

Identity, Privacy, and Information Technology

The rapid advance of information technology (IT) over the past decade has threatened two essential components of individual security: identity and privacy. Institutions—including educational institutions, which must deal with identity and privacy of students on a large scale—have an obligation at the least, and an exposure to liability at the worst, in the verification and protection of information directly related to an individual's identity and privacy.

The transforming effect of IT on commerce, communication, health care, and learning, among other areas, was noted in the 1999 PITAC report.¹ Inherent in this transformation, because of the speed and reach of IT, is the critical need for attention to the security of identity. In this era of faceless business transactions enabled by IT, identity can no longer be taken for granted as a fundamental physical characteristic. Rather, identity has become a database entity that can be disconnected from physical recognition—even bought and sold as a commodity—and as such is subject to easy theft and widespread misuse.

Identity theft is being called the "Crime of the Twenty-First Century." It was, in fact, made a federal crime in 1998.² Although the locality of life in small towns, and on college campuses, has traditionally insulated these communities from criminal access, the broad reach of IT now allows criminals ready access to faceless victims anywhere in the world. And college students, generally with no

established credit histories, are particularly exposed to disruption, at the formative stage of their careers. For an individual, the loss of control that comes as a result of identity theft can be devastating. The consequences can be far-reaching and enduring—having an effect on the ability to obtain a good credit rating, loans for homes or small businesses, and professional licenses and even on freedom



Illustration by Philip Kaake, © 2002

from arrest and incarceration. For a nation too, identity theft can be debilitating, as it is often the means for criminals to gain unauthorized entry to secure installations or to a country's transportation and communication systems.

Enabling Factors

Identity theft is a crime that requires the (inadvertent) participation of legitimate

enterprise for its accomplishment. The theft of identity starts when the criminal falsely represents himself or herself to a business or institution in some manner, often by providing another person's name and Social Security number. Business transactions have two fundamental elements: delivery of goods or services, and assignment of financial obligation. The criminal's misrepresentation causes damage via the first of these only to the business, in that the goods or services are delivered to and accepted by an individual who has no intention of paying for them. But the second element causes damage to the unknowing individual—the victim whose identity is being usurped. Only the business is in any position to thwart the identity theft, since the victim is not even aware of its occurrence. And the unwarranted assignment of financial obligation to the unknowing victim is made by the business, not by the criminal. It is thus the responsibility of the business to exercise due diligence to verify identity not only before exposing itself to loss of goods or services but also before incorrectly assigning financial obligation to an unknowing individual. It is essential today to recognize these two elements of business transactions, elements that were once closely connected but that are now disconnected in a faceless economy. Without the inadvertent collusion of the business or institution, no theft of identity can occur.

The initial misuse of identity in a single transaction is amplified into full-blown identity theft when the credit-reporting agencies accept the transaction,

without confirmation of validity, as part of the victim's credit history, incorporating an incorrect address or other erroneous information as fact in later transactions. Thus, although the criminal is the instigator of identity theft, businesses and institutions are the unintentional enablers if their practices do not adequately contend with the identity-misrepresentation possibilities that are offered by the emerging information-based economy. It might eventually be argued that there is liability associated with the unwarranted assignment of financial liability, or with the provision of credit history information, if there is no confirmation and verification.

A fundamental problem is that no U.S. national standard of identity (ID) has been established for use in business transactions. Too often the Social Security number (SSN) is taken alone as a definitive identifier. But the SSN was never intended as a national ID and has never been protected as such. Driver's licenses have become fundamental ID for access to airlines as well as in business transactions, but no national standard exists, and very good counterfeit licenses are available via the Internet. An established physical address is made ineffective when false addresses are readily accepted as changes of address. In large measure, business practices of confirmation, and of remediation, have not kept pace with the advances enabled by IT. And whereas the criminal who instigates the identity theft is innocent until proven guilty, the unknowing victim to whom financial obligation is incorrectly assigned is presumed liable until he or she can establish otherwise.

The problem is exacerbated by the desire of consumers for, and the competitive pressures on businesses to provide, quick transactions and instant credit. And it is compounded by aggressive marketing based on database correlations of consumer activity. This cross-database sharing of information on individuals can endanger privacy and has the unfortunate effect of raising concerns over a national standard for an ID that would be better protected from identity theft. The dual concerns of identity and privacy—the fundamental elements of individual security—are thus brought into conflict in

attempts to adopt standards and to draft corrective legislation.

Corrective Actions

Testimony before congressional committees and public meetings held by government agencies, consumer groups, and privacy advocacy groups has chronicled unwarranted credit card charges, drained bank accounts, fraudulent loans, declined job applications, denied licenses, false bankruptcies, incorrect arrests and detentions, and even undeserved prison records. Law enforcement agencies are also concerned about the potential for the organized use of identity theft, and invasion of privacy, to mount mass disruption of targeted groups or even of an entire country.

Unfortunately, there is little that an individual can do to protect against identity theft or loss of privacy. The Federal Trade Commission (FTC) has established a Web page (<http://www.consumer.gov/idtheft>) as a central source of information on both prevention and remediation of identity theft. Use of the SSN should certainly be limited as much as possible, and legislation has been introduced in Congress toward that end. Businesses and institutions, including colleges and universities, should not ask for the SSN to be given on checks and routine forms and should never display the SSN on public lists (even without names) or on ID cards and badges. Student information available on publicly accessible college or university networks and portals may be utilized for unsolicited, preapproved credit offers that can possibly be misdirected to enable identity theft. Students are, in fact, raising such concerns themselves.³ Educational institutions should examine and question the need of every use of the SSN.

Businesses and institutions, such as colleges and universities, must recognize their role as inadvertent enablers of identity theft and must exercise due diligence in the confirmation of proffered identity, the quality control of marketed credit-history information, and the adaptation of business practices to the speed and range of IT. Government must institute reliable standards of identity through legislation and regulation while protecting privacy and preventing the inappropriate sharing

of personal information. And individuals must realistically appreciate the competing aspects of information sharing and privacy and must balance anonymity with responsibility for actions.

All use of the SSN must be seriously questioned and restricted by businesses, institutions, government agencies, and the public. By accepting the SSN as primary identification and by inadvertently making SSNs accessible, businesses and government agencies, including colleges and universities, facilitate identity theft and thus endanger individuals. The only recourse available to the individual is to refuse to give the SSN—an action that may lead to being denied service. This is ineffective recourse for a student interacting with a college or university. Some use of the SSN may be reasonable; some may be problematic but very difficult to change; and some may be inappropriate and unnecessary. The use of the SSN as an identifier of students or employees may be convenient and expedient, but universal use creates opportunities for full theft of identity.

Identity is a basic element of the U.S. infrastructure: it is fundamental to the integrity of commerce and the assumption of personal responsibility. It is also one of two essential components of individual security. As we have seen in the United States, our infrastructure can and will be used against us. The government, public and private institutions, businesses, organizations, and individuals must all give the definition and protection of identity the highest attention, in the interest of both individual and national security.

Notes

1. President's Information Technology Advisory Committee (PITAC) Report to the President, *Information Technology Research: Investing in Our Future*, February 24, 1999 <<http://www.itrd.gov/ac/report/>> (accessed September 3, 2002).
2. *Identity Theft and Assumption Deterrence Act*, 18 U.S. Code, sec. 1028 (1998).
3. "ID Theft Turns Students into Privacy Activists," *Chronicle of Higher Education*, August 2, 2002.

Joe F. Thompson, Distinguished Professor of Aerospace Engineering at Mississippi State University, was a member of the President's Information Technology Advisory Committee (PITAC) from 1997 to 2001, in both the Clinton and the Bush administrations.

