Hastings Law Journal

Volume 54 | Issue 4 Article 10

1-2003

Did Privacy Cause Identity Theft?

Lynn M. LoPucki

Did Privacy Cause Identity Theft?

by
LYNN M. LOPUCKI*

Introduction

In the Bad Old Days—before privacy became the shibboleth of a political movement—most Americans had public identities. The large majority listed their names, addresses and telephone numbers in telephone and organization directories. Driver and automobile licensing records were open to the public, as were court records. Newspapers published lists of local arrests, bankruptcies, and divorces. If your kid's little league team won the series, the kids' names, addresses, and pictures were also in the local paper. You could find out who your neighbors were by consulting a city directory that listed them by street addresses.[1] As a legal matter, consumer credit reports were available to anyone with a "legitimate business need,"[2] and as a practical matter they were available to "virtually anyone."[3] Whatever else one may think of that environment, it was information-rich.

That richness made impersonation for credit purposes (what we now call "identity theft") difficult. An imposter's lies were subject to contradiction from numerous, sometimes unpredictable sources. For example, today's identity thief often switches the victim's address on the records of creditors or credit reporting agencies to the thief's own, thus capturing key portions of the victim's mail. That trick would not

* Security Pacific Bank Professor of Law at the UCLA Law School. I thank Daniel Solove and participants in the Enforcing Privacy Rights Symposium for comments.

1. Some such directories are still published. *E.g.*, HAINES CRISS+CROSS 2000–2001 DIRECTORY, LOS ANGELES, CALIFORNIA. A description of the Haines directories is *available at* http://haines.com/ccdir1.htm(last visited Dec. 1, 2002).

2. Fair Credit Reporting Act, Pub. L. No. 91-508, Title VI, § 604, 84 Stat. 1127, 1129 (1970) (codified as amended at 15 U.S.C. § 1681(b) (2000)).

3. WILLARD P. OGBURN, FAIR CREDIT REPORTING ACT 34 (4th ed. 1998) ("[Before adoption of the Fair Credit Reporting Act, m]any credit reporting agencies supplied their reports to virtually anyone."); 114 CONG. REC. 24,903 (1968) (statement of Sen. Proxmire) ("There have also been many stories telling of the ease with which an unauthorized person can get a look at an individual's file.").

have worked nearly so well in a world where home addresses were listed in numerous public places and names were plastered on the sides of mailboxes.

It is probably no coincidence that the rise of identity theft coincided with the decline in public identities. That decline began in the 1970s. Credit-based identity theft emerged as a significant problem in the 1980s, hitting epidemic proportions only in the 1990s.[4] The inverse relationship between privacy and public identity—logically and chronologically—suggests that privacy is a cause, if not the principle cause, of identity theft.

Like most writers before him, Professor Daniel Solove regards thieves' access to personal information as the principal cause of identity theft.[5] Without access to their victims' personal information, he reasons, identity thieves could not commit their crimes. His reasoning is correct, but his conclusion is of less practical use than might at first seem. Note that the same reasoning would apply to oxygen. Without oxygen, identity thieves would quickly suffocate, thus bringing the problem of identity theft to a close. Identity thieves' need for personal information—like their need for oxygen—will become useful in solving the problem of identity theft only when practical means are proposed for selectively denying personal information or oxygen to identity thieves. No such means have been proposed with respect to either.

To commit their crimes, identity thieves also need privacy. One person cannot safely pass as another in public. Practical means do exist for making the process for identifying people public, and so depriving identity thieves of the privacy they need. Unlike personal information securing, public identification offers a real-world solution to the problem of identity theft.

Public identification does not require a return to the Bad Old Days. One can have a public, thief-proof identity without sacrificing privacy. That is, one can have it without publicizing one's physical characteristics or physical location, without inviting an avalanche of junk mail, telemarketing calls, or spam, without significant increase in risks from stalking, and without having to trust either the government or private parties with personal information. In an article recently

4. The phrase "identity theft" appears in only nine stories in the LEXIS Allnws file from 1980 to 1986. Only the last of those stories is about impersonation for credit purposes and it refers to the problem as "so new that industry statistics on the size of the problem are virtually nonexistent." Thomas P. Fitch, *To Catch a Thief*, U.S. BANKER, Nov. 1986, at 92.

5. *See, e.g.*, Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1251 (2003) ("Identity theft is a consequence of an architecture .... It is an architecture ... where personal information is not protected with adequate security, where identity thieves have easy access to data ....").

published in the *Texas Law Review*,[6] I described the legal and physical infrastructure necessary. I did not name the system I proposed in that article, but for convenient reference now dub it the Public Identity System ("PIDS").

In his article published in this issue, Professor Solove disputes the workability of PIDS.[7] While I disagree, I believe that his article advances substantially the debate over the causes and potential remedies for identity theft. Perhaps Solove's most important contribution is his advocacy of what he calls an "architectural" approach to the problem. While the architectural metaphor is not perfect, it closely resembles the systems approach that I have been advocating and using. Solove and I agree that to solve the problem of identity theft requires analysis and understanding of the concrete system in which that theft occurs.

We also agree on three specific aspects of the solution. First, system transparency to the consumer is a crucial element.[8] A consumer should receive notice of activities conducted under the consumer's identity and have easy access to the records of such activities. Second, imposters should be put at risk by requiring them to make personal appearances.[9] Third, the government should ban the use of social security numbers as passwords.[10] That is, no one should be entitled to assume that I am you, simply because I know your social security number.

To understand why Solove and I nevertheless disagree as to the desirability of PIDS, the reader must first understand the relevant features of the credit reporting system. Part I explains those features. Part II then describes and evaluates the changes in system operation Professor Solove recommends. Part III explains PIDS. Part IV compares the effects of the two competing proposals, concluding that PIDS would perform in virtually every respect better than Solove's proposal.

6. Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89 (2001).

7. Solove, *supra* note 5, at 1264.

8. Solove, *supra* note 5, at 1268 ("I recommend an architecture that requires entities gathering personal information about people to keep individuals informed about their information.").

9. Solove, *supra* note 5, at 1271 ("[C]redit card companies should be required to meet with people in person when first creating the account. This will make identity thieves more reluctant to engage in fraud, as it will increase their chances of being caught.").

10. Solove, *supra* note 5, at 1270 ("An SSN, mother's maiden name, and birth date should be prohibited as the method by which access can be obtained to accounts.").

I. How the Credit Reporting System Works

Consider the example of Consumer, a person who has never before had credit. Consumer applies for credit from Lender, a consumer reporting system participant. In the loan application, Lender requires several items of personal information. They include name, social security number, address, telephone number, and perhaps more. This information will serve three distinct system functions: as an extended name, as contact information, and as a password. The information functions as an extended name whenever participants use it to distinguish Consumer from the approximately 190 million other Americans who are subjects of the system. The information functions as contact information when Lender uses it to find or get in touch with Consumer, perhaps regarding nonpayment. The information functions as a password when system participants accept Consumer's knowledge of it as proof that Consumer is the person Consumer claims to be.

A. Why Thousands of People Have Access to Your Personal Information

Upon receiving Consumer's loan application, Lender will seek a credit report from a credit reporting agency ("CRA"). CRAs are private firms that collect information on the credit worthiness of consumers and sell reports based on that information to prospective lenders, prospective employers and others. Because the CRA maintains files on some 190 million consumers in the US alone, Consumer's name may not be sufficient to distinguish Consumer's file. Others may have the same name, or a confusingly similar name.[11] To make the distinction, the CRA will require that Lender's request for a credit report be accompanied by additional information about the applicant. The most important will be Consumer's social security number. If accurate, name plus social security number constitute an "extended name" that is always sufficient to distinguish a person from all other persons (a "unique identifier").

Credit files are, however, notoriously inaccurate.[12] Names may be misspelled, social security numbers may contain typos, and other information may be obsolete or corrupted. In part for that reason, CRAs encourage or require their correspondents to furnish other information, such as address and telephone number, that might enable the CRA to overcome errors in names and social security numbers to nevertheless locate the correct file. As a result, Lender's

11. *See* LoPucki, *supra* note 6, at 99–100 (explaining the problem of similar names).

12. Research on the types and frequency of errors in credit files is collected in OGBURN, *supra* note 3, at 201–04.

request for a credit report on Consumer will probably contain nearly all the personal information Consumer surrendered to Lender.

Because the Consumer in this example is assumed to have no credit record, the CRA will find none, and report that to Lender. Because it now has information about Consumer, however, the CRA may use that information to establish a file.

If Lender extends credit, Lender may also report Consumer's repayment or default to the CRA. Each such report must also contain Consumer's personal information. The CRA must have that information to match the incoming report to the correct credit file.[13]

The next time Consumer opens an account, the new lender will require that Consumer furnish the same personal information. The new lender will forward that information to the CRA so that the CRA can identify Consumer's file and furnish a credit report based on it. This process will repeat as Consumer applies for credit from banks, department stores, landlords, utility companies, and others. As a result, Consumer furnishes extended name information—name, social security number, address, phone number, and perhaps additional information—to every prospective lender, and every prospective lender forwards it to a CRA.

To complicate matters further, there is not one CRA, but many. Three CRAs maintain files on nearly every American; and hundreds (perhaps thousands) of others maintain files on consumers in particular geographical areas or resell reports compiled by others. For the current system to operate, dozens of organizations must have extended name information on Consumer and thousands of employees in those organizations must have day-to-day access to that information. Consumer's personal information is everywhere.

B. An Inherently Faulty System for Password Identification

In addition to serving as an extended name, so-called "personal information" serves a second, more insidious function—that of a password. That is, the system operates on the assumption that anyone who knows Consumer's personal information is Consumer. To illustrate, consumers are entitled by law to see the file any CRA maintains on them. To do so, the consumer must, in most states, pay a fee. The consumer must also prove the consumer's identity to the satisfaction of the CRA.[14] Online or by telephone, the "proof" is accomplished entirely by answering questions about one's self. The CRA compares the applicant's answers to information in the credit

13. *See* LoPucki, *supra* note 6, at 98–99.

14. 15 U.S.C. § 1681h(a)(1) (2000) ("A consumer reporting agency shall require, as a condition of making the disclosures required... that the consumer furnish proper identification.").

file. If the applicant answers a sufficient number of questions correctly, the CRA concludes that the applicant is the consumer, and reveals the file.

Of course, information can play no role in the identification process unless that information is already in the hands of the CRA before the identification process begins.[15] The CRA does not "know" the consumer. All the CRA can do is match the applicant's answers to the credit file. No other investigation is conducted. It follows logically that any of the thousands of people with access to Consumer's credit file has the information necessary to successfully impersonate Consumer.

To illustrate, assume that Consumer has good credit. A corrupt employee of a creditor or a CRA sells a copy of the CRA's credit file on Consumer to Imposter, a professional identity thief.[16] Imposter is now in possession of all information that the CRA could possibly use to distinguish Consumer from Consumer's impersonators. Imposter can now open accounts in Consumer's name, monitor the CRA's file on Consumer for changes, and even make changes to the CRA's file that may prevent Consumer from monitoring it. To the system, an imposter who knows Consumer's "personal" information looks exactly like Consumer.

C. An Inherently Faulty System for Documentary Identification

To assist consumers in proving their identities, governments issue identity documents. The concept is that a government agency will determine the consumer's identity and then issue to the consumer a document or card that the consumer can use to prove that identity when necessary. In the U.S., the most commonly used document is a driver's license or identification card issued by the Department of Motor Vehicles ("DMV") of a state government (a "license"). To prevent an imposter from using a license issued to someone else, the license may contain a photograph of the person to whom the government issued it.

The system for documentary identification suffers from the same flaw as the consumer reporting system. The system has no means for determining the identity it will certify. As proof of identity, the DMV will accept a social security card or any of several other documents.[17]

15. *See* LoPucki, *supra* note 6, at 98–99.

16. Such illicit sales of credit reports are common. *See, e.g.*, Chris Taylor, *Giving Credit Where Credit is Not Due, The Big Identity Theft Bust Last Year Was Just a Taste of What's to Come*, TIME MAG., Dec. 9, 2002, at 100 (reporting sale of 40,000 passwords for access to credit reports).

17. A list of documents acceptable in California appears on the Department of Motor Vehicles website at http://www.dmv.ca.gov/dl/dl_info.htm (last visited Dec. 1, 2002).

A social security card—which contains no photograph—will be issued on presentation of a birth certificate, or, for a person born outside the U.S., a document authorizing entry to the U.S. Yet neither document is in any real sense proof of identity. Anyone can obtain a person's birth certificate, simply by ordering a copy from the state's Bureau of Vital Statistics and anyone of approximately the same age can use it, since it contains no information that can be compared to the user other than date of birth. Documents of entry to the U.S. are often based on nothing more than the self-serving statements of the applicant. As a result, virtually anyone can obtain a license identifying them as virtually anyone else they choose.[18] The California DMV recently estimated that it erroneously issues 100,000 licenses to identity thieves each year.[19]

The system for documentary identification could easily be improved, and efforts to improve it are under way. But a substantial proportion of Americans are opposed to the establishment of a national identity card or improvements in state licensing that would enable that system to function like a national identity card. As a result, the improvements actually made in licensing probably will be ineffective ones.

D. How Privacy Causes Identity Theft

In the consumer reporting system, identification is an entirely mechanical process. When an organization receives personal data, it compares that data to data already in its possession. If the data matches, the organization concludes that the person initiating the transaction is the person he or she purports to be.

Because the process uses sensitive personal information, identification must occur in secret. Consumer does not know the route his or her information travels or into whose hands it falls. Consumer cannot participate in his or her own identification. A lender who identifies a loan applicant as Consumer will not even notify Consumer of the identification. As a consequence, victims of identity theft only learn they are victims an average of fourteen months after the theft.[20]

18. *See* LoPucki, *supra* note 6, at 98 (describing layered nature of the identification process).

19. *See* Jerilyn Stanley, *Identity Theft: Supporting Victims in Recovering From the Crime of the Information Age*, 32 MCGEORGE L. REV. 566, 570–71 (2001) ("[T]he DMV issues over 100,000 fraudulent driver's licenses to identity thieves each year.").

20. Janine Benner et al., *Nowhere to Turn: Victims Speak Out on Identity Theft,* A CALPIRG/Privacy Rights Clearinghouse Report (CALPIRG/Privacy Rights Clearinghouse, Sacramento/San Diego, Ca.), May 2000, at 3, *available at* http://www.privacyrights.org/ar/idtheft2000.htm (last visited Sept. 6, 2001).

Consumer has the right to examine the file any CRA keeps on Consumer.[21] But as the system currently operates, Consumer has no means of knowing which CRA's file may contain evidence of an ongoing identity theft. Privacy pundits glibly recommend that Consumer monitor them all.[22] To obtain a single copy of his or her file at each of the three major CRA's, Consumer must pay about $25 and prove his or her identity to the satisfaction of the CRAs. Recall that to prove his or her identity, Consumer must provide personal information to the CRAs by answering questions. If Consumer's answers match the information in the credit file, the CRA will accept Consumer's identity and sell Consumer a copy of the file.

Also recall, however, that much of the information in CRA files is incorrect. Correct information furnished by Consumer may not match the information in the file. In that event, the CRA will deny Consumer access to the file. For example, I was unable to access my credit file because a creditor furnished the CRA with an incorrect address for me.[23] My actual address did not match the address in my credit file. In my Information Law class each semester, I illustrate the difficulty of accessing one's own credit file by requiring that each student try to do it. I query them in class on the results. On average, about 10% are denied access to their files.

Identity theft flourishes because identification occurs in secret—in a faulty process that victims are unable to monitor effectively. The system cannot simply dispense with the secrecy. The secrecy exists to protect Consumers' privacy rights in the information used to identify them. As previously noted, privacy objections also prevent improvements in the system for identification. Thus privacy claims are at the root of the chain of causation that leads to identity theft.

II. Professor Solove's Changes

Professor Solove proposes to remedy none of the three problems described in Part I. After implementation of his reforms, thousands of employees would continue to have access to Consumer's personal information. Creditors and CRAs would continue to identify credit applicants mechanically by the applicant's knowledge of personal

21. 15 U.S.C. § 1681g (2000).

22. For example, under the heading "What you can do today [to prevent identity theft,]" the Federal Trade Commission website advises: "[o]rder a copy of your credit report from each of the three major credit reporting agencies every year." Federal Trade Commission, *ID Theft: When Bad Things Happen To Your Good Name*, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm (last visited Dec. 2, 2002). *E.g.*, Taylor, *supra*, note 16, at 100. ("[T]he most effective way to keep your identity clean is to check your credit reports once or twice a year.).

23. Lynn M. LoPucki, *No Credit Where Credit Was Due*, N.Y. TIMES, Sept. 20, 1997, at A2 (recounting the denial of access).

information in the file, and no improvements would be made in the system for documentary identification. Instead, Solove would attempt to ameliorate the identity theft problem by plugging information leaks and making three sets of changes.

A. Personal Appearances

First, Solove would require that a consumer personally appear in the office of the lender to open a new account: "[C]redit card companies should be required to meet with people in person when first creating the account. This will make identity thieves more reluctant to engage in fraud, as it will increase their chances of being caught."[24]

While such arrests would certainly be possible, they would not be common. Few lender's would know an imposter by appearance. To determine whether a personally-appearing applicant was an imposter, lenders could only continue to use the means they currently use for determining identity: obtaining personal information from the applicant and seeing if it matches a credit report.

As Solove recognizes, personal appearances would be an expensive change in the functioning of the consumer credit system.[25] Each consumer opens numerous credit accounts. Today, they do so without making personal appearances.

If the law were changed to require appearances, many kinds of lenders would have to reorganize their businesses to make such appearances feasible. For example, a New York bank that wanted to continue to solicit credit card customers nationwide would have to arrange for local agents in every city before whom credit card applicants could appear. A consumer who wished to rent an apartment in a distant city might have to travel to that city to make the required appearance. Most importantly, every consumer who opened an account would at least have to travel locally to make the required appearance. Consumers would no longer have the convenience of opening accounts by mail, by telephone, or on the internet.

B. Mandatory CRA Reports and Notices

As an alternative to his proposal for mandatory personal appearances, Solove would require that every creditor opening a new account purchase a CRA report containing the applicant's name, address, and telephone number.[26] Probably most creditors already

24. Solove, *supra* note 5, at 1271.

25. Solove, *supra* note 5, at 1271 ("The downside to this solution is its high cost.").

26. Solove, *supra* note 5, at 1271 (proposing to "require companies that want to open a new account through the mail to verify a person's address, date of birth, and phone

obtain credit reports, which include this information. But many, including most landlords, most utility companies, some stores, and probably even some credit card lenders, do not obtain credit reports. They would have to purchase a CRA's contact information, thus adding to total credit reporting system costs. The CRAs would no doubt be pleased with the increase in business.

Solove would required creditors to purchase this information to facilitate a second requirement he would impose: that each creditor opening a new account notify the consumer in three ways. First, the creditor would mail notice to the consumer at the address on the loan application. Second, the creditor would mail notice to the consumer at the address listed in the CRA's file. Third, the creditor would phone the consumer at the telephone number in the CRA's file.[27] Solove does not indicate whether the creditor should lend before these notices are given and the consumer has had an opportunity to reply.

Either way, these notices would make identity theft more difficult by alerting some victims at an earlier date. Those victims could then take steps to protect themselves.

The notices would, however, be expensive and inconvenient. Because the vast majority of account openings are by consumers rather than imposters, the vast majority of notices would convey information of which the consumer was already aware.

Identity thieves have already developed methods of working around such notices. For example, before opening the new account, the thief—impersonating the consumer—could report a change of address and telephone number to the CRA. When the thief then opened the new account, the required notices would go to the thief rather than the consumer. Even if the address in the CRA's file is that of the consumer, an enterprising thief could still beat the system. The thief would steal the address-change notice from the unsuspecting consumer's mailbox. To facilitate that theft, imposters might target victims whose mailboxes are insecure and for whom the CRAs do not have telephone numbers.[28]

---

number with a credit reporting agency . . . ."). These reports are commonly referred to as "credit headers."

27. Solove, *supra* note 5, at 1271 (referring to "written confirmation both to the address that the applicant lists on her application as well as to the address that the credit reporting agency has. Further, the company should follow-up by calling the applicant's telephone number listed with the credit reporting agency.").

28. Greg Botonis, *Deputies Round Up Five Suspects in Mail, Identity-Theft Ring*, L.A. DAILY NEWS, Nov. 28, 2002, at AV1 ("Identity thieves, investigators said, target neighborhood delivery and collection mail boxes and curbside home boxes, especially those that are difficult to see from the residence.").

C. Free, Easy Access to Credit Files

Professor Solove recognizes that under the current system, consumers' access to their CRA files is expensive and difficult. He would solve the problem by making access free and easy. A few states already mandate free access.[29] Aside from the expense—which presumably will be passed along to creditors in the form of higher prices for credit reports and then passed along by creditors to consumers in the form of higher loan closing costs—free access should create little difficulty.

Easy access is a different matter. Credit files from the big three CRAs are already available on the internet. The difficulty in obtaining them is almost entirely the difficulty of proving one's identity to the satisfaction of the CRA. The proof requirement exists to protect the privacy of the consumer's credit file. This puts Solove in a bind. Any easing of the proof requirement would reduce the consumer's privacy protections—a consequence that Solove clearly does not intend.

As it currently operates, the credit reporting system has no means for distinguishing Consumer from an imposter who knows the information in Consumer's credit file. Thus, any change that would make it cheaper and easier for consumers to examine their credit files would also make it cheaper and easier for imposters to examine consumers' credit files.

Solove responds to these observations by proposing an "opt-in regime to credit reporting."[30] A CRA would be entitled to sell a report only on a consumer who chose to become the CRA's customer. While the idea is intriguing, Solove gives no clue as to how he would implement this massive change or what the effect would be on the cost and availability of credit reports. Nor does he offer any explanation of the mechanism by which the opt-in regime would "curtail problems of improper access."[31]

III. The Public Identity System ("PIDS")

In an earlier article, I described a system that would completely eradicate the most common and most troublesome form of identity theft: new account openings.[32] In his article, Professor Solove considers and rejects the system.[33] In this part, I briefly describe the essentials of the system and respond to Solove's objections.

29. OGBURN, *supra* note 3, at 83–84 n.117 (listing provisions of state law).
30. Solove, *supra* note 5, at 1269.
31. Solove, *supra* note 5, at 1269.
32. *See* LoPucki, *supra* note 6.
33. Solove, *supra* note 5, at 1263–66.

PIDS would enable any consumer to publicly claim his or her identity and publicly provide instructions for his or her identification. Creditors who opened new accounts for imposters without using the system and following the consumer's instructions would lose the exemption creditors currently enjoy from lawsuits based on defamation, negligence or invasion of privacy.[34]

Instead of identifying persons from scratch each time they appear, PIDS would make a "primary identification," establish a contact link to that person, and thus enable anyone to make a "secondary identification" through the link.

A. Primary Identification

Any consumer who chose to participate in the system could make application to the administering agency. To facilitate concreteness in this discussion, assume that the agency delegated its duties to local DMVs. Upon receipt of the application, the DMV would do two things. First, it would post the applicant's name, social security number, and proposed instructions for identification on a public, read-only website. The posting would recite that a primary identification was in progress. Second, the DMV would investigate to determine if the applicant is the person to whom the social security number was issued. In most instances, the investigation would be cursory. The DMV would compare the applicant's information with the information in the files of a single CRA and the earnings information shown on the relevant social security account.[35] In suspicious cases, the investigation would be more extensive.

The investigation contemplated would be inexpensive. Similar investigations are done by firms that issue SSL Web Server Certificates. Those firms identity and verify the physical location of the person or entity to whom the firm issues a certificate. In the course of that investigation, they may require documentary evidence or check public records. I paid $65 for a SSL Web Server Certificate issued by Thawte, Inc. for lopucki.com, which included the cost of the identification.[36] Like the Web Server Certificate System, PIDS could be supported by user fees.

34. 15 U.S.C. § 1681h(e)(2002); OGBURN, *supra* note 3, at 274–81.

35. One expert on identity theft estimates that most impersonations could be eliminated by creditors spending "two minutes" comparing each credit application they receive to information contained in a credit report. Telephone interview with Beth Givens, Director of the Privacy Rights Clearinghouse (Nov. 27, 2002). Comparison by the DMV under PIDS would be equally effective, but more efficient because the comparison would be required only once per participant, not once per credit application.

36. *See* Thawte, Web Server Certificates, *available at* http://www.thawte.com/html/RETAIL/ssl/index.html (explaining what a web server certificate is) (last visited Dec. 3, 2002).

The DMV would have thirty days in which to complete its investigation. At the end of that period, the applicant would be required to make a personal appearance at the offices of the DMV to complete the application process—without yet knowing the results of the investigation.

Imposters could not complete the application process, because the likelihood of arrest would be too high. Even if the DMV investigations were generally ineffective, the public posting of the application would be sufficient to deter. Anyone could be monitoring the website searching for fraudulent applications. They might include non-participants guarding their own identities, services hired by them, or merely curious friends, relatives, or strangers. Any of those people could have notified the DMV of the fraudulent nature of the application. Prodded by the victim, even a generally dull, non-responsive agency could stumble through to make the arrest. DMV performance would be enhanced by the public nature of its failures: any successful impersonation would have appeared publicly, on the DMV's watch, for a period of thirty days. If the victim complained to the DMV during that period, the DMV's malfeasance would be inescapable.

The primary identification process would provide a crucial element missing from the current system. Through the DMV's investigators, the process could determine identity on the basis of personal relations, personal appearances, and multiple sources rather than on the basis of a mechanical matching of characteristic values.[37] Because the current system cannot distinguish the consumer from an imposter who knows the consumer's personal information, actors in the current system—including law enforcement agencies—always remain unsure whether they are dealing with a victim or an imposter. Identity theft victims may be jailed. Notices intended for victims may go to imposters instead. Imposters may place alerts on credit files, thereby preventing victims from accessing them. In this uncertain environment, public or private enforcers find it difficult to take decisive action against a suspected imposter. They realize they don't really know for sure who is who. The primary identification process would eliminate that uncertainty by assuring that the person listed on the website was not an imposter.

Even if an imposter did get through the primary identification system, in most cases no serious damage to the consumer would result. Imposter's use of Consumer's identity for credit purposes inflicts no loss on Consumer until false reporting occurs. The

37. *See* LoPucki, *supra* note 6, at 115–17 (describing the investigation); *id.* at 120–21 (describing the investigation's ability to reach into the applicant's community); *id.* at 125–27 (describing the theory behind the primary identification requirement).

principal damages are the costs Consumer incurs in time and money setting the record straight. Those damages are great in the current system because the inaccurate credit record is spread throughout the files of numerous CRAs, creditors, government agencies, and others. The victim must correct them one by one. Even during the correction process, the identity thief may continue to impersonate the victim. Also, because the corrected records are no more authoritative than the uncorrected ones, creditors and CRAs often inadvertently reverse corrections already made.

PIDS provides a single, authoritative focal point for identification. Once the website is corrected, the victim need make no further *proof* of identity—mere *notice* to creditors and CRAs will be sufficient to enable them to correct their records. Under PIDS, cleaning up a credit record would take a few days, not years.

The DMV might make stupid errors and bullheadedly refuse to correct them, just as creditors and CRAs do in the current system. The difference is that under PIDS, the victim would have a right to a hearing, and ultimately judicial appeal. It is difficult to imagine a case in which an imposter would contest a victim's identity claim in a hearing.[38]

B. Secondary Identification

At minimum, the public website would contain the consumer's name, social security number, and instructions for identification. Consumer would be entitled to choose among several alternative instructions.[39] They might require that prospective lenders merely send notice of an account opening to the consumer. Alternatively, the instruction might require that prospective lenders wait for the consumer's reply before opening the account. The contact might be by mail, by telephone, by email, or by encrypted email if the creditor uses that technology. If the consumer's contact information has changed in the preceding ninety days, the instructions may require the creditor to comply with both the old and new instructions.

Creditors who chose to use the system would access the website before opening any new account. They would obtain the consumer's instructions and comply with them. For example, assume that a consumer posted an instruction to contact her by cell phone, and later went to a bank to apply for a credit card. The loan officer at the bank would confirm her identity by consulting the website, obtaining the cell phone number, and calling it. She could take the phone out of her purse, answer it, and confirm her own identity. A participant who

38. *See* LoPucki, *supra* note 6, at 128–29 (describing the method for handling challenges to a claim of identity in the primary identification system).

39. *See* LoPucki, *supra* note 6, at 118 (listing the permissible instructions).

did not want to publicly list his cell phone number might instead obtain an email address for use only in PIDS. If the participant applied for a credit card online, the lender would consult the website, obtain the email address, and send notice of the credit application to it. The participant would confirm his identity by answering the email.

C. Why the Public Information Is Harmless

To obtain the full benefit of PIDS, consumers would have to publicly display at least three items of information: name, social security number, and contact information. Social security number is necessary to enable a participating creditor to identify its credit applicant as the person listed on the website. The consumer's name is needed to provide redundancy in matching and thereby overcome the inevitable errors in transcription of social security numbers. Contact information is necessary for the recipient of a credit application to give the system participant notice that a transaction on the participant's identity is in progress.

(1) Social Security Numbers

Public display of their social security numbers is unlikely to harm participants. Before the system is implemented, federal law would be changed to prohibit the use of social security numbers as passwords. No one should be entitled to assume that a loan applicant is a particular person simply because the loan applicant knows the person's social security number. Social security numbers will no longer be a key that unlocks a consumer's financial information, educational record, or other personal information. Such a law should be enacted whether or not PIDS is implemented and is already long overdue. Professor Solove agrees.[40]

Professor Solove objects to the public disclosure of social security numbers because disclosure "will increase the use of the number to link up records about people."[41] The increase would not, however, be significant for people who chose to list minimal information on the website. To understand why, consider the two possible types of people: people like myself whose names are unique, and people like John Smith whose names are not unique. (For convenience, I will refer to the latter as people with "common names.")

Social security numbers cannot increase matching for people with unique names for the simple reason that any information accompanied by a name can be matched without the social security

40. Solove, *supra* note 5, at 1270 ("An SSN, mother's maiden name, and birth date should be prohibited as the method by which access can be obtained to accounts.").

41. Solove, *supra* note 5, at 1265.

number. The social security number could only increase matching in situations where information is available by social security number, unaccompanied by name. I can think of no situation worthy of concern in which that occurs.[42]

Nor could the public display of social security numbers significantly increase unwanted linking for persons with common names. Human identification theory tells us that for information to be used in linking, that information must be present on both sides of the match.[43] The website would, at minimum, contain only three items of information: name, social security number, and contact information. Without other information, a common name is useless in linking—the link would be to relevant and irrelevant information. The contact information displayed could be an email address used for no other purpose. Such an address could never appear on the other side of the match, also rendering it useless in profiling.

The social security number could be used only to match to other records that also contained the participant's social security number. Such a match might seem sinister, but is not. To make the match, the user would already need to have the participant's social security number, and would almost certainly already have the participant's name. Thus, success of the match could add only a single new item of information to the user's "digital dossier" on the consumer:[44] an email address that could not be used for marketing purposes[45]

Some participants will choose to list more than the minimum required information on the PIDS website. When they do so, they may be contributing to the "digital dossiers" kept by unknown persons and organizations. I am one of many people who consider the dangers of such "dossiers" vastly overblown and easily outweighed by the benefits of a public identity. That some do not want information-rich public identities is not in itself a reason to deny them to others.

42. If a name were rendered illegible on a record that contained a social security number, information from the website might be used to restore the name. But I know of no reason why anyone would deliberately render a name but not a social security number illegible, so the restoration of the name will almost certainly be a convenience, not a threat.

43. LoPucki, *supra* note 6, at 98–99.

44. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) (complaining that private sector entities are compiling "digital dossiers" on individuals and sharing them with government).

45. The prohibition on use of PIDS information for marketing purposes is discussed in the next subsection.

(2) Use of Website Information for Marketing Purposes

Federal law should also prohibit use of the information displayed on the website for marketing purposes. Such laws have already been upheld against First Amendment challenge in other contexts.[46]

Both the government and participants would have a role to play in "seeding" the website so that violations of the prohibition could be discovered and prosecuted. The government's role would be to list non-existent persons on the website, with contact points that the government would monitor. Because the person was non-existent, marketing materials could be addressed to the person only by abuse of information on the website. The government would respond to such materials with prosecutions. The participants' roles would be to create variants of their contact information that would appear nowhere except on the website and to report marketing materials sent to those variants to the government enforcement agency for prosecution.

Professor Solove correctly observes that few people have any expertise in seeding.[47] Fortunately, none is necessary to obtain the benefits of seeding. A few people, who do have expertise, will intentionally seed their own information. Others will unintentionally seed theirs by making errors in the entry of data. The appearance of either kind of seed information in mailings to system participants would prove the mailer's misuse of PIDS information. Because the mailer has no way of distinguishing seeded entries from unseeded ones, the seedings of the few would protect all system participants.

(3) Stalking

The information listed on the website will enable anyone to contact the participant. Most people consider the resulting threat to privacy minor. They list their telephone numbers in publicly-distributed telephone directories.

For some, like stalking victims, the threat is more serious. But even a stalking victim could comfortably participate in PIDS. The challenge she would face would be to provide contact information that would work quickly and easily without divulging her physical location.

Celebrities have long dealt with this problem by publicly listing only their agents' contact information. The agent passes the message

46. *E.g.*, Fed. Election Comm'n v. Int'l Funding Inst., 969 F.2d 1110, 1118 (D.C. Cir. 1992), *cert. denied*, 506 U.S. 1001 (1992) (upholding a statute providing that lists of political contributors filed with the Federal Election Commission may not be sold or used by anyone else to solicit contributions or for a commercial purpose).

47. Solove, *supra* note 5, at 1266 ("However, it is unclear whether many individuals have the sophistication to concoct creative attempts to seed their information.").

along to the celebrity and then passes the celebrity's answer—if any—along to the inquirer. For people of ordinary means, a telephone answering service or a friend can perform essentially the same function.

Most stalking victims could protect themselves adequately by displaying an email address as their sole point of contact on the website. If the email address is through a national provider, such as Hotmail or AOL, the address would provide no clue to the recipient's physical location. A sophisticated stalker might send the victim an email containing a web-bug that would send a return message when the user opened the email, but software is available to discover and disarm such programs.[48] By posing as a creditor seeking to confirm identity, the stalker might induce the victim to send him a message. But the victim's response will not reveal her physical location if she uses the services of an anonymous remailer.[49] Even if the stalker succeeded in tracing a response from the victim's computer, the stalker could at best learn the location of the first internet router to handle the message—not the physical location of the victim's computer.

Professor Solve objects that the difficulty of using these techniques may "disadvantage those who are not computer savvy" by excluding them from the voluntary PIDS system.[50] I take this as a compliment to PIDS, because it recognizes participation in PIDS as a valuable benefit. The fact that not everyone can benefit equally or as easily from the system is not sufficient reason to deny the benefit to everyone.

D. Professor Solove's Other Objections

Professor Solove raises three other objections to PIDS, none of them valid. First, he complains that PIDS "relies too heavily upon the initiative of individuals" in requiring that consumers make application to participate, make a personal appearance, and engage in monitoring of the website.[51] A system that could eradicate identity theft without requiring consumer initiative would, of course, be better. None, however, has been proposed. The alternatives that have been proposed—including Solove's own—would require greater consumer initiative than PIDS to merely ameliorate identity theft. For example, Solove's proposed solutions would require that

48. E-mail from Michael Froomkin, Professor of Law, University of Miami School of Law, to cyberprof_list (Nov. 23, 2002) (on file with author).

49. E-mail from Declan McCullagh to cyberprof_list (Nov. 27, 2002) ("Any competent remailer will strip out identifying headers.") (on file with author).

50. Solove, *supra* note 5, at 1264.

51. Solove, *supra* note 5, at 1264.

consumers take the initiative to guard their personal information, monitor their credit files at several, often hostile, credit reporting agencies, establish customer relationships with CRAs, and make personal appearances to open accounts. Even more initiative is required of consumers under the current system. Not only must they guard their personal information and monitor their credit files before they become victims; after the crime they must initiate CRA "alerts" and reinvestigations, file complaints with the police, and prove their innocence to every creditor or CRA who would misreport information about them. For PIDS participants, all that need for initiative would disappear.

Second, Solove believes that so few people will use PIDS that "it would function as little more than a band-aid solution. Identity thieves could concentrate their efforts on the vast majority of people who do not participate in the system."[52] Essentially, Solove is saying that people are not sufficiently concerned about identity theft to use a cheap, easy system that would prevent it. I believe the people who are the most vulnerable to identity theft would participate in PIDS. Thieves would migrate to the next most vulnerable group of nonparticipants, who would then become participants. The process would continue until the next most vulnerable group of non-participants was insufficiently vulnerable to support the crime. Only a minority of Americans would be members at that point, because only a minority of Americans—those with good credit—are significantly vulnerable to identity theft.

Neither of us has proof for our beliefs. The only practical way to generate that proof would be to implement PIDS. The system is not incompatible with other proposed solutions, it can be supported almost entirely by user fees, and it can operate at almost any scale. There would be no harm in trying.

Third, Solove complains that "[t]here is no guarantee that LoPucki's government agency will have better data security practices than other government agencies" whose websites "have been hacked numerous times."[53] Solove does not even suggest what he fears from this lack of security. No data can be taken, because all data on the website is already public. Data on the website cannot be changed because the website is read-only. It is constantly refreshed from an off-line database. If data on the website were somehow changed, the change would occur publicly, would be noticed, and so would be remedied. That compares favorably with Solove's reliance on private CRAs, where intrusions occur in secret and consumers do not even have the right to know of them.

52. Solove, *supra* note 5, at 1264–65.
53. Solove, *supra* note 5, at 1265.

Comparison and Conclusions

PIDS is superior in virtually every respect to both the current system and to the systems Solove proposes. In the latter systems, each consumer must monitor his or her identity at several, password-protected CRAs. In PIDS, each consumer could monitor his or her identity on a single web page, with a single click. Under one of Solove's proposals, every consumer would have to make a personal appearance to open each new account and the consumer would make those appearances in circumstances unlikely to deter imposters. Under PIDS, only system participants would have to make personal appearances, each ordinarily would have to appear only once, and the appearance would be in circumstances highly likely to deter imposters.

Solove and I both recognize the need to give notice to consumers of transactions involving their identities. Solove's notices would go to all consumers, whether they wanted them or not, by mail and telephone, reaching them only after the transaction. PIDS notices would go only to consumers who wanted them, would go by the medium the particular consumer preferred, and would reach the consumer in time to prevent identity theft.

Under Solove's proposals, knowledge of personal information would continue to serve as proof of identity, forcing consumers to continue their futile attempt to secure their personal information to prevent identity theft. Under PIDS, knowledge of personal information would no longer serve as proof of identity; identification would be determined by public claim and personal contact. Consumers would no longer need to guard their personal information to prevent identity theft. Even a thief with all of Consumer's personal information could not impersonate Consumer.

PIDS would generate fewer personal appearances, fewer notices, and fewer transactions with CRAs, giving it a cost advantage over the systems Solove proposes. PIDS would have two expenses that Solove's system would not: investigating identities and maintaining the web site. However, those costs would be incurred and paid only by voluntary participants. Solove's system incurs no cost of investigating identity only because it has no mechanism for investigating identity.

In summary, today's credit reporting system has two fatal flaws. First, the system identifies people only mechanically and therefore lacks the ability to distinguish a consumer from an imposter who knows the contents of the consumer's credit file. Second, integration of the identification subsystem with credit files that contain sensitive personal information forces the identification subsystem into secrecy. Even if the system were to adopt an ideal of full transparency, the

need to protect that sensitive personal information would hobble the mechanisms of access and so prevent realization of the ideal. Solove proposes to remedy neither flaw.

PIDS separates the personal identification function from the credit reporting system. Persons can publicly claim their identities and thus prevent theft, without disclosing, or risking the disclosure, of sensitive personal information. The system is fully scalable,[54] could be voluntary for both consumers and lenders, and could be supported entirely by reasonable user fees. The system was developed with new-account identity theft in mind, but could be effective in protecting participants against almost any kind of impersonation. PIDS would provide immediate relief to millions of Americans who have been the victims of identity theft and are still struggling with the effects. In contrast to the long, determined struggle against identity thieves that Solove advocates, PIDS also has the potential to eradicate identity theft quickly and inexpensively.

54. *See* LoPucki, *supra* note 6, at 123–24 (discussing scalability of PIDS).

***