Cultural Phenomenon of Identity Theft**

To be sure, the three commercials exhibit a comedic ingenuity that is derived largely from their juxtaposition of voices and bodies. This drollness, however, is the very same mechanism by which they achieve such ideological potency. The voices and bodies, for example, do not reproduce the identities of fully developed individuals; rather, they reproduce facsimiles of identities, identities that represent nothing more than stereotypes. After all, it is preposterous in *Geek* to hear and watch the whiny, broken voice of a sexually frustrated teenage boy—a bland stereotype of adolescent male awkwardness—issue from the larynx of a hip and stylish Black woman, a quintessential icon of cool in American culture. Likewise, hearing Larry’s libidinous voice ooze from the mouth of the female dental hygienist in *Babe Magnet* is absurd; the voice evokes images of leisure suits and smoking jackets—articles that complete the image of the middle-aged Lothario—not sensible clogs and a smock, which are the standard attire of the stereotypically asexual and pragmatic middle-aged Asian woman. But the depiction of racist and ageist stereotypes is not the purpose of the commercials; it is rather an afterthought to their true purpose: the revision of cultural narratives governing the technosocial relationships between DIT and its users.

And yet Citigroup’s advertisements may be said to function as more than vessels for the transmission of naked ideology. Were that the case, then they could be viewed as merely embellishing the juridico-political definition of identity theft. Instead, through their reliance on stereotypes and comedy, among other things, they behave as mechanisms of discipline. As we just saw, the form of the commercials is just as crucial to understanding their meaning as is their content. They do not simply transfer ideology in toto, as was the case with the juridico-political definitions of identity theft, but instead Citigroup’s commercials blur ideology through a sophisticated interplay between audio, video, and textual components. To understand their implications for DIT and the formation of identity through DIT, it is therefore necessary to supplement ideological analysis with semiotic analysis. This leads
to the imperative of mythology, which Barthes (1982) identified as “part both of semiology inasmuch as it is a formal science, and of ideology inasmuch as it is a historical science: it studies ideas-in-form” (p. 97). Unlike ideology, which is chiefly concerned with the unmasking of historicized ideas and which was demonstrated in this critique when I contextualized Public Laws 105-318 and 108-275 within a larger framework of three notorious examples of identity theft, mythology is concerned with reading what lies behind the mask, the mask itself, and the relationship between the two. In this way, *Geek, Babe Magnet,* and *Saddlebags* can be understood as disciplinary mechanisms that do not so much hide meaning as actively manufacture it through ideological distortion. As such, the cultural phenomenon of identity theft is mythical because it is productive rather than merely occlusive. Ultimately then, understanding Citigroup’s commercials in terms of myth allows for an exploration of the cultural phenomenon of identity theft, which is itself a knot of power dynamics inaccessible to ideological analysis alone.

Drawing on the work of Barthes, Porter (2000) suggested that myth serves to “distort, naturalize and depoliticize ideology” to “protect power by converting historical and contingent social formations into natural and necessary ones” (p. 60). Whereas ideology is incendiary and robust, myths distort and refashion ideology so that it may be consumed and circulated with minimal agitation. To bastardize a familiar line, myths are the spoonful of sugar that help the ideological poison go down. One of the most powerful ways that myths are able to function is through their ability to create identification. Instead of relying on logos or suasive language alone, myths create signification between their own content and those who hear and see them. This characteristic led Barthes to claim that “myths are nothing but this ceaseless, untiring solicitation, this insidious and inflexible demand that all men recognize themselves in this image” (pp. 145-146). In the case of the cultural phenomenon of identity theft, this is achieved by presenting actors working against a background that construct a narrative with which viewers can identify. Returning to the issue of stereotypes for a moment, Citigroup’s Citi Identity Theft Solutions commercials are powerful precisely because of their use of stereotypes. Whereas stereotypes are ideologically reprehensible, the reduction of identity to stereotypes is essential for the effective deployment of myth. By relying on broad stereotypes and actors posing as ideal types of consumers, Citigroup’s Citi Identity Theft Solutions television commercials effectively nurture a perceived commonality between the victims represented on the screen and the users of DIT that view these advertisements on their televisions.

So then, the point is not that stereotypes are divisive or promote inequality, but rather, it is that stereotypes through their vacuity allow viewers to graft their own histories onto the people represented on the screen. As such, “we can say that the fundamental character of the mythical concept is to be appropriated,” and this appropriation, moreover, is facilitated by a lack of historical specificity (Barthes, 1982, p. 105, emphasis original). As critics, we may wonder about the missing histories of Eric Nguyen, Helen D., and Sandra T., but as viewers, we are invited to believe that through identification, their histories and the peculiarities of their identities are congruent with our own. In contrast to the colorful personalities and spending habits of the voices that we hear in the commercials, we are never given a sense of who the actual victims are. Both the dynamics of power and comedy function precisely because of this elision. Viewers only know that Eric Nguyen does not need liposuction, that Helen D. is not Larry, and that Sandra T. is not a geek, but viewers have no sense of who they are, where they come from, whose lives they touch, and indeed what they would have spent their money on had it not been stolen. These representations have no meaning except for an absence of deviance. Consumers of the myth might reasonably wish to be nothing like the imaginatively flawed persecutors, so by default they look to the other half of the binary, the victims, for identification. The rich story of the victims is therefore purposefully left unembellished so that they can more effectively solicit readers to identify with the images that they project.

The mythic efficacy of Citigroup’s advertisements is further enhanced by the effect of mastery that is created by the reduction of the actor onscreen to nothing more than a passive flesh puppet who is under the control of the conscious, dominating voice. The level of control is so great that even the gestures and expressions of the controlled bodies reflect the guilty satisfaction inflected in the voices of their masters. This occurs in all three commercials, but it is perhaps best illustrated in *Saddlebags* when the slender young man punctuates his reminiscence of adding “a little juice to the caboose” by reaching around to pat his posterior. These exaggerated gestures, ticks, and facial expressions signal that the body has been fully disciplined, or as Foucault (1979) put it, “a well-disciplined body forms the operational context of the slightest gesture”
(p. 152). To be fair, this juxtaposition does heighten the comedy in the commercials, but it also reveals the difficulty of identity expression in a system that views DIT solely as an efficient tool for data calculation. By extension, this juxtaposition also demonstrates the friction that develops when identity becomes codified as readily quantifiable information, which is to say when consciousness becomes abstracted from corporeality. The message here is that on entering the Web, bodies become vacated, and unless they are protected, they can become the instruments of another mind. To put it bluntly, they become prostheses. In this respect, the body becomes an analogue for the computer itself, where both are vessels that house information. Thus, the Citi Identity Theft Solutions program seeks to police the quantifiable aspects of a stable, corporeally based identity that can be potentially effaced by DIT.

In addition to promoting an ethos of material stability, Citibank’s commercials complicate the role of corporeality by construing the body as a source of shame and deviance. Indeed, Saddlebags, Babe Magnet, and Geek all employ a discourse of sexuality. In this respect, they are representative of all eight of the commercials in the campaign. This discourse, however, is not celebratory; it is rather one cautioning against perversion. The voiceovers in the advertisements represent misfit bodies, and viewers are meant to intuit that these bodies are sexually undesirable. The spindly geek in the ad of the same name who has to build a sexual automaton, the predatory swinger in Babe Magnet, and the rasping older woman willing to commit a crime to reduce her saddlebags, are all reduced to voices because their bodies violate cultural conventions regulating the erotic. They must usurp the identities and corporeality of others to gratify their illicit desires. Going even further, they actually penetrate their victims at the deepest level so that Eric Nguyen, Helen D., and Sandra T. become sexual automatons’ themselves. The scratchy-voiced geek in the commercial of the same name has built a “girl robot,” but this machine is superfluous because he has already used his mastery of DIT resources to puncture Sandra T.’s firewall, force himself inside her, and dominate her from within. What occurs in these commercials then is a rape of identity and the underlying message is that when left unregulated DIT can facilitate such odious behavior. One of the central components of the cultural phenomenon of identity theft, then, is a conflation of criminality with sexual depravity. The myth of identity theft is thereby enmeshed with a moralism railing against what are imagined to be illegitimate uses of the Web, be they fraud or pornography. In this way, identity theft in general and the Citi Identity Theft Solutions program in particular function hegemonically to gain assent from viewers by depicting a pageant of discipline.

Power, of course, is supple and it deploys discipline in various and oftentimes conflicting ways. With the cultural phenomenon of identity theft that is promulgated in part by Citigroup’s Citi Identity Theft Solutions campaign, discipline functions on the one hand by depicting disciplined bodies on the screen and on the other by relying on mythic solicitation and appropriation to induce viewers to discipline themselves. As such, this is a case of discipline once removed. Such self-discipline is of course the hallmark of power, and it reveals how identity theft in juridico-political discourse differs from the cultural phenomenon of identity theft. The legal definition of identity theft is meant only to prohibit certain misdeeds, but the cultural phenomenon of identity theft labors to channel and create deeds. Through the climate of fear that is created by the myth of identity theft, viewers are motivated to behave according to the paths of action that Citigroup has sanctioned. This means that they are to endorse the usage of DIT as both a virtual shopping mall and as a repository for personal data that is meant to stand in for the depth of an individual’s identity. Such a return to a bourgeois morality, which heightens anxieties regarding DIT by dovetailing financial deviance with sexual deviance, further facilitates the domestication of the Web.

Consonant with this maneuver is the role of protector that Citibank assumes. Babe Magnet, for instance, ends with the voice of the female announcer reassuring viewers that “when we see suspicious spending, we’ll alert you and stop it.” Saddlebags has the same announcer pledging that Citigroup offers “help getting your life back.” No doubt these statements are meant to be comforting, but on examination, their implications are disconcerting. They reveal how Citigroup is able to not only observe all of their customer’s spending habits but also how well they know their customers. On the surface, this builds consumer confidence because, after all, only a friend or relative would truly know an individual so well as to deduce whether purchases seem out of character. This implies a familiarity with customers’ preferences, distastes, leisure activities, occupations, marital status, number of children, and so forth. But of course Citigroup is a friend or relative of no one; it is a bureaucratic, international banking conglomerate.
Information that cannot be quantified remains irrelevant to its practices, and DIT applications that do not efficiently store, monitor, and synthesize quantifiable information are equally irrelevant. Instead of gathering this information through years of intimate conversations and shared experiences as a friend or relative would, Citigroup has gathered it much more efficiently through the surveillance applications of DIT. This reality, however, is distorted by the mythic depiction of identity theft on the screen. Because viewers are given clear villains and victims, victims who are readily appropriable, attention shifts away from the ethics of surveillance to instead focus on gratitude for Citigroup’s vigilance. Who could honestly wish ill will against Eric Nguyen, a young man who calls to mind the perfect older brother at the apex of his popularity or an ageless college friend who fell out of touch? Had he not been systematically observed so efficiently, there is no telling how badly his credit rating could have been damaged. Similarly, what viewer would be so crass as to trivialize the victimization of Sandra T. by critiquing and intellectualizing her situation? With her dramatic flair for style, she looks as though she instinctively knows where the best dance clubs are and which musical acts will be immanently igniting the charts. These characters are the equivalent of cumulus clouds: They are simultaneously suggestive and amorphous enough to assume a plethora of shapes by a plethora of viewers. As such, they inflect Citigroup’s admissions of surveillance in such a way that the prospect of being monitored ceases to cause anxiety and on the contrary becomes comforting.

In fact, a majority of the eight commercials composing the total campaign end with a pledge from Citigroup to examine suspicious spending activity and to police fraudulent charges. Citigroup, therefore, offers an aegis of security by cultivating viewers’ trust. Of course, this protection can only function if an individual agrees to restrict her identity to the narrow list of consumer preferences that Citigroup can then index and administrate. In his analysis of DIT and power dynamics, Poster (1996) arrived at a similar conclusion. Describing what he termed as the “superpanopticon”—which is essentially an update of Foucault’s reading of the panopticon for the era of computer networks—Poster claimed that the resources that enable online communication and commercial activities can develop into “an extensive discourse of surveillance, [changing] our private behaviors into public announcements, [and] our individual deeds into collective language” (p. 184). Elsewhere, Poster (1990) made a similar claim, writing that

the populace has been disciplined to surveillance and to participating in the process. Social security cards, drivers’ licenses, credit cards, library cards and the like—the individual must apply for them, have them ready at all times, use them continuously. . . . Home networking constitutes the streamlined culmination of this phenomenon. (p. 93)

For individuals to escape the insidious threat of identity theft, they must willingly enter the protective custody of Citigroup and accept its oversight of their behavior while entrusting it to store the data that have come to represent their identities. By trucking in the politics of fear, Citigroup is able to coerce individuals into accepting their services, even though this acceptance engenders a stripping away of the fullness of their identities. However, like any effective deployment of power, the pervasive scrutiny and surveillance that Citigroup promises is not experienced as a form of control. Rather, it is experienced as relief. For if individuals are to be reduced to information and if, as was shown earlier in this critique through references to Hayles (1999) and Poster (2001), that information is a commodity, then individuals themselves are agreeing to their own commodification. What the cultural phenomenon of identity creates, though, is a choice: either commodification by bureaucracies such as Citigroup or commodification by thieves and criminals.

This process of translating identity into quantifiable information, which in turn transforms individuals into commodities, is akin to what Fromm (1969) described as instrumentalization. And though he lived and wrote before the rise of DIT, Fromm gave a careful explanation of instrumentalization as it functioned during the technological era that he lived in. He described instrumentalization as a psychosocial imperative thrust on the individual, thereby causing the individual to consent to the loss of his or her own identity, and which in turn allowed for a degree of protection from private and public institutions. Fromm explained that the well-disciplined individual “thinks, feels, and wills what he believes he is supposed to think, feel, and will; in this very process he loses his self upon which all genuine security of a free individual must be built” (p. 280). What is gained
from this process is really just a cleverly disguised loss, for the individual only gains an illusory security from his conformity to the dictates of technosocial systems: “This loss of identity then makes it still more imperative to conform; it means that one can be sure of oneself only if one lives up to the expectations of others” (p. 280). Such a formulation clearly resonates with the cultural phenomenon of identity theft, where through fear individuals are impelled to accept the promises of security made by organizations like Citigroup instead of rejecting the configurations of DIT that are supported by these same organizations and that make individuals less safe to begin with. Rather than question how disciplinary mechanisms promote specific versions of DIT and identity, individuals find themselves striving to perfect these versions of DIT while simultaneously striving to make themselves more applicable to these systems. All of this effort and self-discipline accord individuals the luxury of a respite from the politics of fear, but as Fromm cautioned, “the price paid is high” (p. 280), for individuals literally become what they buy.

Conclusion

To clarify, the question is not whether crime can occur on the Web (it does), but rather the question is, “How does identity theft alter technosocial relations?” To ask this with greater specificity, how does the cultural phenomenon of identity theft affect the reconfiguration of DIT resources and representations of identity on the Web? The answer to this question, as this critique has attempted to demonstrate, is that disciplinary mechanisms working in conjunction with the myth of identity theft alter the course of power so that DIT functions primarily as a technique for the storage, monitoring, and synthesis of information and that this alteration of technology in turn constrains the expression of identity to the limited language of quantifiable data. Citigroup’s Citi Identity Theft Solutions campaign is a striking example of how the cultural phenomenon of identity theft occludes a host of technosocial relations. Although the multinational corporation Citigroup is active in using a specific version of DIT to reduce identity to a host of quantifiable consumer statistics, it is also at the same time able to manipulate the cultural meaning of identity theft to benefit from the insecurities that this process creates. In essence, then, it is able to assuage the fears of DIT that it itself has promoted. This form of reification is achieved through the language of myth that surreptitiously promotes the idea that crime on the Web is perpetrated by private deviants rather than by the negligence of those bureaucracies that control information. Such maneuvering in turn inhibits individuals’ capacity to question and retaliate against the system of information management itself.

This shift away from a technosocial configuration of DIT that initially appeared to be, in Miller’s (1991) phrasing, “inherently democratic” is indicative of a change in the balance of power underlying the contest between commerce and community on the Web. It is important, however, that the novelty of this contest not be overstated, for the elements of commerce and community have been from the beginning as much a part of computer culture as integrated circuits and microprocessors.

Indeed, Lyotard (1993), whose original French version of The Postmodern Condition: A Report on Knowledge was published in 1979, well before the rise of advanced DIT database-networking systems, identified it:

We are finally in a position to understand how the computerization of society affects this problematic. It could become the “dream” instrument for controlling and regulating the market system, extended to include knowledge itself. . . . In that case, it would inevitably involve the use of terror. But it could also aid groups discussing metaprescriptive by supplying them with the information which they usually lack for making knowledgeable decisions. The line to follow for computerization to take the second of these two paths is, in principle, quite simple: give the public free access to the memory and data banks. (p. 67)

It is hard to miss the similarities between the first half of Lyotard’s prescient statement about the proliferation of computers and the current implications for DIT and identity formation wrought by the cultural phenomenon of identity theft. Certainly there are echoes of the terror that Lyotard feared in the rhetorical subtext of Citigroup’s Citi Identity Theft Solutions advertising campaign. From the dread of being possessed, mastered, or figuratively raped by a deviant, disembodied consciousness to the persistent anxiety resulting from uninterrupted surveillance, the capacity for terror is tremendous. Of equal weight to this critique is the fact that Lyotard did not express the modernist fear of a fascistic government, but rather, he expressed the fear of a far more subtle, yet equally insidious, healthy market economy supported by
corporate bureaucracies eager to use the ‘‘dream’ instrument’’ of DIT. For as it was demonstrated in the preceding pages, juridico-political discourse cannot adequately use DIT to achieve the reformulation of society; its only recourse is a negative form of action where prohibition stands in for creation. The cultural phenomenon of identity theft, with its disciplinary mechanisms, is an expression of power that unlike criminalization and prohibition can reshape every aspect of technosocial relations.

Going even further than Lyotard, Marcuse (1964), although writing before Lyotard, described an even more developed scenario of technology gone awry. Marcuse offered an unequivocal analysis that decried the deleterious effects of technology on societies and individuals. Writing well ahead of the appearance of the first industrially manufactured personal computers, let alone before the integration of DIT into society, Marcuse nonetheless warned against the dangers of advanced technology:

Only in the medium of technology, man and nature become fungible objects of organization. The universal effectiveness and productivity of the apparatus under which they are subsumed veil the particular interests that organize the apparatus. In other words, technology has become the great vehicle of reification—reification in its most mature and effective form. The social position of the individual and his relation to others appear not only to be determined by objective qualities and laws, but these qualities and laws seem to lose their mysterious and uncontrollable character; they appear as calculable manifestations of (scientific) rationality. The world tends to become the stuff of total administration, which absorbs even the administrators. (pp. 168-169)

Although the current critique does not completely share Marcuse’s fatalism, it does parallel his anxiety over the rationalization of individuals and society that can occur when advanced technologies such as DIT are used as mechanisms for discipline. To the detriment of his argument, though, Marcuse relied on a form of technological determinism. Certainly he allows for change, though he did seem to possess reservations as to whether substantial change was truly possible, but that change is predicated on an equation whereby either technology will become an instrument of justice because society will behave justly, or else it will become an instrument of injustice because society will behave unjustly. And though Lyotard seemed more optimistic than Marcuse that the possibility for the just usage of technology could be realized, his assessment also relied on the sort of dichotomy that results from technological determinism.

The issue of how to conceive of technosocial relations therefore needs to account for simultaneity. Such a prescription might seem odd, given that this critique has paid exclusive attention to how the cultural phenomenon of identity theft domesticates the Web and rationalizes individuals. True enough, the cultural phenomenon of identity theft is important because in it we can observe a locus of power involving the technosocial relations between DIT and its users, but it would be a mistake to understand it as being synecdochal for the entire range of technosocial relations involving DIT. The consequences of the cultural phenomenon of identity theft do not describe the full activity on the Web. For at the same time that Citigroup deployed a myth of identity theft, other facets of the Web that were far less hostile to communal interaction and identity expression have also grown in notoriety. For example, scholars, such as Grossman (1995) and Ferber, Foltz, and Pugliese (2005), have demonstrated that the proliferation of DIT resources positively affects technosocial relations by improving democratic efficacy and increasing political participation. Likewise, Brady (2005) and Marlow (2004) examined the role of blogs both in terms of their epistemic value and in terms of their role in identity formulation. Turkle (1995) summarized the positive social and individual effects of these resources well when she wrote that “the many manifestations of multiplicity in our culture, including the adoption of online personae, are contributing to a general reconsideration of traditional, unitary notions of identity” (p. 260). It is quite clear, then, that noncommercial DIT resources offer forms of resistance against the constraints imposed by the cultural phenomenon of identity theft.

Ultimately, then, the purpose of this critique has not been to demonstrate the inevitability of the rationalization of identity and of the domestication of the Web. That those are the consequences of the cultural phenomenon of identity theft does not mean that they are ineluctable results or that they will even have a lifespan ranging beyond the next decade. At the same time, though, this critique has attempted to demonstrate that technosocial relations are shaped by more than just new technological developments and the vicissitudes of the law. That, of course, does not mean that new DIT applications are unimportant or that the criminal act of identity theft is not a serious catastrophe for its victims. Indeed, even as I composed this critique, I allowed my mouse to wander to
Web sites touting the newest breakthroughs in computer technology, and I of course used encryption software and alpha-numerical passwords when making all of my online purchases. But that reality does not undermine the fact that seemingly innocuous cultural phenomena such as Citigroup’s Citi Identity Theft Solutions campaign can dramatically affect the role of technology in society and the role of the individual in society. By ignoring these dynamics, we invite far greater dangers into our world than those posed by identity theft.

References


Daniel A. Caeton holds a BA in sociology with a minor in women’s studies from the University of California, Berkeley. He recently earned an MA degree in english composition and rhetoric from California State University, Fresno. His current research focuses on technosocial systems of disability and warfare.