VIA ELECTRONIC SUBMISSION

Electronic Privacy Information Center
1718 Connecticut Ave NW
Washington DC 20009
202-483-1140

Identity Theft Task Force, P065410
Federal Trade Commission Office / Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
taskforcecomments@idtheft.gov

January 19, 2007.

RE: Comments of the Electronic Privacy Information Center to the Federal Identity Theft Task Force, P065410

I. Introduction

The Electronic Privacy Information Center (EPIC) submits these comments regarding the growing problem of Identity Theft in the United States for consideration by the Federal Identity Task Force. EPIC is a non-profit public interest research organization founded in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, free speech and constitutional values. For many years, EPIC has played a leading role on the issue of identity theft, testifying before Congress, submitting comments to federal agencies, and urging the adoption of stronger privacy laws and more

effective technologies that would safeguard the privacy of American consumers.[1] (Law school students associated with the On the Identity Trail project of the University of Ottawa School of Law assisted in the preparation of these comments.)[2]

The crime of identity theft has reached a crisis level in American society. According to the Federal Trade Commission (FTC), the annual cost to the United States economy is over $50 billion, with $5 billion incurred by victims of identity theft.[3] Identity theft affects 10 million people each year[4] and the FTC reports that identity theft is routinely the number one complaint cited by consumers.[5] Considering the substantial economic cost of the problem and the detrimental effects that identity theft has on American society, EPIC submits that the approach proposed by the Identity Theft Task Force in its Interim Recommendations is inadequate as it fails to address the root cause of the problem. While many of the recommendations address the consequences of identity

---

[1] In 2001, EPIC Executive Director Marc Rotenberg traced the history of the SSN as an identifier and raised privacy issues associated with the Social Security Administration's Death Master File and in 2002, EPIC testified that the problem of identity theft had grown worse, with the states acting to limit collection and disclosure of the SSN. In 2003 EPIC again testified in favor of privacy protections, highlighting recent abuses, the continuing unnecessary use of the SSN as an identifier by private and public sector entities, and the developing trends of state legislation crafted to limit collection and use of the identifier. *See also*, *Social Security Numbers and Identity Theft, Joint Hearing Before the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security*, Nov. 8, 2001 (testimony of Marc Rotenberg, Executive Director, EPIC), *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; *Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves, Joint Hearing Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims*, Sept. 19, 2002 (testimony of Chris Jay Hoofnagle, Deputy Counsel, EPIC), *available at* http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html; *Hearing on Use and Misuse of the Social Security Number, Hearing Before the House Ways and Means Subcommittee on Social Security*, July 10, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, EPIC), *available at* http://www.epic.org/privacy/ssn/testinomy7.10.03.html.

[2] On the Identity Trail, http://idtrail.org/

[3] SYNOVATE, FEDERAL TRADE COMMISSION – MDENTITY THEFT SURVEY REPORT (September 2003), *available at* http://www.consumer.gov/idtheft/pdf/synovate_report.pdf.

[4] *Id*.

[5] FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT: JANUARY – NECEMBER 2005 (January 2006), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

theft, the Task Force recommendations fail to address the systemic problems that have contributed to the dramatic increase in this problem. Identity theft is a crime of opportunity. It results from the failure of organizations to adopt privacy and security practices that safeguard personal information. Minimizing the risk of identity theft is therefore most effectively achieved by reducing opportunities for the compromise of personal information. Towards this end, EPIC's strategy calls for increased data security measures and the minimization of data collection and retention by government and private entities.

In pursuit of increasing data security and reducing data collection, EPIC urges the Task Force to recognize the need for policies that force organizations to fully internalize the cost of their data collection practices, much as governments have recognized the need to require organizations to incorporate the consequences of pollution as is commonly found in environmental analyses.[6] In the context of identity theft, this argument requires policies that compel data collectors to recognize the economic and legal externalities associated with data breaches and identity theft by creating an information architecture in which security vulnerabilities and unnecessary data collection are penalized.[7] Comprehensive data security regulation would lead to the adoption of privacy enhancing technologies (PETs) that will minimize the likelihood of the misuse of personal information and the problem of identity theft. Such policies will contribute to the overall goal of minimizing the amount of data collected and retained by adjusting the incentives

---

[6] *See, e.g.*, The United Nations Conference on Environment and Development, June 3-14, 1992, *Rio Declaration on Environment and Development*, June 14, 1992, http://www.unep.org/Documents.multilingual/Default.asp?DocumentID=78&ArticleID=1163.

[7] Daniel Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003), *available at* http://ssrn.com/abstract=416740.

of data collectors. If data collectors are faced with the possibility of having to compensate victims of identity theft, they will seek to reduce their liability by reducing the amount of personal information they collect and retain. Once the true costs associated with the collection and use of personal information are recognized, innovative companies that respect privacy and seek to limit the risk of identity theft will be rewarded in the marketplace. Those companies that ignore privacy concerns and contribute to the problem of identity theft will appropriately be put out of business.

When data is collected and retained, data custodians should be responsible for data security breaches through a strict liability regime, which would make them accountable for damage and loss suffered by identity theft victims regardless of culpability or proof of fault.[8] Strict liability is generally imputed to situations considered inherently dangerous in order to discourage reckless behavior and needless loss by forcing potential defendants to take every possible precaution to prevent injury or loss.[9] In the context of identity theft, victims of data breaches are owed compensation based on the fact that a data breach increases their risk of identity theft.

A strict liability regime has the effect of simplifying litigation and allows victims to become whole more quickly. Expediency of recovery is a critical consideration for victims of identity theft whose lives may be paralyzed when they lose control of their personal information. Without public policies that make businesses and government agencies responsible for the actual costs of privacy and security, the burden of identity

---

[8] Causation is problematic in cases of identity theft because it is often impossible to know with certainty exactly where, or from whom the data was leaked or stolen.
[9] *See* PROSSER AND KEETON ON TORTS §75 (W. Keeton ed.) (5th ed, 1971).

theft will continue to fall upon its victims who must bear the costs for poorly designed systems, inadequate security practices, and the overuse of SSNs.

II. Responsible Data Collection Practices

Increasing and ensuring the security of consumer data includes limiting data collection when possible, and imposing consequences for data breaches upon organizations that collect and store personal data. PETs are one way to minimize the amount of data collected. For instance, PETs can allow authentication to occur without the need for identifying information to be disclosed. Such techniques enable commerce, communication, web browsing, and even voting without unnecessary privacy risks.

Among other recommendations, EPIC supports the establishment of a baseline national breach notification requirement as a proactive means of protecting consumers. Breach notification allows consumers the opportunity to minimize or prevent the occurrence of actual identity theft following a data breach. For example, a consumer can freeze his or her credit or carefully monitor credit records for possible identity theft once he or she has been notified that a data breach has occurred.[10] Of course, it would be preferable that credit information regarding a consumer not be disclosed unless the consumer grants affirmative consent. The federal baseline should be a credit "freeze," which would allow consumers to decide on a case-by-case basis whether to disclose information contained in a credit report. This would almost certainly reduce the occurrence of identity theft.

---

[10] Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, SECURING PRIVACY IN THE INTERNET AGE, (2005) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=650162.

Breach notification requirements demand the imposition of fines or statutory causes of action in order to promote compliance by providing an incentive for private sector entities to take reasonable steps to protect consumer data. Breach notice is a form of negative press that may be persuasive; however the imposition of fines provides a powerful economic incentive for data custodians to actively secure the data they collect and retain. Breach notification contributes to internalizing the costs of information aggregation by private sector entities, and dissuades the excessive collection of data.

The minimum national standard for breach notification should be consistent across economic sectors, business models and business sizes. Any delay that law enforcement might seek for breach notification should be limited in time to no more than 7 days. Moreover, the FTC should maintain a national database of security breach incidents so that consumers could easily determine which companies have failed to adequately safeguard personal data and so that the Commission could do a better job policing the problem.

III. Minimize Use of Social Security Numbers

In the 1974 Privacy Act Congress sought to limit the use of the Social Security Number and to prevent it from becoming a *de facto* national identifier. The Privacy Act makes it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN. Section 7 of the Privacy Act specifically provides that any agency requesting that an individual disclose his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what

statutory authority such number is solicited, and what uses will be made of it."[11] The Privacy Act makes clear Congress' recognition of the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of section 7, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." [12] Short of prohibiting the use of SSNs, the Privacy Act attempts to limit their use to those purposes where there is clear legal authority to collect SSNs.

Despite its clear purpose, the effectiveness of the Privacy Act is significantly weakened in practice by a lack of government oversight and by administrative interpretations allowing for disclosure of personal information for a "routine use" compatible with the purpose for which the information was originally collected.[13] A "routine use" does not, under subsection (a)(7) of the Privacy Act, have to be a purpose identical to the purpose for which the record was collected; it need only be a compatible purpose. This phrasing can lead to a situation in which routine uses for a particular database gradually increase until its scope is far greater than its originally stated goals.[14] This contributes to the current undue reliance on SSNs by both government and private entities, a major aspect of the identity theft problem.[15]

SSNs are prime targets for identity thieves. Reducing their collection and use will contribute to a decrease in identity theft. SSNs should only be collected when explicitly

---

[11] Privacy Act 1974, 5 U.S.C. § 552 (a) (2006).
[12] *See* EPIC, *Social Security Numbers*, EPIC.org, Jan. 17, 2006, http://www.epic.org/privacy/ssn.
[13] EPIC, PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 1060 (2006).
[14] *See* EPIC, *The Privacy Act of 1974*, EPIC.org, Aug. 26, 2003, http://www.epic/org/privacy/1974act/.
[15] EPIC has highlighted this problem on a number of occasions. *See* Rotenberg, *supra* note 1.

authorized by law for social security and taxation purposes. An employer should be permitted to ask an employee for his or her SSN for tax-reporting purposes (assuming the SSN remains the Taxpayer Identification Number), but a health club should not be permitted to ask a customer for his or her SSN as a condition of membership. The difficulty with SSNs is that they are currently used both to identify an individual and to authenticate that individual, two distinct functions. Using the SSN as both the identifier and authenticator is equivalent to using an identical password and user name when signing into an email account.

EPIC supports the Task Force's recommendation to reduce reliance on SSNs at all levels of government. Reducing use of SSNs and limiting the amount of data collected by government bodies is fundamental to maintaining the security of consumer data. This is an especially critical limitation upon the public sector, since government has the power to compel individuals to disclose personally identifiable information. The personal data collected by government entities should never be disseminated in public records or sold to the private sector. The Task Force should curtail the publicly available sources of the SSN, including the Social Security Death Register; bankruptcy filings and other court records; birth and death records; and records of other life events.

The Task Force should also carefully investigate and analyze SSN use in the private sector, as there is evidence that private sector use of SSNs contributes substantially to the problem of identity theft. Restricting the sale, purchase and display of SSNs by private entities is a critical consideration in combating identity theft. The private sector must move away from using SSNs as identifiers, a goal which is feasible as

demonstrated by Empire Blue Cross' transition from SSNs to alternative identification numbers for its 4.8 million customers.[16]

The SSN permits the aggregation of personal information, allowing for the combination of seemingly innocuous data from different sources that together can reveal a great deal about an individual's personal life:[17]

> With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes. The profile includes personal identifying information (name, alias name, date of birth, social security number), all known addresses, drivers license information, vehicle information ... telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapons permits, liens, judgments, lawsuits, marriages, worker compensation claims, etc.[18]

The Task Force should examine existing state laws aimed at limiting the collection and use of SSNs by commercial entities. In January 2002, a statewide grand jury empanelled by the Florida Supreme Court found in its first report that:

> We have identified that the government and business take in much more information than necessary to conduct business. For example health clubs require members to disclose their social security numbers on applications for

---

[16] *Empire Blue Cross Will End Use of SSNs, Use Alternate Number System,* Privacy and Security Law Report (Jun. 7, 2004) at 666 *available at* http://www.empireblue.com/wps/portal/ehpvisitor?content_path=shared/noapplication/f0/s0/t0/pw_ad069546.htm&label=May%2028,%202004.

[17] For example, research at the Carnegie Mellon Laboratory for International Data Privacy has shown that 87% of the United States population can be uniquely identified with just a few pieces of personal information, for example, zip code, gender and date of birth. Information collected and stored for one purpose can be combined with information collected and stored for a completely different purpose through data mining. *See* Latanya Sweeney, Comments to the Department of Health and Human Services on Standards of Privacy of Individually Identifiable Health Information April 26, 2002, http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.html. *See also* Latanya Sweeney, *Protecting Job Seekers from Identity Theft*, 10 IEE INTERNET COMPUTING 2, 74 (2006), and Latanya Sweeney, *AI Technologies to Defeat Identity Theft Vulnerabilities*, AAAI SPRING SYMPOSIUM: AI TECHNOLOGIES FOR HOMELAND SECURITY (2005), http://privacy.cs.cmu.edu/dataprivacy/projects/idangel/idangel1.pdf (describing Sweeney's Identity Angel, a technology that searches the internet and notifies "people for whom information, freely available on the Web, can be combined sufficiently to impersonate them in financial or credentialing transactions).

[18] Sole Source Justification for Autotrack (Database Technologies) (n.d.) (document obtained from the USMS), *available at* http://epic.org/privacy/choicepoint/cpusms7.30.02j.pdf.

> membership; video rental stores ask for social security numbers on applications; and life insurance companies ask for social security numbers of beneficiaries; local governments ask for social security numbers on routine transactions. We were distressed to learn from the Interim Project Report by the Committee on State Administration and Committee on Information Technology that 96.3% of state agencies do not even have a written policy relating to the collection of social security numbers. This same report indicates that 63% of these agencies disclose social security numbers on some public record requests.
>
> Medical service providers and insurance companies routinely substitute social security numbers for patient or policy numbers, unnecessarily exposing this sensitive information to scrutiny on such documents as health and insurance cards. Unsecured mailboxes and trash containers provide thieves with easy access to this personal information.[19]

The Task Force must respond to this call to action by establishing regulations to discourage private sector use of SSNs and encourage adoption of alternative identifiers. In many cases, the collection of SSNs by private organizations is not necessary. Congress should act swiftly to curb such practices.

EPIC supports the use of alternative identifiers by both commercial and government entities. Alternative identifiers contribute to internalizing the costs of data collection by placing the burden on the data collector to create, maintain and secure a database of alternative identifiers. An example of an alternative identifier to the SSN is the bank account system. A bank account number identifies the individual's bank record, while a separate password or personal identification number (PIN) is used to authenticate the individual. The PIN is a password known only to the individual.

---

[19] *Identity Theft in Florida, First Interim Report of the Sixteenth Statewide Grand Jury*, SC 01-1095 (Fla. Jan. 2002), *available at* http://myfloridalegal.com/pages.nsf/4492d797dc0bd92f85256cb80055fb97/758eb848bc624a0385256cca0059f9dd!OpenDocument.

IV. Develop Better Security Practices

Once consumer data has fallen into the hands of an identity thief, the potential for its misuse is proportionate to the extent that the information can be used for illegitimate authentication. The Task Force's Interim Report recommends developing more reliable methods of authenticating identities in order to prevent misuse of consumer data. Rather than promoting reliability through universal identifiers, EPIC advocates the distribution of identity or an identity metasystem in which authentication is confined to specific contexts in order to limit the scope for potential misuse. The danger of a single identifier is that the harm will be magnified when it is compromised. A system of distributed identification reduces the risks associated with security breaches and the misuse of personal information.

Universal identifiers, including biometrics, will not solve the fundamental problem of how much damage an identity thief can do once a victim's identifiers are compromised.[20] Biometric authentication involves comparing the previously captured physical characteristics of a consumer with newly provided samples of that same characteristic.[21] EPIC has previously warned that biometric identification will create new, more severe identity theft problems.[22] Among other considerations, biometric identifiers have elaborate enrollment requirements that create new vulnerabilities when,

---

[20] Universal identifiers have also generated significant criticism on grounds of human rights. *See, e.g.* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U.J. SCI. & TECH L. 37, 48 (2002). *See also* National Research Council, IDS – HOT THAT EASY: QUESTIONS ABOUT NATIONWIDE IDENTITY SYSTEMS, (Stephen Kent & Lynette Millett eds. 2002), *available at* http://www.nap.edu/catalog/10346.html?opi_newdoc041102.

[21] PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 49 (EPIC ed., 2006).

[22] EPIC, *Comments Use of Biometrics to Curb Identity Theft to the Department of Treasury*, 2004, http://www.epic.org/privacy/biometrics/factabiometrics.html.

for example, authenticating documents are collected. Biometrics are also difficult to reissue when they are compromised. Government agencies have also urged caution in the use of biometric identifiers.[23] While biometric technologies may improve the reliability of authentication when compared with alpha-numeric alternatives, universal identifiers increase the potential for misuse once biometric data has been illegitimately obtained.[24]

For example, a fingerprint can be used as a universal identifier to authenticate a consumer. While a fingerprint may be more difficult for thieves to obtain than a traditional password, it remains vulnerable to anyone with sufficient motivation and expertise.[25] A stolen fingerprint would prove enormously valuable to an identity thief should it become a widely adopted authentication method. Increasing the value of identifiers inevitably attracts a professional, international criminal fringe.[26] Moreover, a biometric identifier cannot be changed by a victim once his or her identity has been breached – a fingerprint is unalterable. Any move towards universal identifiers, while potentially deterring amateur identity thieves, increases the potential for misuse once that data is stolen.

Alternatively, a banking PIN number, in conjunction with a bank card, provides a better authentication system because it is not coupled with a single, immutable consumer identity. If a bank card and PIN combination is compromised, a new bank card and PIN

---

[23] *See, e.g.,* Keith A. Rhodes, General Accounting Office, *Challenges in Using Biometrics* (testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives), September 9, 2003, *available at*: http://www.gao.gov/new.items/d031137t.pdf.
[24] Simon Davies, *The Id Card is the Fraudster's Friend*, THE SUNDAY TELEGRAPH, July 7, 2002. *See also*, Oscar H. Gandy, Jr., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993).
[25] Robert Lemos, *This hacker's got the gummy touch*, CNET.COM (2002), http://news.com.com/2100-1001-915580.html.
[26] Kim Cameron, *The Laws of Identity,* IDENTITY WEBLOG, Dec. 9, 2004, http://www.identityblog.com/stories/2004/12/09/thelaws.html.

number can be issued and the old combination cancelled, limiting the damage done by the compromised data. Drawbacks of such structures, including the possibility for the existence of multiple cards, are currently being addressed by the creation of an identity metasystem in which multiple identities can be loosely coupled within a single secure system.[27]

Distributing identity in this way allows for different profiles to be used in different authenticating contexts. New profiles can be created as required within a single identity metasystem. Misuse is therefore limited to the context of the information breached, whether it is a single bank account, online merchant, or medical records.

Possibilities for data misuse can also be limited at the data collection stage. EPIC has previously called attention to the need for websites to stop storing customer credit card information.[28] Amassing large databases of credit card numbers creates an attractive target for potential identity thieves. One simple response to identity theft is to require a PIN to be used in conjunction with all credit cards. An identity metasystem would further reduce the value of such aggregated database targets because authenticators would be separate and distinct from all personally identifiable information.

Finally, technological measures can be used to improve the reliability of authentication while respecting consumer privacy. International research efforts are currently underway to create authentication systems that preserve anonymity, and include the development of new PETs for use in such schemes.[29] These PETs allow for the

---

[27] *Id.*
[28] EPIC, *Identity Theft: Causes and Solutions,* EPIC.ORG, 2006, http://www.epic.org/privacy/idtheft/.
[29] See, e.g., Carlisle Adams, Delegation and Proxy Services in Digital Credential Environments, Presented at the 7th *Annual Privacy and Security Workshop Your Identity Please: Identity Theft and Identity*

separation of authentication and identification and are being deployed in response to security vulnerabilities. Such technologies may plug-in to identity metasystems, such as Microsoft's CardSpace.[30] While the default settings of Cardspace do not currently meet recognized standards for privacy preservation,[31] this model should be studied in detail during the Task Force's workshops on authenticating technologies.[32]

It bears repeating that the misuse of stolen consumer information can be minimized by tying authentication to a specific context rather than promoting universal identifiers. Even strong biometric identifiers can be stolen, presenting an undue burden on victim recovery.

V. Ensure Meaningful Privacy Remedies

The Task Force identifies the goal of victim recovery in the context of identity theft as making the victim whole, an objective which may include both monetary compensation and other reparations that aim to restore a victim's privacy to the greatest extent possible. Non-monetary compensation should include a victim's ability to access and correct personal data that may have been falsified by the identity thief. EPIC has

---

Management in the 21st Century, (Nov. 2, 2006), http://www.idtrail.org/files/cacrwkshpdigcred02nov06.pdf; Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management,* in PROCEEDINGS OF THE 3RD ANNUAL PKI R&D WORKSHOP (Apr. 2004), http://www.idtrail.org/files/cross_domain_identity.pdf; David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, in SECRET-BALLOT RECEIPTS: TRUE VOTER-VERIFIABLE ELECTIONS, National Institute of Standards and Technology (May 19, 2004); Paul Van Oorschot and S. Stubblebine, *Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling* in FINANCIAL CRYPTOGRAPHY AND DATA SECURITY (2005), available at http://www.scs.carleton.ca/~paulv/papers/pvoss6-1.pdf.

[30] Wikipedia Contributors, *CardSpace*, WIKIPEDIA: THE FREE ENCYCLOPDIA, Jan. 12, 2007, http://en.wikipedia.org/wiki/CardSpace.

[31] Stefan Brands, *User centric identity: boon or worst nightmare to privacy?,* THE IDENTITY CORNER, Nov. 17, 2006, http://www.idcorner.org/?p=142.

[32] *See generally*, National Research Council, WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY (2003).

previously called attention to the importance of providing rights and assistance to identity theft victims and in light of the current prevalence of this crime, victim rights and restitution have become increasingly important.[33] Privacy laws that establish a right of access and correction help reduce the risk of identity theft by ensuring that individuals are able to routinely able to access their personal information that is held by third parties.

The International Organization for Economic Cooperation and Development (OECD) *Privacy Guidelines* (1980) are unequivocal on the issue of access and correction rights. In the Annex entitled *Guidelines Governing the Protection of privacy and the Transborder Flows of Personal Data*, section 13(d) states, "[a]n individual should have the right: to challenge data relating to him (sic) and, if the challenge is successful, to have the data erased, rectified, completed or amended." Similar provisions guaranteeing rights of access and correction exist with respect to education records[34] and medical files.[35] Making victims of identity theft whole must include access and correction rights, providing victims with the ability to quash personal information that is incorrect, and to control their stored personal information. Fair Information Practices recognized and enforced in other contexts, including credit reporting, could provide an important template for ensuring access and correction rights to victims of identity theft.[36]

---

[33] EPIC, *Request to State Attorneys General to Act to Assist Identity Theft Victims in Using New Federal Rights*, EPIC.ORG, Jan. 15, 2004, http://www.epic.org/privacy/fcra/factagltr1.15.04.pdf.
[34] *Federal Education Records and Privacy Act* 20 USC 1232g (1993), regulations at 34 CFR 99 (1993). *See*, David A. Banisar, *Privacy of Education Records*, January 1994, *available at* http://www.epic.org/privacy/education/school.html.
[35] *Health Insurance Portability and Accountability Act*, *Privacy Rule* 45 CFR Parts 160 and 164 (2003). *See Medical Privacy*, http://www.epic.org/privacy/medical/.
[36] EPIC, *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*, EPIC.ORG, http://www.epic.org/privacy/fcra/.

The *Fair Credit Reporting Act* (FCRA) and amendments contained in the *Fair and Accurate Credit Transactions Act* (FACTA) are intended to promote accuracy, fairness and the privacy of personal information assembled by Credit Reporting Agencies (CRAs).[37] The FCRA requires CRAs to follow "reasonable procedures" to protect the confidentiality, accuracy, and relevance of credit information, and establishes a framework of practices for personal information that includes some rights of data quality (right to access and correct), data security and use limitations.[38] Under this legislation, consumers have the right to access their credit files and may dispute inaccurate information that appears in a credit report. The FACTA provides consumers with additional rights to accurate furnishing and reporting of credit information.

The FCRA and the FACTA are valuable as models of the kind of rights that would be useful both to victims of identity theft and to consumers who have not yet suffered the crime of identity theft. Recognizing a consumer's rights as against any data custodian holding his or her personal information, including rights to data quality, security and accountability, would allow victims of identity theft to quickly regain some measure of control over their personal information following an identity theft, and would permit victims to monitor and correct any fraudulent information stored in databases as a result of identity theft.

The Task Force has issued a recommendation that Congress allow victims of identity theft to seek restitution from the identity thief for the value of their time in attempting to recover from the effects of the identity theft. Victims should have access to

---

[37] *Id.*
[38] *Id.*

restitution from identity thieves, however this avenue alone will not always be a feasible option. There must be alternate ways for victims to pursue restitution that correspond to the risks created by data collection practices.

The imposition of agency fines, whereby data collectors are held liable for breaches of data security regardless of whether proof of causation of identity theft has been shown, should be a key aspect of responsible data security practices.[39] Mandatory notification laws already exist in a number of states.[40] No harm need be proven in order for a data custodian to be fined; once a data breach or leak of any sort has occurred, the collector or holder of that information is liable. Amounts for damages could be determined by the Credit Watch Plans sold by various credit bureaus. Agency fines, along with money from identity theft insurance plans could be paid into a central fund upon which victims of identity theft could draw in the course of re-building their identities post-theft.[41] Agency fines provide a further disincentive for excessive data collection and storage by data custodians.

A further consideration in victim recovery is the means by which identity theft victims may authenticate their identities when mistaken for the identity thief. The Task Force has proposed recommendations, including passport-like identity documents, and a

---

[39] Data security breaches are remarkably commonplace. A recent Ponemon Institute survey reports that 81% of companies and governmental entities report having lost or misplaced one or more electronic storage devices such as laptops containing sensitive information within the last year. Another 9% did not know if they had lost any such devices. PONEMON INSTITUTE, *U.S. Survey: Confidential Data at Risk*, Aug. 15, 2006, http://www.vontu.com/uploadedFiles/global/Ponemon-Vontu_US_Survey-Data_at-Risk.pdf#search=%22ponemon%20vontu%22.

[40] *See, e.g.*, California Security Breach Information Act, CAL. CIV. CODE § 1798.82 and 1798.82 (West 2003) *available at* http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

[41] If data collectors are liable for identity theft and data breaches, we assume that they would have the option of taking out insurance to limit this liability.

voluntary identity database to address this issue. Allowing identity theft victims to authenticate through these secondary or "superior" identity mechanisms is problematic because, like the stolen identity documents themselves, they equate identity and authentication. These solutions therefore pose the same risks as the identity that has been stolen.

The Task Force's recommendation of creating a system to allow identity theft victims to avoid being mistaken for the identity thief or someone else would certainly assist victims, however, it is critical that such a scheme not rely solely on the authentication of a victim's identity. A victim should be able to authenticate him or herself as distinct from the records related to the identity theft. For example, if a victim of identity theft finds that an arrest warrant has been issued in his or her name, he or she should be able to authenticate as *not* the person for whom the arrest warrant is issued.

This approach is preferable to one where a victim is forced to identify as a legitimate person according to the stolen documents. Contextualizing authentication in this way is critical to breaking the connection between identity and authentication, which is highly problematic and increases opportunities for identity theft. Further, a move away from remedying identity theft by producing more identity documents for authentication contributes to the overarching goal of data minimization

VI. Conclusion

The Identity Theft Task Force has, with its Interim Recommendations, advanced a series of proposals to address the consequences of identity theft. This approach fails to acknowledge that the root of identity theft lies not with consumers or identity thieves, but

with government and private agencies that collect and store excessive amounts of often unnecessary personal information in systems that lack adequate privacy and security safeguards. The best long-term approach to the problem of identity theft is to minimize the collection of personal information and to develop alternative technologies and organizational practices that make authentication without identification possible. If the data is not "out there" in the first place, the opportunities for data leaks and identity theft are drastically reduced.

Proceeding from the premise that a proper policy framework will encourage businesses and government agencies to develop record keeping practices that are less dependent on the collection of personally identifiable information, the proposals advanced here by EPIC aim to reduce the overall collection of personal information leading to an immediate reduction in identity theft. When data collection is absolutely necessary, appropriate security measures must be developed, implemented and enforced by data custodians, thereby internalizing the costs of identity theft. Moreover, the adoption of comprehensive privacy laws and the development of innovative techniques that separate identification from authentication may provide the best long-term solution to the ongoing challenge of safeguarding privacy in the digital age.

EPIC urges the Task Force to address the underlying factors that have contributed to the dramatic increase of identity theft in the United States – the externalization of costs for security breaches and weak privacy safeguards; the absence of comprehensive privacy laws that impose clear obligations on data holders to protect the privacy of data subjects; and the failure to encourage the development of genuine Privacy

Enhancing Technologies that would minimize or eliminate the collection of personally identifiable information.

Identity theft has quickly become one of the leading problems in the United States. The impact on American consumers is far-reaching, severe, and likely to get worse. The Task Force Interim Recommendations, while generally helpful, may simply be too little, too late.

Marc Rotenberg
EPIC Executive Director

Guilherme Roschke
EPIC Skadden Fellow

Jeremy Hessing-Lewis
Law Clerk

Jena McGill
Law Clerk

Felix Tang
Law Clerk