No. 08-108

IN THE

Supreme Court of the United States

IGNACIO FLORES-FIGUEROA,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On a Writ of Certiorari
to the United States Court of Appeals
for the Eighth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF THE PETITIONER

MARC ROTENBERG
Counsel of Record
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

December 22, 2008

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

INTEREST OF THE AMICI CURIAE 1

SUMMARY OF THE ARGUMENT 7

ARGUMENT 8

1.Identity Management is a Field in Information Science that Concerns Assignment of Attributes and Credentials so as to Promote Privacy and Security 8

2."Identity Theft" has a Well Understood Meaning in the Technical Community 10

3.The Definition of "Identity Theft" Does Not Include the Unknowing Use of Inaccurate Credentials 15

A. The Application of Section 1028A's Knowledge Requirement to All the Section's Terms is Consistent with the Technical Definition of "Identity Theft" 18

B. Failure to Apply Section 1028A's Knowledge Requirement to All the Section's Terms is Inconsistent with the Technical Definition of "Identity Theft" 19

CONCLUSION 26

TABLE OF AUTHORITIES

CASES

Flores-Figueroa v. United States, 274 Fed. Appx. 501, (8th Cir. 2008), cert. granted, 2008 U.S. LEXIS 7827 (U.S. October 20, 2008) (No. 08-108) 20

Guy Montag Doe v. San Francisco Housing Authority, No. 08-03112 (N.D. Cal. Filed June 27, 2008) 22

Roe v. Wade, 410 U.S. 113 (1973) 22

United States v. Mendoza-Gonzalez, 520 F.3d 912 (8th Cir. 2008) 20

STATUTES

18 U.S.C. § 1028A (2008)..... 17, 18, 19, 20

OTHER AUTHORITIES

About PRIME – Portal for the PRIME Project, https://www.prime-project.eu/about..... 9

Andreas Pfitzmann and Marit Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, TU Dresden Faculty of Computer Science, Feb. 15, 2008 8

At Checkpoints in Baghdad, Disguise Is a Lifesaving Ritual, Wash. Post, Sept. 29, 2006 20

BARRON H. LERNER, WHEN ILLNESS GOES PUBLIC (2006) 23

BBC History – George Eliot (1819-1880), http://www.bbc.co.uk/history/historic_figures/eliot_george.shtml..... 22

Brief for the United States at 2-3, *Flores-Figueroa v. United States*, No. 08-108 (U.S. Sept. 19, 2008) 16, 17, 18

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 Management in the 21st Century* (Nov. 2, 2006) 12

David Chaum *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, Communications of the ACM (Oct. 1985) 23, 24

David Chaum, *Achieving Electronic Privacy*, Scientific American (Aug. 1992) 24

David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Presented at ITL Seminar Series, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Nat'l Inst. of Standards & Tech. (May 19, 2004) 12

David Chaum, *Signatures Transferred Between Unconditionally Unlinkable Pseudonyms* (1986) 24

Denise I. Smith and Renee E. Spraggins, U.S. Census Bureau, *Gender: 2000*, Sept. 10, 2001 14

Dozens killed in Baghdad attacks, BBC, July 9, 2006 20

Global 500 2008: Wal-Mart Stores, CNNMoney.com, http://money.cnn.com/magazines/fortune/global500/2008/snapshots/2255.html 14

H.R. Rep. No. 108-528 (2004) 19

Harris County Public Library – About – Internet Safety, http://www.hcpl.net/about/internetsafety.htm 24

ID Theft Project, *US: 2 go to prison in identity theft*, Nov. 12, 2008 ..... 13, 14

Identity Management – Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Identity_management 8

Jerry Kang, *Cyberspace Privacy: A Primer and Proposal*, 26 Hum. Rts. 3 (1999) 10

Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998) 10

Letter from EPIC, Privacy International, and Human Rights Watch to Secretary Robert M. Gates, U.S. Department of Defense (July 27, 2007) 20

LUNA, HOW TO BE INVISIBLE (2004) 16

Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 Tex. L. Rev. 89 (2001) 10

Marie Price, *Grand jury in OKC indicts for bank fraud, identity theft*, Oklahoma City Journal Record, Sep 10, 2007 13

Nat'l Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (2003) 10, 11, 12, 13, 15, 24

National Electronic Commerce Coordinating Council, *The Technology of Identity: A Primer & Resource Guide* (Dec. 2006) 9

Office of the Inspector General, U.S. Social Security Administration, *Review of Universities' Issuance of Temporary Social Security Numbers to Foreign Students* (April 2004) 21

Paul Van Oorschot and S. Stubblebine, *Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling*, Fin. Cryptography & Data Sec. (2005) 12

Petition for a Writ of Certiorari at 4, *Flores-Figueroa v. United States*, No. 08-108 (U.S. July 22, 2008) 16, 18

RAY BRADBURY, FAHRENHEIT 451 (1953)..... 22

ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2000) 22

Social Security Administration, "Which Social Security numbers are invalid (impossible)?" (Answer ID 425) http://ssa-custhelp.ssa.gov/cgi-bin/ssa.cfg/php/enduser/std_adp.php?p_faqid=425..... 16

Stefan Brands, *A Primer on User Identification*, Panopticon, The 15th Annual Conference on Computers, Freedom & Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle (April 12, 2005) 10

Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004) 12

U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, (Mar. 2002) 10

U.S. Marshals Service Talks WitSec to the World, America's Star:FYI, Aug. 2006..... 23

INTEREST OF THE *AMICI CURIAE*[1]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values. EPIC has participated as *amicus curiae* in several cases before this Court and other courts concerning privacy issues, new technologies, and Constitutional interests, including *Herring v. United States*, 492 F.3d 1212 (11th Cir. 2007), *cert. granted* 76 U.S.L.W. 3438 (Feb. 19, 2008) (No. 07-513); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *National Cable and Telecommunications Association v. Federal*

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. On December 12, 2008, Petitioner filed with the Court his "Consent to the filing of amicus briefs, in support of either party or neither party." *Amici* lodged with the Court Respondent's letter of consent contemporaneous with the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Communications Commission, No. 07-1312 (D.C. Cir. filed Aug. 7, 2007); *Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a particular interest in the proper interpretation and application of identity theft statutes. Several members of the EPIC Advisory Board are leading experts in the development of identity management systems, computer security protocols, encryption standards, and other related technical measures that seek to minimize the risk of identity theft while ensuring privacy and security. EPIC supports the right of individuals to remain anonymous or pseudonymous, as well as to submit fictitious, incomplete, or inaccurate information in response to invasive or unnecessary demands for personal information, as long as the individual does not knowingly impersonate someone else or intend harm to someone else.[2]

---

[2] *See, e.g., Brief of Amicus Curiae Electronic Privacy Information Center, American Civil Liberties Union, American Civil Liberties Union of Ohio and 14 Legal Scholars in Support of Watchtower Bible, etc, Petitioners*, *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002) (No. 00-1737) *available at* http://www.epic.org/anonymity/watchtower.pdf (supporting First Amendment Right to anonymous door-to-door speech); *Brief of Amicus Curiae Electronic Privacy Information Center*, *Peterson v. National Telecommunications and Information Association*, 478

EPIC has also routinely urged lawmakers, regulators, and courts to take meaningful steps to curb identity theft.[3]

The Eighth Circuit's determination in the present case threatens to impose aggravated identity

---

F.3d 626 (4th Cir. 2007) (Nos. 06-1216, 06-1548) *available at* http://www.epic.org/privacy/peterson/epic_peterson_amicus.pdf (supporting First Amendment Right to anonymity in Internet domain name registrations); Letter from EPIC, Privacy International, and Human Rights Watch to Secretary Robert M. Gates, U.S. Department of Defense (July 27, 2007) *available at* http://www.epic.org/privacy/biometrics/epic_iraq_dtbs.pdf (supporting Iraqi nationals who change their names or carry fake IDs to avoid being murdered by rival sects).

[3] *See, e.g.*, Marc Rotenberg, EPIC Executive Dir., *Statement Before Joint Session of the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security*, 109th Cong. (Nov. 8, 2001) *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; *Comments of the Electronic Privacy Information Center to the Federal Trade Commission*, ID Workshop Comment P075402, Mar. 23, 2007, *available at* http://epic.org/privacy/id-cards/epic_ftc_032307.pdf; *Brief of Amici Curiae AARP, ACLU of Northern California, California Public Interest Research Group, Consumer Federation of California, Consumers Union, Electronic Privacy Information Center, Evan Hendricks, National Association of Consumer Attorneys, Privacy Rights Clearinghouse, and US PIRG, in Support of Defendant-Appellees, Supporting Affirmance*, *American Bankers Assoc. v. Lockyer*, 541 F.3d 1214 (9th Cir. 2004) (Nos. 05-17163, 05-17206) *available at* http://epic.org/privacy/preemption/lockyer_brief.html.

theft penalties on individuals who use fictitious identities but do not intend to impersonate someone else. The outcome is inconsistent with the widely understood meaning of "identity theft." EPIC believes that the Congressional statute accurately reflected this distinction and was therefore misapplied in this case where a person was convicted of aggravated identity theft even though he did not intend to impersonate someone else.

Technical Experts and Legal Scholars

Steven Aftergood
Project Director, Federation of American Scientists

Anita Allen
Professor of Law and Professor of Philosophy, University of Pennsylvania

Christine L. Borgman
Professor & Presidential Chair in Information Studies, UCLA

Stefan Brands
Principal Architect (Identity & Security), Microsoft

David Chaum
Chaum, LLC

Bill Coleman
Founder, CEO & Chairman, Cassatt Corporation

Whitfield Diffie, Dr. sc. techn. (hc)
Chief Security Officer, Sun Microsystems

Addison Fischer
Former owner, RSA Data Security
Co-founder, Verisign

Chris Larsen
CEO, Prosper Marketplace

Mary Minow
Library Law Consultant

Pablo G. Molina
Associate VP of IT and Campus CIO, Georgetown University

Peter G. Neumann
Principal Scientist, SRI International Computer Science Lab

Dr. Deborah C. Peel
Founder and Chair, Patient Privacy Rights

Anita Ramasastry
Professor, University of Washington School of Law

Bruce Schneier
Security Technologist

Robert Ellis Smith

Publisher, *Privacy Journal*

Frank M. Tuerkheimer
Professor of Law, University of Wisconsin Law School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The statute under consideration by the Court was intended to punish intentional, fraudulent impersonation of another, not the creation of partly fictitious documents to receive employment or public benefits. This distinction is crucial, not only to the proper application of federal law, but also to the development of appropriate techniques to safeguard privacy and security. The Court should not set a precedent that might inadvertently render the use of privacy enhancing pseudonyms, anonymizers, and other techniques for identity management unlawful. Such an outcome could result in an increase in identity theft and undermine the very purpose of the statutory provision.

ARGUMENT

I. "Identity Theft" is Defined as the Knowing Impersonation of Another

The term "identity theft" has a specific meaning among technologists, academics, security professionals, and other experts in the field of identity management, which is reflected in the statute under consideration by the Court. It refers to the knowing impersonation of one person by another. The unknowing use of inaccurate credentials does not constitute identity theft.

A. Identity Management is a Field in Information Science that Concerns Assignment of Attributes and Credentials so as to Promote Privacy and Security

Identity management is a relatively young field in Information Science.[4] Identity management involves managing individuals' various partial identities, often expressed as pseudonyms, and addresses the establishment, description, activity,

---

[4] Andreas Pfitzmann and Marit Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, TU Dresden Faculty of Computer Science, Feb. 15, 2008 at 6 *available at* http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.doc.

and destruction of identities.[5] The field recognizes that "all social and economic interactions between human beings in modern civilization require the exchange of some personal data," and endeavors to resolve the privacy and security issues that arise from these interactions through the use of identity management systems.[6] Identity management systems are commonly encountered in everyday life. They are generally used to control access to valuable assets or space, facilitate interactions or transactions, or track the locations of people or things.[7]

One example of identity management is the use of passwords or PIN numbers by Internet web sites and banks.[8] Other identity management systems are

---

[5] *Id.* at 31 (stating "identity management means managing various partial identities (usually denoted by pseudonyms) of an individual person, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re) used in a specific context or role."); *see also* Identity Management – Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Identity_management (last visited Dec. 16, 2008).

[6] About PRIME – Portal for the PRIME Project, https://www.prime-project.eu/about (last visited Dec. 16, 2008).

[7] National Electronic Commerce Coordinating Council, *The Technology of Identity: A Primer & Resource Guide* (Dec. 2006) at 4, *available at* http://www.ec3.org/downloads/workgroups/2006/Technology%20of%20Identity%20-%20white%20paper.pdf.

[8] *Id.* (stating "One of the most ordinary examples of using the technology of identity is that of logging onto a website, desktop or network that requires a PIN or username and password.").

used to confirm credit card transactions, issue electronic airline tickets, and pay for highway tolls.[9] Effective identity management systems must provide security and protect individuals' privacy.[10] Identity management systems are also designed to prevent identity theft.

B. "Identity Theft" has a Well Understood Meaning in the Technical Community

Data security specialists use precise terms to describe identity authentication and identity theft, insisting that "a common understanding and consistent use of . . . terms . . . are a prerequisite for informed discussion."[11] "Identity theft" involves the knowing impersonation of one person by another.[12]

---

[9] Nat'l Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (2003) at 23-25.

[10] *Id.* at 28, 178; Stefan Brands, *A Primer on User Identification*, Panopticon, The 15th Annual Conference on Computers, Freedom & Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle (April 12, 2005) *available at* http://www.idtrail.org/content/view/21/42/ at 4-12.

[11] *Id.* at 2.

[12] *See, e.g., Id.* at 99 ("Identity theft occurs when someone usurps a portion of another person's personal identifying information in order to pose as that person." emphasis added); Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1215 n. 84 (1998) (stating "[i]n identity theft, an impostor obtains enough personal information to impersonate his victim in financial transactions."); Jerry Kang, *Cyberspace Privacy:*

Identity theft is characterized by the use of numerous attributes that describe the identity theft victim, usually including "some combination of name, address, Social Security Number, mother's maiden name, password, credit card number, date of birth, driver's license number, and employer."[13] Identity theft goes beyond the theft of one of the victim's attributes "to the misappropriation of a person's very identity."[14]

The definition of identity theft stems from a crucial distinction between "identity" authentication and "attribute" authentication.[15] The distinction is critical; many authentication systems provide security while preserving anonymity by allowing for

---

A Primer and Proposal, 26 Hum. Rts. 3 (1999) ("personal data can be used to commit identity theft, in which an impostor creates fake financial accounts, runs up enormous bills, and disappears leaving only a wrecked credit report behind."); Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 Tex. L. Rev. 89, 90 (2001) (defining "identity theft" as "any impersonation of a specific individual."); *but see* U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, (Mar. 2002) at 5 n. 7 *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-02-363 ("the Secret Service defined 'identity theft' as any case related to the investigation of false, fraudulent, or counterfeit identification; stolen, counterfeit, or altered checks or Treasury securities; stolen, altered, or counterfeit credit cards; or financial institution fraud.").

[13] *Who Goes There?*, note 9 *supra,* at 99.

[14] *Id.*

[15] *Id.* at 19-20. (distinguishing between "individual authentication" and "attribute authentication").

the separation of attributes and identification.[16] In simple terms, this can be understood when a member of a health club, for example, is granted access to the club on the presentation of a credential that certifies membership. The individual's actual identity is not necessary for the entry determination; it is the presentation of the credential that provides the basis for the determination.

Identity authentication involves "establishing … confidence that an identifier refers to an identity."[17] Attribute authentication establishes "confidence that an attribute applies to a specific individual."[18]

---

[16] *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 Management in the 21st Century* (Nov. 2, 2006), *available at* http://www.idtrail.org/files/cacrwkshpdigcred02nov06.pdf; Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), *available at* http://www.idtrail.org/files/cross_domain_identity.pdf; David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Presented at ITL Seminar Series, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Nat'l Inst. of Standards & Tech. (May 19, 2004); Paul Van Oorschot and S. Stubblebine, *Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling*, Fin. Cryptography & Data Sec. (2005), *available at* http://www.scs.carleton.ca/~paulv/papers/pvoss6-1.pdf.

[17] *Who Goes There?*, note 9 *supra,* at 2.

[18] *Id.*

An identity is "a set of information about an individual that is associated with that individual."[19] Identities "consist of more than just names," and "include other [identifying] facts," such as biographical data.[20] Attributes are "propert[ies] associated with an individual," including physical attributes and job status.[21]

The technical definitions demonstrate that "identity theft" involves the improper impersonation of another individual, complete with the theft of the "set of information about an individual that is associated with that individual" and "the misappropriation of a person's very identity." A person who uses many attributes belonging to another individual is likely to be an identity thief. In contrast, the use of a false, incomplete, or inaccurate attribute, which may or may not belong to another individual, would not generally be considered identity theft. A person who uses many attributes that belong to another individual is more likely to be committing identity theft than a person who uses a single attribute that may or may not belong to another.

For example, in 2007, a criminal ring impersonated others in an effort to obtain credit from merchants and defraud their creditors – they are plainly identity thieves.[22] To execute the scam, the

---

[19] *Id.* at 20.

[20] *Id.*

[21] *Id.* at 19, 43.

[22] Marie Price, *Grand jury in OKC indicts for bank fraud, identity theft*, Oklahoma City Journal Record, Sep 10, 2007 *available at* http://findarticles.com/p/articles/mi_qn4182/is_/ai_n19516519; ID Theft Project, *US: 2 go to prison in identity theft*,

thieves fraudulently obtained driver's licenses and Social Security cards, produced fake ID's in the victims' names, and created counterfeit checks linked to the purloined identities.[23] These activities involve misappropriation of many elements in the "set of information about an individual that is associated with that individual" and constitute "the misappropriation of a person's very identity."

The use of another individual's single attribute is altogether different. Many individuals share attributes. For example, the most recent census indicates that 138.1 million "men" live in the U.S.[24] Millions of American males cannot be branded "identity thieves" for listing their gender attribute on ID documents. Similarly, Wal-Mart employs approximately 2,055,000 individuals.[25] An unemployed young man may be up to mischief if he tells his date that he is a "Wal-Mart employee." But he is not an identity thief.

Nov. 12, 2008 *available at* http://www.id-theftprotect.com/news.php?news_id=258&news_keyword=identity%20theft.

[23] *Id.*

[24] Denise I. Smith and Renee E. Spraggins, U.S. Census Bureau, *Gender: 2000*, Sept. 10, 2001 *available at* http://www.census.gov/prod/2001pubs/c2kbr01-9.pdf.

[25] Global 500 2008: Wal-Mart Stores, CNNMoney.com, http://money.cnn.com/magazines/fortune/global500/2008/snapshots/2255.html (last visited Dec. 10, 2008).

C. The Definition of "Identity Theft" Does Not Include the Unknowing Use of Inaccurate Credentials

As set forth above, there is a clear understanding of what behavior constitutes identity theft – the knowing impersonation of another individual. The unknowing use of inaccurate credentials does not fall within this definition. Individuals present credentials to support their claim to an attribute.[26] Credentials, such as Social Security Numbers, are often presented to support the authenticity of an attribute, such as citizenship or taxpayer status.[27]

Unknowing use of another's credentials does not meet the identity theft definition's knowledge requirement. A person who uses a credential that they believe to be fictitious – for example, an ID number created out of whole cloth, which the person believes to be unassigned to anyone – does not knowingly pose as another individual, because they do not know to whom (if anyone) the credential belongs. Furthermore, use of a single inaccurate credential does not typically qualify as "impersonation" – a term that embodies the requirement that identity thieves steal a "set of information about an individual" and misappropriate the victim's "very identity." Use of a single inaccurate credential rarely equates with stealing another person's "very identity." Identity theft only occurs if

---

[26] *Who Goes There?*, note 9 *supra* at 20 (referring to credentials as "authenticators").

[27] *Id.*

the imposter knows that she is impersonating a particular individual, and most often includes the use of multiple, consistent credentials. For example, it is possible to create a Social Security Number that is not one's own, but that also provably does not belong to someone else, *e.g.* 487-00-4218, 666-38-4719, and 987-65-4329.[28] Such use of SSNs may, in certain circumstances, be improper, but it does not involve "identity theft."

In the case now before this Court, Ignacio Flores-Figueroa presented two inaccurate credentials to his employer.[29] The credentials, a Social Security card and Permanent Resident card, bore Mr. Flores-Figueroa's real name, but numbers assigned to others.[30] The Social Security card included a number assigned to a minor, while the Permanent Resident card featured a number assigned to an adult.[31]

---

[28] Social Security Administration, "Which Social Security numbers are invalid (impossible)?" (Answer ID 425) http://ssa-custhelp.ssa.gov/cgi-bin/ssa.cfg/php/enduser/std_adp.php?p_faqid=425&p_created=972930021&p_sid=V8vXQkOi&p_accessibility=0&p_redirect=&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Jvd19jbnQ9OSw5JnBfcHJvZHM9JnBfY2F0cz0xNiZwX3B2PSZwX2N2PTEuMTYmcF9wYWdlPTEmcF9zZWFyY2hfdGV4dD12YWxpZA**&p_li=&p_topview=1; *See* LUNA, HOW TO BE INVISIBLE (2004).

[29] *Petition for a Writ of Certiorari* at 4, *Flores-Figueroa v. United States*, No. 08-108 (U.S. July 22, 2008); *Brief for the United States* at 2-3, *Flores-Figueroa v. United States*, No. 08-108 (U.S. Sept. 19, 2008).

[30] *Petition for a Writ of Certiorari*, *supra* note 29 at 4; *Brief for the United States*, *supra* note 29 at 3.

[31] *Id.*

Neither person shared Mr. Flores-Figueroa's name.[32] In addition to his proper name, Mr. Flores-Figueroa presumably shared other accurate attributes with his employer – home address, telephone number, age, and work history data. At trial, the government presented no evidence that Mr. Flores-Figueroa knew that the numbers on his inaccurate credentials were assigned to others. Petitioner's use of a single credential linked to each alleged identity theft victim strongly suggests that he did not steal a "set of information about an individual" and misappropriate the victim's "very identity." Most dramatically, Mr. Flores-Figueroa's use of his own name on the inaccurate credentials indicates a complete absence of intent to impersonate another.

II. The Identity Theft Penalty Enhancement Act's Knowledge Requirement Appropriately Reflects the Distinction Between "Identity Theft" and Presentation of Inaccurate Credentials

As discussed above, "identity theft" is defined as the knowing impersonation of another individual. The Identity Theft Penalty Enhancement Act, 18 U.S.C. § 1028A(a)(1) (2008) ("Section 1028A"), contains a knowledge requirement, which appropriately reflects the distinction between identity theft and the presentation of inaccurate credentials.

---

[32] *Id.*

A. The Application of Section 1028A's Knowledge Requirement to All the Section's Terms is Consistent with the Technical Definition of "Identity Theft"

Petitioner has asked the Court to apply Section 1028A's knowledge requirement to all the section's terms, including the statutory phrase "means of identification of another person."[33] Such an application would permit conviction of a defendant for "aggravated identity theft" only when the accused "transfers, possesses, or uses … a means of identification of another person" and the defendant knew that the "means of identification" – the credential – belonged to another person. This interpretation is consistent with the widely accepted technical definition of identity theft, which also contains a knowledge requirement, and defines an "identity thief" as one who misappropriates a set of information – usually numerous attributes – about a particular individual, thus robbing the individual of her very identity.

---

[33] *Petition for a Writ of Certiorari*, *supra* note 29 at 21.

B. Failure to Apply Section 1028A's Knowledge Requirement to All the Section's Terms is Inconsistent with the Technical Definition of "Identity Theft"

The Respondent has argued that the Court should not apply Section 1028A's knowledge requirement to the statutory phrase "means of identification of another person."[34] Respondent's interpretation would permit aggravated identity theft convictions in circumstances involving individuals who present inaccurate credentials, but do not know that the credentials belong to another person. This could include situations in which individuals use fictitious ID numbers, names, or other attributes in order to obtain work, protect their privacy, or engage in lawful but unpopular speech. Such an interpretation is squarely at odds with the technical definition of "identity theft" described above. The Court should interpret Section 1028A to ensure consistency with the plain meaning of "identity theft." This is particularly important given Congress' intent to narrowly target the Identity Theft Penalty Enhancement Act at the crime of identity theft, and not other frauds, no matter how closely related.[35]

---

[34] *Brief for the United States*, *supra* note 29 at 4.

[35] H.R. Rep. No. 108-528 at 3 (2004) (stating that Section 1028A's aggravated identity theft penalties were enacted to "provide[] enhanced penalties for persons who steal identities to commit … serious crimes.").

III. The 8th Circuit Interpretation Threatens to Impose Enhanced Identity Theft Penalties on Individuals Who are Not Identity Thieves – Individuals Who Present Inaccurate Credentials In an Effort to Protect Their Privacy Through Pseudonymous or Anonymous Activities

In *Flores-Figueroa v. United States* and *United States v. Mendoza-Gonzalez*, the 8th Circuit interpreted Section 1028A to permit conviction of a defendant for "aggravated identity theft" when the accused "transfers, possesses, or uses … a means of identification of another person" even if the defendant did not know that the "means of identification" – the credential – belonged to another person ("the 8th Circuit interpretation").[36] By failing to apply Section 1028A's knowledge requirement to the phrase "means of identification of another person," the 8th Circuit interpretation of Section 1028A imposes a two-year sentence enhancement for "aggravated identity theft" on individuals who are not identity thieves.[37] Because Petitioner truthfully identified himself while proffering an inaccurate credential, the 8th Circuit's characterization of Petitioner as an "identity thief" is contrary to the definition of "identity theft" widely accepted by identity management and security experts and implicit in the statutory provision. Beyond the

---

[36] *Flores-Figueroa v. United States*, 274 Fed. Appx. 501, (8th Cir. 2008), *cert. granted*, 2008 U.S. LEXIS 7827 (U.S. October 20, 2008) (No. 08-108); *United States v. Mendoza-Gonzalez*, 520 F.3d 912 (8th Cir. 2008).

[37] 18 U.S.C. § 1028A.

improper sentence enhancement in this case, the 8th Circuit's interpretation threatens to impose aggravated identity theft penalties on individuals who present inaccurate credentials in an effort to protect their privacy through pseudonymous or anonymous activities.

Individuals engage in pseudonymous or anonymous activities for a variety of reasons. For some, it is a matter of life or death.[38] Others have less grisly reasons for using pseudonyms. Higher education administrators regularly use constructed identity attributes for student records and

---

[38] *See, e.g.,* Letter from EPIC, Privacy International, and Human Rights Watch to Secretary Robert M. Gates, U.S. Department of Defense (July 27, 2007) *available at* http://www.epic.org/privacy/biometrics/epic_iraq_dtbs.pdf (describing how Iraqi citizens change their names or carry fake IDs to avoid being murdered by rival sects, and observing "numerous reports indicate that Iraqis regularly risk death if they are proven to be of a different sect than gunmen at a checkpoint."); *Dozens killed in Baghdad attacks*, BBC, July 9, 2006, *available at* http://news.bbc.co.uk/1/hi/world/middle_east/5162510.stm (describing a July 2006 militia attack involving the establishment of a fake Shiite-run checkpoint near Baghdad, which resulted in the deaths of 50 Sunnis after their identification documents were examined); *At Checkpoints in Baghdad, Disguise Is a Lifesaving Ritual*, Wash. Post, Sept. 29, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092801996_pf.html (quoting Gianni Magazzeni, head of the U.N. human rights office for Iraq, "People are basically killed or taken away simply because of their name, their identity or specific affiliations.").

admissions applications for a variety of reasons, including the varied credentials of international students pursuing a global education.[39] Litigants proceed under pseudonyms to protect their privacy.[40] Others pursue lawsuits under pseudonyms that both protect their identities and serve as extensions of their advocacy.[41] Mary Ann Evans published under the pseudonym "George Eliot" in an effort "to ensure her works were taken seriously in an era when female authors were usually associated with romantic novels."[42] Many of America's founders published anonymously or pseudonymously.[43]

---

[39] Office of the Inspector General, U.S. Social Security Administration, *Review of Universities' Issuance of Temporary Social Security Numbers to Foreign Students* (April 2004) (analyzing "numerous instances in which universities issued temporary … 'dummy' or 'pseudo'" social security numbers, including circumstances in which "the Florida Bureau of State Payrolls assigned a range of temporary 9-digit identification numbers (800-series) to 11 State universities and referred to them as temporary SSNs.").

[40] *See, e.g., Roe v. Wade*, 410 U.S. 113 (1973).

[41] *See, e.g., Guy Montag Doe v. San Francisco Housing Authority*, No. 08-03112 (N.D. Cal. filed June 27, 2008) (Plaintiff challenges the Constitutionality of San Francisco gun control ordinance under pseudonym referencing Guy Montag, a literary protagonist who rebels against authoritarian regulations); *see also* RAY BRADBURY, FAHRENHEIT 451 (1953).

[42] BBC History – George Eliot (1819-1880), http://www.bbc.co.uk/history/historic_figures/eliot_george.shtml (last visited Dec. 12, 2008).

[43] *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO

Famous individuals have elected to receive medical care under pseudonyms.[44] The U.S. government is likely the largest single user of pseudonymous credentials in the country, providing them to enrollees in the Department of Justice's Witness Protection Program.[45]

Other, less famous individuals simply wish to protect their privacy. Anonymity – the ability to conceal one's identity while communicating – and pseudonymity – the use of a multiple identities – help to decrease the likelihood that a person's privacy will be violated, and their personal information exposed.[46] This is particularly important because technological

---

THE INTERNET 41-43 (2000) (citing well known pseudonymous authors including Benjamin Franklin, Alexander Hamilton, and Samuel Adams, and further estimating that "six Presidents, 15 Cabinet members, 20 Senators, and 34 Congressmen published unsigned political writings or writings under pen names" in the first two decades following Constitutional ratification).

[44] BARRON H. LERNER, WHEN ILLNESS GOES PUBLIC 144 (2006) (detailing Steve McQueen's use of a pseudonym while receiving mesothelioma treatment at Cedars-Sinai Medical Center in 1980).

[45] *See U.S. Marshals Service Talks WitSec to the World*, America's Star:FYI, Aug. 2006 *available at* http://www.usmarshals.gov/witsec/americas_star.pdf (stating that the federal government has given "more than 18,000 witnesses and their families … new names, new identities, assistance with employment, and vocational training" through the Witness Protect Program, also called the "Witness Security Program.").

[46] David Chaum *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, Communications of the ACM, at 1030-1044 (Oct. 1985).

developments have increased privacy risks by enhancing surveillance and data retention capabilities. Generally speaking, public and private entities are collecting more personal data, and retaining more information for longer periods.

"It is becoming increasingly easy and common for organizations to routinely exchange data on individuals"[47] and "[i]ndividuals have no way of knowing if this information is inaccurate, outdated, or otherwise inappropriate, and may only find out when they are accused falsely or denied access to services."[48] However, individuals who wish to protect their privacy can limit distribution of their personal information by taking steps to safeguard it. One way to protect personal information is to use inaccurate credentials, thus preserving pseudonymity or anonymity.[49] Privacy experts advocate that individuals act anonymously or pseudonymously in some circumstances, and build such transactions into digital security and identity systems.[50]

---

[47] David Chaum, *Signatures Transferred Between Unconditionally Unlinkable Pseudonyms* (1986).

[48] *Security Without Identification*, note 44 *supra*.

[49] *Who Goes There?*, note 9 *supra,* at 178 (observing that "preserving the ability of citizens to interact anonymously with other citizens, with business, and with the government is important because it avoids unnecessary accumulation of identification data that could deter free speech and inhibit legitimate access to public records.").

[50] *See, e.g.,* David Chaum, *Achieving Electronic Privacy*, Scientific American, p. 96-101 (Aug. 1992) (describing a digital authentication system in which users "establish relationships with different organizations under

The 8th Circuit interpretation threatens to improperly brand as identity thieves individuals who seek to protect their privacy through the use of inaccurate credentials. This would be a wholly unintended and undesirable result of the Congress' enactment of the Identity Theft Penalty Enhancement Act. It could also chill the use of privacy-protecting pseudonyms. Individuals could be deprived of a simple and effective tool in the battle for greater privacy – pseudonymous and anonymous transactions.

---

different digital pseudonyms," and lauding the privacy benefits that accrue because "Each [organization] can recognize [the user] unambiguously, but none of their records can be linked."); Harris County Public Library – About – Internet Safety, http://www.hcpl.net/about/internetsafety.htm (last visited Dec. 16, 2008) (advising library users to reduce the risks of online data collection by "using a pseudonym and think carefully before revealing any personal information such as age, financial information, or marital status.").

CONCLUSION

Amici respectfully request this Court to grant Petitioner's motion to reverse the decision of the lower court.

Respectfully submitted,

MARC ROTENBERG
JOHN A. VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

December 22, 2008