COMMENT

Data Privacy: The Use of Prisoners for Processing Personal Information

TABLE OF CONTENTS

> Your life is for sale for twenty-five cents. No matter if it's in Texas or California or Florida or West Virginia — anywhere.[1]
>
> – Hal Parfait, convicted rapist and burglar who served time in Huntsville, Texas state prison

INTRODUCTION

When Beverly Dennis completed a home-products survey for Metromail Corporation ("Metromail"), a leading direct marketer, she only expected to receive coupons and free samples.[2] Instead, the Ohio grandmother received a twelve-page handwritten letter from Hal Parfait, a convicted rapist and burglar, recently released from a Texas state prison after completing a seven and one half year term.[3] Parfait bought Dennis's personal information[4] for twenty-five cents from a fellow prisoner while they were processing Metromail's consumer surveys under a Texas prison work program.[5] The letter contained explicit and offensive material, including sexual fantasies and threats to rape Dennis in her own shower upon his release from prison.[6]

Other prisoners, including murderers, rapists, and burglars, routinely process data for public and private industries.[7] Federal prisoners work for several public agencies, including the Internal Revenue Service.[8] State prisoners in at least twenty-seven states

---

[1] *Prime Time Live: Inmates Inc.* (ABC television broadcast, Oct. 22, 1997) [hereinafter *Prime Time Live*].

[2] *See* Plaintiff's Fifth Amended Class Action Petition at 2-7, 10-19, 23, 29-36, 45, Dennis v. Metromail (Tex. Dist. Ct., Jan. 9, 1998) (No. 9604451) (on file with author) (discussing deception of consumer circulars for coupons and product discounts).

[3] *See id.* at 23; *Prime Time Live, supra* note 1 (stating prison term for Parfait's burglary and rape charges).

[4] *See* Plaintiff's Fifth Amended Class Action Petition at 23, *Dennis* (No. 9604451) (referring to personal information such as Dennis's income level, birthday, magazine selections, and personal care product preferences).

[5] *See id.* at 4 (noting that prisoners receive access to personal information through data entry work).

[6] *See id.* at 23 (quoting Parfait's letter as stating "I'd do whatever I could for you to make your life and sexual desires and fantasies become a fulfilled reality").

[7] *See Prime Time Live, supra* note 1 (explaining that convicted felons have access to private information in prison as part of their job).

[8] *See* Nina Bernstein, *Lives on File: The Erosion of Privacy — A Special Report; Personal Files Via Computer Offer Money and Pose Threat*, N.Y. TIMES, June 12, 1997, at A1 (indicating number of states that use prison labor to process information for government in discussing Dennis's lawsuit); *cf.* Larry MacIntyre, *Prisoners Get a Crack at Private Records; State Cancels Project that Gave Inmates Access to Personal Data from Child Support Cases*, INDIANAPOLIS STAR, Sept. 30, 1994, at A01 (stating that Indiana halted project to log thousands of child support case records into computer network after county clerks discovered that prisoners would perform job).

handle public records such as motor vehicle registrations.[9] In at least thirty-one states, prisoners take motel reservations for private businesses.[10] In more than twelve states, they answer 800-number calls[11] and work as telemarketers.[12] As a result, these prisoners have access to some of our most private and confidential information, including tax records, court rulings, medical files, phone numbers, addresses, social security numbers, credit card numbers, divorce decrees, and income levels.[13]

An analysis of case law and statutory law at both the federal and state levels reveals that legal protections designed to keep personal information private in the United States are woefully inadequate.[14] Beverly Dennis is one of several citizens who completed Metromail's consumer survey. None consented to give prisoners access to their personal information.[15] Dennis filed a class action lawsuit against Metromail, its parent corporation R.R. Donnelly & Sons,

---

[9] *See* Bernstein, *supra* note 8, at A1; *cf.* Rich Hein, *State Uses Inmates to Process Vehicle Records; Critics Decry Risk to Privacy*, CHICAGO SUN-TIMES, June 9, 1998, at 1 (debating merits of using Illinois prisoners to handle vehicle registration information in light of cost savings to taxpayers, lack of complaints, and privacy concerns); Jason Piscia, *Legislator Calls for Ban on Prisoner Access to Vehicle Data*, COPLEY NEWS SERV., June 9, 1998 (reporting that Chicago legislator will introduce legislation to ban 13 year practice of allowing prisoners to process vehicle registrations despite $374,000 savings to state). Two years ago, Illinois's Secretary of State Office ended its $600,000 per year business of selling personal information about driver's license applicants to direct markets out of privacy concerns. *See* Michelle Stevens, *Question of Privacy*, CHICAGO SUN-TIMES, Apr. 8, 1996, at 27.

[10] *See* Stephanie Saul, *Inmate's Abuse of Job Sullies Program*, NEWSDAY, Nov. 8, 1994, at A35 (discussing increasing number of prison work programs in partnerships with private companies).

[11] *See* CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, FREE VENTURE PROGRAM BROCHURE (1997) (discussing California juvenile prisoners who answer toll-free calls for Department of Consumer Affairs and take flight reservations for private airline company); *Prime Time Live*, *supra* note 1 (stating that tourists making vacation plans who dial toll-free number tell maximum security Iowa prisoners where they live and when they plan to travel).

[12] *See Prime Time Live*, *supra* note 1 (showing prisoners in Utah working as telemarketers and prisoners in Washington making fundraising calls for Red Cross); *see also* James P. Miller, *Donnelley Unit Sued After Inmate Allegedly Misuses Marketing Data*, WALL ST. J., May 6, 1996, at B5 (reporting on Dennis's lawsuit and privacy issues in light of routine use of prison labor to process data).

[13] *See* Plaintiff's Fifth Amended Class Action Petition at 13, Dennis v. Metromail (Tex. Dist. Ct., Jan. 9, 1998) (No. 9604451) (on file with author) (listing detailed sensitive personal information solicited by Metromail's questionnaires such as credit cards used, dietary, personal and smoking habits, investments, medication, and shopping habits); *Prime Time Live*, *supra* note 1 (setting forth examples of sensitive personal information available to prisoners).

[14] *See generally* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995) (arguing that regulation of personal information is ad hoc and minimal in United States).

[15] *See* Plaintiff's Fifth Amended Class Action Petition, *Dennis* (No. 9604451) (outlining class action allegations and injuries).

Inc. ("R.R. Donnelly"), subcontractor Computerized Image & Data Systems, Inc., and the Texas Department of Criminal Justice in *Dennis v. Metromail*, currently pending in Texas state court.[16]

Dennis's class action lawsuit challenging prisoner access to consumer surveys containing personal information brings the issue of data privacy to the forefront of political debate.[17] This Comment argues that both government and private businesses should discontinue, or at least substantially curtail, the use of prisoners for processing sensitive personal information in order to protect the right to privacy. Part I of this Comment discusses the legal background of privacy, including traditional and modern definitions. Part I further explains the prison industry's and privacy advocates' arguments supporting and opposing the use of prisoners to process personal information and then analyzes the current state of privacy law. Part II compares and contrasts federal and state privacy laws and analyzes the weaknesses in the current privacy approaches of the United States, Texas, and California. Finally, Part III introduces the principles of the European Directive on data protection as a source for a proposed federal data privacy statute.

I. THE LEGAL BACKGROUND OF PRIVACY

As Americans, privacy is one of our most valued and cherished rights.[18] The term "privacy" encompasses a variety of personal rights, including keeping government out of the bedroom[19] and protecting a woman's right to choose.[20] While the right to privacy is a broad concept that involves the protection of the person and his home, data privacy is a narrower concept that involves the per-

---

[16] *See* Docket, Dennis v. Metromail (Tex. Dist. Ct., Apr. 18, 1996) (No. 9604451) (listing chronology of events); Telephone Interview with Robert M. Long, Dennis's local counsel in Texas, (Sept. 28, 1998) (on file with author) (discussing status of case).

[17] *See* Kathryn Ericson, *Suit over Prisoner Access to Marketing Survey May Open Privacy Discussion*, WEST'S LEGAL NEWS, July 1, 1996, *available in* 1996 WL 359993 (explaining groundbreaking significance of Dennis's case in light of data privacy and technology).

[18] *See* LOUIS HARRIS & ASSOCS. & ALAN F. WESTIN, EQUIFAX, INC., THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE 7, 11 (1990) (finding that 79% of Americans believe that privacy is fundamental right and 71% believe they have no control over use and dissemination of personal information).

[19] *See* Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (striking down state statute forbidding married persons from using contraceptives and creating zone of privacy as penumbra in Bill of Rights).

[20] *See* Roe v. Wade, 410 U.S. 113, 152-53 (1973) (holding that right to privacy is fundamental right in abortion case).

sonal information of individuals.[21] Personal information consists of facts, communications, or opinions that an individual would reasonably regard as private, confidential, or sensitive and, therefore, would want to prohibit or restrict from use or dissemination.[22] Established minimum standards aimed at protecting the personal information of individuals are known as fair information practices.[23]

A. The General Right to Privacy

The modern definition of privacy stems from the right "to be let alone."[24] In 1888, Judge Thomas Cooley recognized the right of personal immunity as the right "to be let alone."[25] Judge Cooley cited the right of an individual to protect his person to justify why the law should confer the right to privacy upon that individual.[26]

In an 1890 law review article, Samuel Warren and Louis Brandeis offered one of the most influential discussions on the right to privacy.[27] Noting first that the law prohibits the unauthorized public dissemination of the content of an individual's private writings, Warren and Brandeis argued that the acts and relations of an individual in a social or personal context deserve equal protection. They believed that an individual had a right to be free from the unauthorized publishing of all private matters, not just private writings.[28] They argued that the increasing abuses of journalists demanded a remedy for individuals who suffered pain and mental distress from the public revelation of private information.[29]

---

[21] *See* Reidenberg, *supra* note 14, at 498. Reidenberg associates the treatment of personal information with an individual's personality and human dignity because the ability to control such information is critical to a citizen's participation in society. *See id.*

[22] *See generally* RESTATEMENT (SECOND) OF TORTS § 652(A)-(E) (1977) (listing acts that result in violations of right to privacy).

[23] *See* Reidenberg, *supra* note 14, at 498 (referring to fair practices as treating collection, storage, use, and disclosure of personal information with integrity).

[24] THOMAS COOLEY, THE LAW OF TORTS 29 (2d ed., Chicago, Callaghan & Co., 1888).

[25] *See id.* (recognizing right to be free from physical or bodily injury with corresponding duty not to inflict or attempt to inflict injury).

[26] *See id.*

[27] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890) (recognizing right to privacy as separate principle that had immediate effect upon law).

[28] *See id.* at 213 (recognizing that abuses of press required new cause of action separate from existing causes of action such as defamation, invasion of property right, or breach of confidence or implied contract).

[29] *See id.*

Warren and Brandeis reexamined old cases in which courts granted individuals the right to determine when and to what extent their thoughts and actions are revealed to others.[30] They concluded that English and American courts had already implicitly recognized the right to privacy. Not realizing they were doing so, courts granted relief on alternative grounds, such as the right of property,[31] breach of confidence,[32] and breach of implied contract.[33] Warren and Brandeis, thus, advocated the recognition of a new legal principle that courts could invoke to protect personal privacy.[34]

---

[30] *See, e.g.*, De May v. Roberts, 9 N.W. 146, 149 (Mich. 1881) (holding doctor liable for allowing stranger to watch woman giving birth on trespass or battery theories); Hardin v. Harshfield, 12 S.W. 779, 790 (Ky. 1890) (classifying loss of marriage engagement caused by defendant's disclosure of plaintiff's embarrassing flatus in public as slander); *see also* PROSSER, WADE, AND SCHWARTZ, CASES AND MATERIALS ON TORTS 947 (9th ed. 1994) (tracing evolution of right to privacy).

[31] *See, e.g.*, Gee v. Pritchard, 2 Swanst. 402, 413 (1818) (discussing whether to grant injunction prohibiting publication of private letters pursuant to property law).

[32] *See, e.g.*, Abernethy v. Hutchinson, 3 L.J. Ch. 209 (1825) (granting injunction against magazine's publication of surgeon's oral lectures to hospital on basis of breach of confidence).

[33] *See, e.g.*, Pollard v. Photographic Co., 40 Ch. D. 345 (1888) (granting relief to woman who sought to enjoin photographer from displaying or selling her photograph on grounds of breach of implied term in contract and breach of confidence).

[34] *See* Warren & Brandeis, *supra* note 27, at 213-14. Remedies for a violation of the right to privacy could include damages and an injunction. *See id.* at 219. Warren and Brandeis also considered limitations on the right to privacy when balancing the dignity of the individual against the public welfare. *See id.* They analyzed the law of slander and libel to privacy for guidance on how to balance rights of individual and society. *See id.* They found that the right to privacy does not prohibit publication of information that is of public or general interest. *See id.* at 216-17. Similarly, if an individual consents to publication, the publisher does not violate the right to privacy. *See id.* at 216-18. Furthermore, unlike actions for libel, the truth of the matter published and the absence of malice or ill will of the publisher are not defenses to a violation of the right to privacy. *See id.* at 218. However, Warren and Brandeis concluded that protection of an individual's right to privacy would ultimately lead to the protection of society's rights and that individuals are entitled to exclusive use and protection of security of person. *See id.* at 219-20.

New York was one of the first states to consider Warren and Brandeis's newly advanced doctrine in *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442, 447-78 (N.Y. 1902). The court rejected a right to privacy argument where defendant used a picture of an attractive woman's face to advertise flour without obtaining her permission first. *See id.* Ignoring two lower courts' acceptance of the right to privacy, the New York Court of Appeals rejected its existence at common law, claiming that such right would "seriously offend the sensibilities of good people" and open the floodgates of litigation. *See id.* at 443. The unpopular *Roberson* decision caused the New York Legislature to enact a statute in 1903 prohibiting the use of a living person's name or picture for advertising or commercial purposes without prior written consent. *See* N.Y. CIV. RIGHTS LAW §§ 50-51 (McKinney 1992); *see also* PROSSER, ET AL., *supra* note 30, at 947 (stating that Virginia, Oklahoma, and Utah have adopted similar statutes).

However, the same question came before the Georgia Supreme Court three years later involving the use of plaintiff's name and picture in defendant's insurance advertising in *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 78 (Ga. 1905). Unlike the *Roberson* court, the

While Warren and Brandeis's discussion on privacy lead courts to formally recognize the right to privacy as an independent cause of action, Dean Prosser's description of the common law privacy torts is similarly important. Prosser focused specifically on the restricted ability of an individual to seek redress for a violation of the right to privacy by private actors.[35] Instead of a unitary privacy tort, Prosser believed that the tort had evolved into four distinct causes of action. Except for the fact that each represents an invasion of Judge Cooley's right to be let alone, they bear little resemblance to each other.[36] First, Prosser defined the "intrusion upon seclusion" tort as an unreasonable encroachment into an area where an individual has a reasonable expectation of being undisturbed.[37] While the intrusion tort involves offensive methods of gathering information, the "public disclosure of private facts" tort focuses on the circulation of such information. This tort consists of unreasonably publishing private information in which the public has no legitimate interest.[38] The "false light" tort consists of the public misrepresentation of a private matter regarding another person.[39] Potential liability exists for the wide dissemination of erroneous or misleading information. Finally, the "misappropriation" tort involves the use of an individual's name or likeness for commercial profit.[40]

Georgia court unanimously recognized the existence of the right to privacy, noting its foundation in natural law. *See id.* *Pavesich* became a leading case in this area. *See id.; see also* W. PAGE KEETON, PROSSER & KEETON ON TORTS 851 (5th ed. 1984) (noting that judicial tide began recognizing privacy rights even though authority was divided).

[35] *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389-407 (1960) (defining and discussing four privacy torts in detail).

[36] *See id.* at 389 (noting that right to be let alone ties four torts together).

[37] *See id.* at 389-92 (discussing cases that have recognized "intrusion upon seclusion" tort); *see, e.g.*, Byfield v. Candler, 125 S.E. 905, 906 (Ga. Ct. App. 1924) (holding defendant liable for intruding into woman's stateroom on steamboat).

[38] *See* Prosser, *supra* note 35, at 392-98 (discussing cases that have recognized "public disclosure of private facts" tort); *see, e.g.*, Briscoe v. Reader's Digest Ass'n, Inc., 4 Cal. 3d 529, 541-42, 483 P.2d 34, 43-44 (1971) (holding that true story about rehabilitated truck hijacker was actionable as invasion of privacy under public disclosure of private facts tort); Melvin v. Reid, 112 Cal. App. 285, 290-93, 297 P. 91, 93-94 (Ct. App. 1931) (finding plaintiff, who alleged invasion of privacy by defendant who exposed her previous prostitute career and murder acquittal in movie, had sufficient cause of action to survive defendant's demurrer).

[39] *See* Prosser, *supra* note 35, at 398-401 (discussing cases that have recognized "false light" tort); *see, e.g.*, Gill v. Curtis Publ'g Co., 38 Cal. 2d 273, 280-82, 239 P.2d 630, 635 (1952) (finding that picture of embracing couple on "wrong kind of love" portrayed plaintiff in objectionable false light in public eye); Linehan v. Linehan, 134 Cal. App. 2d 250, 254-55, 285 P.2d 326, 328-29 (Ct. App. 1955) (holding that public accusation that plaintiff was not lawful wife of defendant's ex-husband as actionable false light tort).

[40] *See* Prosser, *supra* note 35, at 401-07 (discussing cases that have recognized "misappropriation" tort); *see, e.g.*, Stryker v. Republic Pictures Corp., 108 Cal. App. 2d 191, 195-96,

Courts that recognize this tort restrict the circulation of names and images. Thus, Prosser's common law torts against the invasion of privacy guard against improper interference in the personal and confidential aspects of an individual's life.[41] A majority of states have recognized one or more of Prosser's common law torts to create an independent basis for criminal or civil liability.[42]

Many legal scholars, however, reject Prosser's four definitions of privacy. The modern literature classifies privacy into three main schools of thought: privacy as the control over personal information,[43] privacy as a function of individual decision making and self-determination in a democracy,[44] and privacy as fundamental hu-

---

238 P.2d 670, 672-73 (Ct. App. 1951) (allowing plaintiff to recover when his name, picture, or likeness has been used without his consent in motion picture); Goodyear Tire & Rubber Co. v. Vandergriff, 184 S.E. 452, 460 (Ga. Ct. App. 1936) (holding defendant liable for impersonation to obtain secret information).

[41] *See* Hill v. NCAA, 7 Cal. 4th 1, 24, 865 P.2d 633, 647 (1994) (discussing applicability of Prosser's common law torts to California).

[42] *See, e.g.*, CAL. CIV. CODE § 3344 (West Supp. 1991); FLA. STAT. ANN. § 540.08 (West 1988); IND. CODE §§ 4-1-6-1 to -9 (1981); KY. REV. STAT. ANN. § 391.170 (Michie 1984); MASS. ANN. LAWS ch. 214, § 3A (Law Co-op. 1986); NEB. REV. STAT. §§ 20-201 to -211 (1987); N.Y. CIV. RIGHTS LAW §§ 50-52 (Consol. 1986); R.I. GEN. LAWS §§ 9-1-28 to -28.1 (1985); TENN. CODE ANN. §§ 47-25-1103, 47-25-1105 (1988 & Supp. 1990); UTAH CODE ANN. § 45-3-3 (1988); VA. CODE ANN. §§ 2.1-277 to -386 (Michie 1976); WIS. STAT. ANN. § 895.50(2) (West 1983); Kelly v. Franco, 391 N.E.2d 54, 57-58 (Ill. Ct. App. 1979) (holding that Illinois protects only against misappropriation of individual's name or likeness for commercial gain); Stutner v. Dispatch Printing Co., 442 N.E.2d 129, 134 (Ohio Ct. App. 1982) (deciding that Ohio does not recognize false light privacy tort); Gautier v. Pro-Football, Inc., 107 N.E.2d 485, 487-88 (N.Y. 1952) (holding that New York only recognizes misappropriation privacy tort); Kalin v. People Acting Through Community Effort, 408 A.2d 608, 609 (R.I. 1979) (holding that Rhode Island protects limited common law privacy rights); *see also* RESTATEMENT (SECOND) OF TORTS § 652A app. reporter's note (1989 & Supp. 1990) (listing states that have adopted tort for invasion of privacy in one form or another); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 221 n.150 (1992) (listing states that have adopted privacy statutes).

[43] *See Practices of Direct Marketing & Credit Industries & Electronic Privacy Issues: Hearings Before the Joint Task Force on Personal Information & Privacy*, 75th Legis., 1997-1998 Reg. Sess. (Cal. 1997) [hereinafter *Hearings*] (on file with author) (statement of Beth Givens, Chair of Privacy Rights Clearinghouse) (defining privacy as "the ability to control information about you"); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining privacy as individual's complete control over how personal information is communicated to others); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 36 (1967) (defining privacy as control over one's personal affairs).

[44] *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968) (noting that privacy is critical to define ourselves in human relationships); Reidenberg, *supra* note 14, at 498 (maintaining that treatment of personal information gives respect to individual's personality and defines social relationships); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 557 (1995) (shifting away from seclusive notions of right to be let alone in favor of privacy as participatory model because of increasing computer age).

man dignity.[45] Some critics argue that Prosser's common law privacy torts no longer adequately protect individual privacy given the tremendous improvement in the ability of computers to efficiently collect, store, and disseminate massive amounts of personal information.[46]

While many definitions of privacy have emerged from the original common law concept, they still center around the right to be let alone, a right that should severely restrict the use of prison labor to process personal information.[47] Addressing this right to data privacy, however, is not simple. The data privacy debate involves several factors, including the rights of individuals to maintain confidentiality and restrict access to their personal information, the right of government to employ prisoners, and the rights of private industry to process and sell personal information.[48]

B. The Data Privacy Debate on the Use of Prison Labor

Governments and private industry alike have long used prison labor in a number of different business activities.[49] Prison industry

---

[45] *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 974 (1964) (maintaining that invasion of privacy is assault on human personality); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 451 (1980) (noting that privacy promotes individual liberty, autonomy, and personal enrichment).

[46] *See* Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1413 (1987) (arguing that common law privacy torts fail to protect informational privacy in light of encroachments of Information Age).

[47] *See* George B. Trubow, *The Development and Status of 'Information Privacy' Law and Policy in the United States*, *in* INVITED PAPERS ON PRIVACY: LAW, ETHICS, AND TECHNOLOGY 1 (presenting discussion on informational privacy at National Symposium on Personal Privacy and Information Technology, Oct. 4-7, 1981). Trubow has noted the components of data privacy as (1) the kind of personal information collected, (2) the circumstances where a third party can see the personal information, and (3) how the personal information is protected. *See id.*

[48] *See* Reidenberg, *supra* note 14, at 236-43 (framing debate for workable balance between privacy concerns and commercial activities).

[49] *See, e.g.*, Sam Martino, *Using Inmates to Staff Phones Rekindles Debate*, MILWAUKEE J. SENTINEL, Apr. 12, 1998, at 5 (reporting that for several years Wisconsin has used prisoners to take pledges for Leukemia Society, answer state lottery calls, record orders for private companies, and perform data entry for private and public organizations); *see also* David Armstrong, *Registry Ends Prisoner Plan*, BOSTON GLOBE, Feb. 24, 1994, at 34 (reporting that Registrar of Motor Vehicles decided not to employ prisoners to answer phones and process documents, but reserved right to do so in future); David Armstrong, *Registry Head Still Weighs Inmate Work*, BOSTON GLOBE, Dec. 16, 1993, at 47 (noting that head of department considered use of prisoners to process documents with social security numbers and other personal information as partial solution to backlog and personnel problems); *Across the USA: News from Every State*, USA TODAY, Nov. 2, 1993, at 7A (noting that Massachusetts state employees union attacked plan to have prisoners answer telephones for Registry of Motor Vehicles as dangerous).

experts argue that prison work programs benefit both prisoners and the community. First, they argue that these programs prepare prisoners for work, rehabilitate them, and make them productive members of society.[50] Second, such programs keep prisoners busy and provide an incentive to behave.[51] They give prisoners the opportunity to earn money,[52] which they use to pay for room and board, restitution to victims, family support, and taxes.[53] In fact, the prison industry praises juvenile delinquent work programs because they reduce institutional costs and provide financial assistance to crime victims.[54]

While the majority of prisoners work for federal and state governments,[55] the prison industry also points to the enormous benefits that work programs provide private industry. Prisoners are ideal employees because they receive only minimum wage and are not entitled to medical insurance, retirement benefits, or vacation

---

[50] *See* Vince Beiser, *Look for the Prison Label: America Puts Its Inmates to Work*, THE VILLAGE VOICE, May 21, 1996, at 37 (stating that corrections officials and politicians praise prison work programs as way to teach inmates job skills, reduce idleness, and allow them to earn money).

[51] *See* Morgan O. Reynolds, *The Economics of Prison Industries: The Products of Our Prison* (Nov. 1, 1996), *in* VITAL SPEECHES OF THE DAY 58, 59 (claiming that prisoners who work behave better and that prisoners prefer to work over tedious prison life); Beiser, *supra* note 50, at 37. As a result of increases in drug arrests and mandatory sentencing laws, the prison industry work programs have boomed. *See id.* While all prison industry programs are voluntary, "tough on crime" mentality has left work programs as one of the last options for prisoners in overcrowded cells. *See id.* Approximately 20% of federal prisoners and 7% of state prisoners participate in work programs, and many have waiting lists. *See id.* Additionally, the popularity of work programs like data processing has been increasing because funding for educational, drug-treatment, and recreational programs has been drastically reduced or completely eliminated. *See id.*

[52] *See* Saul, *supra* note 10, at A35 (stating that prisoners in Texas are not paid while prisoners in other states earn minimum wage).

[53] *See* CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, *supra* note 11 (noting that although juvenile prisoners working for Trans World Airlines ("TWA") earn $5.33 per hour, Department of Youth Authority requires them to deposit money in various accounts). Juvenile prisoners deposit 20% of their net wages for room and board, place 40% of their net wages into a savings account, contribute 15% of their gross wages to restitution fund for crime victims, and keep remainder of wages. *See id.* Robert Verdeyen of the American Correctional Association claims that prisoners in these programs have returned a significant part of the $32 million they have earned over the last six to eight years to the public. *See* Saul, *supra* note 10, at A35.

[54] *See* CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, *supra* note 11 (describing tax savings as one of many program benefits to private employer); Christian Parenti, *Making Prison Pay: Business Finds the Cheapest Labor of All*, THE NATION, Jan. 29, 1996, at 11 (noting that businesses do not have to pay health insurance, vacation, or sick pay on top of wages).

[55] *See* Beiser, *supra* note 50, at 37 (noting that private businesses in only about 25 states have set up operations within prison walls while government employs majority of prisoners).

and sick leave.[56] Prisoners can neither strike nor belong to unions.[57] Further, many companies receive tax breaks for joint ventures with prison industries.[58] Another proponent acknowledged that while "information sweatshops" in Mexico or Thailand are cheaper than prisoners in the United States, businesses here have direct control over the data entry work and do not have to deal with language problems typically found in Third World countries.[59] Some companies even view the use of prison labor, especially juveniles, as community service.[60] In short, prisoners provide a stable and cheap work force to industry in the United States.[61]

However, the use of prisoners for processing personal information raises serious issues of abuse. Prison industry experts, nevertheless, contend that sufficient controls are in place to prevent prisoners from misusing personal information.[62] Prison officials implement many security measures to prevent prisoners from misusing personal information. Common safeguards include daily strip searches of prisoners and requirements that prisoners wear special clothing on the job.[63] Prisoners also face felony charges if

---

[56] *See* CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, *supra* note 11 (listing economic benefits to employer).

[57] *See* Parenti, *supra* note 54, at 11 (comparing difference in wages between juvenile prisoners, who receive minimum wage as telephone reservationists, and unionized workers, who receive as much as $18 per hour).

[58] *See id.* (noting that DPAS, private company with data processing operation in San Quentin prison, receives 10% tax credit on first $2000 of each inmate's wages).

[59] *See id.* (explaining benefits of domestic prison work force).

[60] *See* Beiser, *supra* note 50, at 37 (stating that TWA characterizes training juvenile prisoners to be ticketing agents as community involvement); Betsy Wade, *The Practical Traveler; When an Inmate Books the Ticket*, N.Y. TIMES, Nov. 9, 1997, at 4 (reporting that travel agency employs 12 female prisoners in South Carolina as reservationists, but does not give them access to personal information). The owners of the travel agency who sell tickets and services to other agencies offer a 50% reduction in reservation costs with the use of prisoners. *See id.* The owners view their project as "socially responsible" and occasionally give children free flights to visit their mothers in prison. *See id.*

[61] *See Prime Time Live*, *supra* note 1 (quoting director of telemarketing firm that set up facility in Utah state prison as stating, "We're finding that they're [prisoners] very courteous, they're hardworking. They're trying to do a good job."); Beiser, *supra* note 50, at 37 (stating that prisoners are cheaper than civilian workers and that they are enthusiastic employees who live on-site at correctional facility).

[62] *See Prime Time Live*, *supra* note 1 (quoting Metromail's characterization of *Dennis* as "unfortunate" and stating that it no longer uses prison labor).

[63] *See* John Moritz, *Prison Inquiry into Privacy of Data Sought by Senator*, FORT WORTH-STAR TELEGRAM, Oct. 24, 1997, at 2 (listing security measures to prevent prisoners' potential abuse of personal information). Larry Fitzgerald, a spokesman for the Texas prison, said, "If we have to strip search them seven times a day we do." *Prime Time Live*, *supra* note 1. Fitzgerald also believes that personal information is safer in prisons. He quipped, "In the free world, what guarantee do you have . . . [that your social security number or credit card

they remove documents from the work place.[64] Finally, taxpayers receive a substantial saving — more than three million dollars in 1997 — when prisoners process information for government agencies.[65] Thus, prison industry advocates conclude that the benefits of such work programs outweigh the risks associated with prisoner processing of personal information.

However, prisoners have misused consumer information in the past and, thus, prisoner access to such information has become a growing concern.[66] Privacy rights advocates argue that consumers have a right to know who has access to their personal information and for what purpose it is used.[67] Americans increasingly express concern about the use of their personal information. For example, a large American credit bureau conducted polls in 1994 and 1995 which revealed that four out of five Americans are concerned about threats to their personal privacy.[68] Ninety percent of Americans surveyed thought that excessive and unnecessary collection of personal information was a problem.[69]

Despite this widespread concern, privacy advocates do not have lofty goals. They seek only to prohibit the use of prisoners to process personal information; they do not want to completely eliminate data entry work or other prison work programs.[70] The use of prison labor for data entry of personal information raises obvious safety and publicity concerns.[71] Privacy rights advocates contend

---

won't] be misused?. . . I think our records are better." *Id.*

[64] *See Prime Time Live*, *supra* note 1 (discussing prisoners' disincentive to steal or tamper with documents).

[65] *See* Moritz, *supra* note 63, at 2 (noting that Texas prisoners who process information saved state taxpayers $3.2 million last year in $2.1 million record conversions contract with Texas Department of Public Safety); *A Prison in a Growth Industry, Inmates Process Data*, N.Y. TIMES, July 12, 1997, at A1 (noting that prison supervisor in Ferguson, Texas believes government will not sacrifice money for privacy).

[66] *See Hearings*, *supra* note 43 (testimony of Beth Givens, Chair of Privacy Rights Clearinghouse) (advocating on behalf of consumers).

[67] *See generally* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996) (discussing public's right to have control over their personal information by studying data privacy law in United States in public and private sectors as compared to law in European Union); Bernstein, *supra* note 8, at A1 (noting disgust of consumers who learn of prisoner access to personal information).

[68] *See* LOUIS HARRIS & ASSOCS., EQUIFAX REPORT ON CONSUMER PRIVACY 15 (1995); LOUIS HARRIS & ASSOCS., EQUIFAX REPORT ON CONSUMER PRIVACY 8 (1994).

[69] *See* LOUIS HARRIS & ASSOCS. & WESTIN, *supra* note 18, at 16 (1990).

[70] *See* Ericson, *supra* note 17 (commenting that use of prison labor to perform data entry work is "egregious").

[71] *See* Beiser, *supra* note 50, at 37 (discussing reluctance of businesses to set up operation inside prison walls).

that no controls can ever be sufficient to prevent prisoner abuse of personal information.[72] Even if prisoners work at minimum wage, or for free, they conclude that cost savings should not come at the expense of public safety.[73]

Privacy advocates also argue that the balance between cost savings from these prison work programs and the risk to public safety is tenuous. They claim that the need for additional security measures and the risk of privacy violations by prison labor negate any cost savings to taxpayers and businesses.[74] Prisoners often require extra training on the job. Moreover, they necessarily require greater supervision and safeguards, further draining taxpayers' funds.[75] The possibility of riots and lockdowns that are commonplace in prisons could also offset any cost savings from such work programs.[76] Thus, as a matter of public policy, privacy rights advocates contend that prisoners should have no part in the processing of personal information.

The economic benefits to government and private businesses, the rehabilitation of prisoners, and the risk to public safety raise important questions about the use of prisoners to process personal information. Various federal and state laws have attempted to address data privacy concerns, resulting in a patchwork of legislation designed to govern the processing of personal information.

II. THE STATE OF THE LAW

Federal and state privacy laws in the United States are ad hoc, unsystematic, and narrowly tailored to specific industries.[77] Similarly, federal and state data privacy protections are derived from a diverse combination of legal rules, industry norms, and business

---

[72] *See Prime Time Live*, *supra* note 1 (interviewing Florence Shapiro, Texas State Senator, who opposes prisoner access to personal information); Bernstein, *supra* note 8, at A1 (describing consumer outrage at prisoner access to personal information).

[73] *See Prisoner Data Access Questioned*, ASSOCIATED PRESS, Oct. 29, 1997 (explaining that public safety is first priority); *see also* Beiser, *supra* note 50, at 37 (expressing concern over public safety).

[74] *See* Beiser, *supra* note 50, at 37 (noting other costs associated with use of prison labor).

[75] *See id.* (stating hesitancy of businesses to enter into partnership with prisons because of additional costs for training and supervising prisoners).

[76] *See id.*

[77] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 7-12 (discussing American data protection); Reidenberg, *supra* note 42, at 208 (noting that American legal system fails to adequately respond to privacy issues as result of data processing in business sector).

practices.[78] This Part will discuss the current state of federal and state privacy law in the United States, focusing specifically on Texas and California.

A. Federal Law

1. Constitutional Privacy Law Restraining Government

The United States Supreme Court has recognized an implicit right to privacy in the federal Constitution.[79] In *Whalen v. Roe*, the Court interpreted the Due Process Clause to include an informational right to privacy with two components.[80] The first involves the government disclosure of personal or confidential information, while the other involves an individual's right to independence when making important decisions, including when and to what extent his personal information is divulged.[81] With respect to an individual's right to prevent the disclosure of personal information, some lower courts have held that the right to informational privacy only applies to fundamental constitutional rights.[82] Under this interpretation, the Constitution only prevents disclosure of personal information relating to activities that already receive the protections of substantive due process.[83] Likewise, with respect to independence in decision making, lower courts have been unwilling to bar the government's information gathering practices and have restricted Whalen to fundamental interests.[84]

---

[78] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 12 (arguing that patchwork of laws comprises privacy protections in United States).

[79] *See* U.S. CONST. amend. IV (granting rights against search and seizure); *see, e.g.*, Roe v. Wade, 410 U.S. 113, 152 (1973) (noting that Court has recognized that right of personal privacy, or guarantee of certain zones of privacy, exists under Constitution); Griswold v. Connecticut, 381 U.S. 479, 484-85 (1964) (stating that several fundamental guarantees create right of privacy).

[80] *See* Whalen v. Roe, 429 U.S. 589, 598-600 (1977) (noting that one kind of privacy interest protects disclosure of personal matters while another privacy interest recognizes independence in personal decision making). *But see* Florida Star v. B.J.F., 491 U.S. 524, 531 (1989) (refusing to hold newspaper liable for publishing name of victim of sexual offense because it had obtained personal information lawfully and matter was of public interest).

[81] *See Whalen*, 429 U.S. at 605 (holding that government should impose duty of care on data collector to avoid unwarranted disclosures of personal information). The Court recognized the implicit threat to privacy as a result of the collection and use of vast amounts of personal information in computerized data banks. *See id.*

[82] *See, e.g.*, Ramie v. City of Hedwig Village, Texas, 765 F.2d 490, 492 (5th Cir. 1985); Plante v. Gonzalez, 575 F.2d 1119, 1124 (5th Cir. 1978).

[83] *See, e.g.*, Gutierrez v. Lynch, 826 F.2d 1534, 1539 (6th Cir. 1987).

[84] *See, e.g.*, Fadjo v. Coon, 633 F.2d 1172, 1174-76 (5th Cir. Unit B Jan. 1981); Faison v.

Constitutional protection for data privacy in the private sector is even more restricted for two reasons. First, the Constitution protects individuals against governmental intrusion and not that of private entities.[85] State action is present when the government encourages private activities that serve a public function traditionally and exclusively occupied by the state.[86] Similarly, private actors can violate the constitutionally protected right to privacy when a close nexus exists between the government and the private entity.[87] Thus, private sector data processing is only subject to constitutional constraints where the government has encouraged private sector participation in largely public activities or has a sufficiently close relationship with the private entity. As a result, most private sector data processing is unlikely to meet the state action requirement because the hiring of prisoners as data entry employees is not an activity the government has either encouraged or traditionally occupied.[88] Nor is there sufficient entanglement between the government and those private entities which process personal information.[89] For example, on at least one occasion, a federal court has held that a private entity's sharing of information with the government does not constitute state action.[90]

In addition, the Constitution does not affirmatively impose a duty on government to take action. Most of the constitutional rights are "negative rights" that allow individuals to prevent certain

---

Parker, 823 F. Supp. 1190, 1198, 1201-02 (E.D. Pa. 1993).

[85] *See* U.S. CONST. amend. XIV, § 1 (applying Constitution to state action). The general exception to the state action requirement is the Thirteenth Amendment, which prohibits slavery and involuntary servitude in the United States. *See* Clyatt v. United States, 197 U.S. 207, 216-18 (1905).

[86] *See* Marsh v. Alabama, 326 U.S. 501, 506 (1946) (applying "public function" doctrine to shopping center when private entity performs governmental function and such conduct constitutes state action).

[87] *See, e.g.*, Blum v. Yaretsky, 457 U.S. 991, 1004 (1982) (holding that state is responsible for private decisions only when its exercise of coercive power provided significant encouragement); Evans v. Newton, 382 U.S. 296, 299 (1966) (holding that private conduct that is so entwined with government policy or character falls under state action); Shelley v. Kraemer, 334 U.S. 1, 20 (1948) (discussing "nexus" theory in racially restrictive covenants in which government is sufficiently involved or benefits from private party's act to constitute state action).

[88] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 33.

[89] *Compare* Flagg Bros. v. Brooks, 436 U.S. 149, 157 (1978) (holding that private entity's proposed sale of personal goods was not "state action") *with* Soldal v. Cook County, Ill., 506 U.S. 56, 72 (1992) (holding that seizure of trailer by company and local police violated Fourth Amendment).

[90] *See* United States v. Shuckahosee, 609 F.2d 1351, 1354 (10th Cir. 1979) (holding that private organization's voluntary aid of law enforcement does not rise to Fourth Amendment or broader constitutional protections against invasions of privacy).

government action.[91] The Supreme Court generally limits the protection of an individual's "reasonable expectation" of privacy to the Fourth Amendment, which protects against unreasonable government searches and seizures.[92] However, the Constitution does not require the government to actively protect personal information. Instead, the constitutional right to privacy negatively prevents the government from collecting and using personal information in an unconstitutional manner.[93] Because constitutional restrictions on data processing in the private sector are inadequate, data privacy advocates must look to federal and state statutes and the common law.

2. Statutory Privacy Law in the Private Sector

The Privacy Act regulates how federal agencies collect and use personal information.[94] The Freedom of Information Act provides when federal agencies may permit third parties to access their records.[95] However, the private sector has no comparable comprehensive measures that regulate information processing. Furthermore, both federal statutes do not apply to state governments.[96]

Congress also has yet to comprehensively address privacy expectations in light of today's technological advances. Instead, Congress has enacted privacy laws applicable to specific private industries including financial services,[97] telecommunications,[98] educa-

---

[91] *See* DeShaney v. Winnebago County Dep't of Soc. Serv., 489 U.S. 189, 195-98 (1989) (holding that government failure to remove petitioner from abusive father did not constitute violation of rights under Due Process Clause).

[92] *See* U.S. CONST. amend. IV (protecting citizens against unreasonable search and seizure by government); *see also* Katz v. United States, 389 U.S. 347, 360-62 (1967) (detailing various Fourth Amendment decisions). For example, the Court has found diminished expectations of privacy when individuals act in public activities and when a third party controls another's property. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 573-76 (1991) (debating whether there is reasonable expectation of privacy in luggage or closed container in vehicle). Furthermore, the Court has not found any Fourth Amendment protection when an individual's expectation of privacy fails to match a reasonable societal expectation of privacy. *See, e.g.*, California v. Craolo, 476 U.S. 207, 215 (1986) (holding that it is unreasonable to expect that marijuana plants were constitutionally protected from observation from air where planes are commonplace).

[93] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 31, 35.

[94] *See* 5 U.S.C. § 522a (1994). However, the Privacy Act does not apply to private organizations or nonprofit corporations that conduct business with the United States.

[95] *See id.*

[96] *See* SCWHARTZ & REIDENBERG, *supra* note 67, at 21.

[97] *See* Fair Credit Billing Act of 1974, 15 U.S.C. § 1666 (1994) (giving consumers rights to correct erroneous personal information); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t (1998) (defining rights relating to individual's personal information on credit

tion,[99] employment,[100] and home entertainment.[101] Moreover, with the exception of video rental and cable services, none of these federally regulated industries have comprehensive laws governing the collection, storage, use, and dissemination of personal information.[102] An example of a federal statute that is specifically tailored to a particular industry is the federal Video Privacy Protection Act, known as the "Bork Bill," which prohibits the disclosure of titles of video sales and rentals.[103] Congress enacted this legislation because of public outrage after a magazine published the video titles rented by then-federal appellate judge and U.S. Supreme Court nominee Robert Bork. Ironically, while video rentals are protected, pay-per-view movies that consumers watch in their own homes are not.[104] Moreover, information regarding similar types of personal information, such as book purchases and CD ROM titles, are not protected from disclosure. One commentator even noted that video rental records receive greater statutory protection than medical records.[105]

Other federal privacy laws similarly fail to protect individuals adequately.[106] For example, the Federal Credit Reporting Act does

---

worthiness, credit standing, and character of consumer fair credit reporting agency); Electronic Funds Transfer Act of 1978, 15 U.S.C. §§ 1693-1693r (1994) (mandating collection of certain data, such as time and place of transactions, and requiring account statements to consumers).

[98] *See* Communications Act of 1984 and Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2520, 2701-2709 (1998) (imposing criminal sanctions for wiretapping and surveillance activities).

[99] *See* Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b)(1) (1998) (prohibiting disclosure of student records to third parties without prior written consent).

[100] *See* Equal Employment Opportunity Act, 42 U.S.C. § 2000e (1988) (prohibiting use or classification of information relating to personal characteristics like race, color, sex, and religion for unlawful employment discrimination).

[101] *See* Videotape Privacy Protection Act of 1986, 18 U.S.C. §§ 2710-2711 (1998) (prohibiting disclosure of titles of rented videos); Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)(1) (1994) (requiring cable companies to inform customers of any collection of personal information, purposes for its collection, disclosures, and procedures for access).

[102] *See* Reidenberg, *supra* note 42, at 201, 219-20 (discussing lack of industry-specific regulations).

[103] *See* 18 U.S.C. §§ 2710-2711.

[104] *See* Bernstein, *supra* note 8, at A1 (discussing government privacy intrusions).

[105] *See* Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy, and Health Care Reform*, 23 HASTINGS CTR. REP. 13 (1993) (denouncing lack of protection for medical records).

[106] *See id.* (discussing lack of systematic and omnibus federal privacy laws in data processing). On a related note, the individual will receive little data privacy protection in general because modern technical advances will likely restrict what an individual can claim as a reasonable expectation of privacy. *See* Bernstein, *supra* note 8, at A1 (noting technology's

not mandate that individuals be notified of the collection or disclosure of their credit information.[107] Similarly, the Electronic Communications Privacy Act permits disclosure of the contents of a private communication with the consent of one party.[108] Yet the statutory definition of "contents" does not include specific details of the transactions such as the time, place, and length of a telephone call.[109] Moreover, the Family Education Rights and Privacy Act does not regulate the kind of information that schools may collect or the duration for storing student records.[110] Federal law insufficiently protects data privacy precisely because it lacks a comprehensive scheme aimed at specifically regulating data processing activities.[111]

The first step toward improving data privacy protection involves the regulation of prison labor involved in processing personal information. Congress enacted the Prison Industry Enhancement Act of 1984 to allow state-run prison industries to hire prisoners to manufacture and sell their products on the open market.[112] How-

---

threat to personal privacy). Courts are less likely to find a reasonable expectation of privacy in personal information now that electronic mail, fax, modems, cordless phones, caller identification, computers, beepers, and the Internet are commonplace. *See, e.g.*, United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion) (holding that subjects recorded via hidden radio bugs do not receive Fourth Amendment protections for content of conversation because anyone can wear electronic surveillance device). Legal scholars agree that the law of privacy is lagging behind the Information Age. *See* Ericson, *supra* note 17 (stating that technology erodes individual's reasonable expectation of privacy because it makes information easier to access, duplicate, record, or steal). Even automated teller machines, credit cards, and supermarket discount cards make counterfeiting and identity theft ordinary. *See* Bernstein, *supra* note 8, at A1 (tracing modern technological advances of everyday life).

[107] *See* 15 U.S.C. § 1681b (1998) (allowing disclosure without consent); 15 U.S.C. § 1681g (requiring no notice to individual before data collection).

[108] *See* 18 U.S.C. § 2511(3)(b) (1994).

[109] *See id.* § 2510(8).

[110] *See* 20 U.S.C. § 1232g (1990 and Supp. 1998).

[111] *See* Bernstein, *supra* note 8, at A1 (noting inconsistencies in privacy laws that govern private sector). American citizens are not the only constituents left unprotected by U.S. privacy laws. American companies that compete in the international marketplace are vulnerable to more stringent foreign regulations. *See* Reidenberg, *supra* note 42, at 198 n.16 (listing Norway, Austria, Germany, and Sweden as countries that have imposed restrictions on internationally transmitting personal information). Similarly, several European countries have prohibited the transfer of personal information to countries that appear to have little or no privacy concerns. *See, e.g.*, Commission Nationale de L'informatique et des Libertes, 10e Rapport au President de la Republique et au Parlement, Annexe 9, at 308-09 (1989) (restricting transfer of personal information from France to Italy on privacy grounds). To compete internationally, the United States must adopt laws that respond to the privacy issues raised by current data processing activities in America and abroad.

[112] *See* Prison Industry Enhancement Act of 1984, 18 U.S.C. § 1761 (1984) (prohibiting transfer of prison-made goods in interstate commerce unless prisoners are participating in

ever, the Act did not address the privacy interests of third parties when prisoners process personal information.[113] In 1996, Congress took a first step when California Senator Dianne Feinstein and New Jersey Representative Bob Franks introduced the Children's Privacy Protection and Parental Empowerment Act to prevent the sale or purchase of personal information about children without parental consent.[114] This legislation would also have prohibited prisoners and convicted sex criminals from processing personal information of children; required list brokers and solicitors to disclose to parents, upon request, the source and content of personal information on file about their children; and banned any exchange of personal information of children that would be likely to result in harm.[115] The legislation, however, stalled in the Senate Judiciary Committee. Senate Bill 2326, currently pending in the Senate Committee on Commerce, Science, and Transportation, provides for similar protection, but limits its scope to the Internet.[116] While these bills represent a significant first step to address parents' privacy concerns about their children, Congress still needs to adopt stronger measures protecting personal information that are applicable to all persons.

B. State Law

1. Constitutional Privacy Law Restraining Government

A number of state constitutions have also recognized a fundamental right of privacy.[117] However, with the exception of California, they only protect citizens against government intrusion on privacy. They do not protect citizens from each other. Moreover,

---

supervised work program in penal or reformatory institution).

[113] *See id.*

[114] *See Feinstein Bill to Keep Info on Children Private*, NEWSBYTES, May 23, 1996, *available in* 1996 WL 10475857. Senator Feinstein learned that a television reporter in Los Angeles, using the name of Polly Klass's convicted killer Richard Allen Davis, was able to purchase from Metromail a list of detailed information about children. *See id.* The reporter, who used Davis's name, a fictitious business, phone number, address, and paid by money order, said that Metromail did not conduct any screening to prevent such information from being sold to child molesters. *See id.*

[115] *See* Children's Privacy Protection and Parental Empowerment Act, H.R. 3508 and S. 1908, 104th Cong. (1996).

[116] *See* S. 2326, 105th Cong. (1997).

[117] *See* ALASKA CONST. art. I, § 22; ARIZ. CONST. art. 2, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; ILL. CONST. art. 1, § 6; LA. CONST. art. 1, § 5; MONT. CONST. art. II, § 10; PA. CONST. art. I, § 1.

thirty-seven of the fifty states have no law directly applicable to government processing of personal information.[118]

2. The Common Law Right to Privacy

The majority of American states have recognized Prosser's common law right to privacy in some form.[119] However, these common law torts inadequately protect data privacy because they are too broad in scope and fail to account for the specific needs involved in data processing activities. For example, they do not impose affirmative obligations such as providing notice, ensuring the quality and accuracy of the data, or maintaining its security. Finally, legitimate violations of the data privacy right often do not fall within the rubric of Prosser's torts.[120] For example, because consumers voluntarily disclose their personal information, completing surveys for coupons and free samples does not meet the elements of the "intrusion upon seclusion" tort.[121] Similarly, the "public disclosure of private facts" tort is not applicable because it only involves the unauthorized publishing of information.[122] Moreover, courts have generally ruled that restricting the distribution of personal information to narrow groups of recipients provides a safe haven for companies that publicly disclose information.[123] Furthermore, the exchange of personal information between data processing companies, no matter how private or embarrassing, does not qualify as

---

[118] *See* ALASKA STAT. § 44.99.300 (Michie 1993); CAL. CIV. CODE § 1798 (West 1998); CONN. GEN. STAT. ANN. § 4-190 (West 1988 & Supp. 1998); HAW. REV. STAT. § 92F (1993 & Supp. 1997); IND. CODE § 4-1-6 (1993); MASS. GEN. LAWS ANN. ch. 66A, § 1-3 (West 1994 & Supp. 1998); MINN. STAT. ANN. §§ 13.01-13.10 (West 1997 & Supp. 1998); N.H. REV. STAT. ANN. § 7-A:1 (1994); N.Y. PUB. OFF. LAW §§ 91-99 (McKinney Supp. 1998); OHIO REV. CODE ANN. §§ 1347.01-1347.99 (Anderson 1994 & Supp. 1998); UTAH CODE ANN. §§ 63-2-101-63-2-909 (1997); VA. CODE ANN. §§ 2.1-377-2.1-386 (Michie 1995 & Supp. 1998); WIS. STAT. ANN. §§ 19.62-19.80 (West 1996).

[119] *See supra* note 42 (listing state statutes and courts that have adopted privacy protection in one form or another).

[120] *See generally* Reidenberg, *supra* note 42, at 221-27 (discussing inapplicability of Prosser's torts to data processing activity).

[121] *See id.* at 224. In the context of data processing, an "intrusion upon seclusion" tort occurs from the methods of collecting personal information rather than its dissemination. *See id.*

[122] *See id.* at 223-24. Companies do not reveal the facts that consumers disclosed in surveys to the public, nor are they highly intimate or embarrassing enough to meet this threshold. *See id.* at 223.

[123] *See, e.g.*, Polin v. Dun & Bradstreet, Inc. 768 F.2d 1204, 1206 (10th Cir. 1985) (finding that no "false light" claim because credit reporting service did not sufficiently publicize personal information).

a public disclosure. The "false light" tort also does not apply to the collection and processing of personal data because the information at issue is usually not erroneous.[124] Finally, the "misappropriation" tort is only useful against the unauthorized use of a person's name, identity, or likeness for commercial purposes.[125] But government agencies and businesses that collect and disseminate personal information do not normally use individual names or likenesses to advertise or sell products.[126] Indeed, no state court has applied the common law privacy torts to prisoner access of personal information.

3. Statutory Privacy Law in the Private Sector

Congress is not alone in failing to provide comprehensive legislation governing data processing in the private sector. State privacy laws also inadequately protect consumers' interests by failing to consider public safety and informational privacy. Like the federal government, many states have enacted privacy laws applicable to specific industries in the fields of financial services,[127] telecommunications,[128] home entertainment,[129] employment,[130] and insurance.[131] Except for video rental and cable services, not one of these state laws systematically addresses notice or consent to the collection of personal information, the use of personal informa-

---

[124] *See* Reidenberg, *supra* note 42, at 225 (stating that companies have every incentive to collect accurate information to create consumer profiles for marketing).

[125] *See id.* at 226 (stating that "misappropriation" tort may not apply if individual gives appearance of consent or publicly discloses information).

[126] *See* Graham, *supra* note 46, at 1412 (stating that businesses do not advertise products with personal information).

[127] *See, e.g.*, LA. REV. STAT. ANN. § 9:3571 (West 1997); ME. REV. STAT. ANN. tit. 10, §§ 1311-1329 (West 1997 & Supp. 1998); MASS. ANN. LAWS ch. 93, §§ 50-68 (Law. Co-op. 1985 & Supp. 1991); N.M. STAT. ANN. §§ 56-3-1 to -8 (Michie 1996); N.Y. GEN. BUS. LAW § 380 (McKinney 1984 & Supp. 1991).

[128] *See, e.g.*, ALA. CODE §§ 13A-11-30 to -37 (1994 & Supp. 1997); DEL. CODE ANN. tit. 11, §§ 1335-1336 (1995); MINN. STAT. ANN. §§ 626A.02(1)-(3) (West Supp. 1998); 18 PA. CONS. STAT. ANN. §§ 5701-5775 (West 1983 & Supp. 1998).

[129] *See, e.g.*, CAL. CIV. CODE § 1799.3 (West Supp. 1998); CAL. PENAL CODE § 637.5 (West 1988 & Supp. 1998); CONN. GEN. STAT. ANN. §§ 53-420 to -422 (West 1994 & Supp. 1998); CONN. GEN. STAT. ANN. § 53-450 (West Supp. 1994); DEL. CODE ANN. tit. 11, § 925 (1995); MICH. COMP. LAWS ANN. §§ 445.1711-.1715 (West Supp. 1991); N.J. STAT. ANN. §§ 48:5A-54 to -63 (West Supp. 1991); R.I. GEN. LAWS § 11-18-32 (1994); WIS. STAT. ANN. § 134.43 (West 1989).

[130] *See, e.g.*, CONN. GEN. STAT. ANN. §§ 31-128a to -128h (West 1997); MASS. ANN. LAWS. ch. 149, § 52C (Law. Co-op. 1989).

[131] *See, e.g.*, CONN. GEN. STAT. ANN. §§ 38-508, -509 (West 1987); D.C. CODE ANN. §§ 35.221-.299 (1988 & Supp. 1990); GA. CODE ANN. §§ 33-39-9 to -23 (Harrison 1990).

tion, or its storage.[132] Some state statutory data protections are derived from federal mandates, including state laws regulating access to educational records and child abuse data banks.[133] While every state has some form of data protection, no two states have adopted the same regulation, resulting in an amalgam of legislation that, when taken as a whole, fails to adequately protect data privacy.[134]

Since 1990, thirty states have legalized the private industry's hiring of prison labor to perform a variety of jobs, including taking hotel reservations over the phone,[135] entering data,[136] restocking shelves,[137] manufacturing car parts,[138] and packaging golf balls.[139] Yet only Texas, California, and Utah[140] have statutorily addressed the possible ramifications of allowing prisoners access to personal information. For two examples of state privacy laws, this Comment looks to Texas and California.

a. Texas Law

(1) *Dennis v. Metromail*

In June 1994, Beverly Dennis received a sexually explicit and highly offensive handwritten letter from Hal Parfait, a convicted rapist and burglar.[141] As one of hundreds of convicted sex felons

---

[132] *See* Reidenberg, *supra* note 42, at 227-36 (discussing lack of comprehensive statutory privacy protection in American states). Reidenberg notes that state laws generally offer greater privacy protections than federal laws. *See id.* at 234-35. However, state laws do not necessarily give individuals privacy protection left by the gaps in federal laws. *See id.*

[133] *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1990 and Supp. 1998) (requiring states to provide data protection for student records as condition for receiving federal funds for institutions of higher learning); Child Abuse Prevention and Treatment Act, 42 U.S.C. § 5106a(b) (1994) (establishing requirements for collection, storage, and dissemination of information in data banks on child abuse for states to be eligible for federal funds).

[134] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 129.

[135] *See* Parenti, *supra* note 54, at 11 (noting that New Mexico prisoners take phone reservations for hotels).

[136] *See id.* (stating that Ohio prisoners perform data entry work).

[137] *See id.* (stating that Toys R Us store in Chicago used night shift of prisoners to restock merchandise).

[138] *See id.* (stating that Ohio prisoners make car parts for Honda Corporation).

[139] *See id.* (noting that prisoners in Hawaii package golf balls for Spalding Company).

[140] See UTAH CODE ANN. § 13-26-11 (1998) (prohibiting telephone soliciting businesses from employing prisoners as operators where they have access to personal information under Utah's Telephone Fraud Prevention Act).

[141] *See* Plaintiff's Fifth Amended Class Action Petition at 23-24, Dennis v. Metromail (Tex. Dist. Ct., Jan. 9, 1998) (No. 9604451). In his letter to Dennis, Parfait wrote, "If you are into sixty-nine, then I am definitely game . . . If I could be there to rub in your Neutrogena . . . I'll close my eyes and recall your bedroom as I made passionate, romantic, love to

entering computer data for Metromail under a state prison work program,[142] Parfait had access to the personal details of Dennis's life provided by her questionnaire answers.[143] In 1996, Dennis brought a class action suit against several corporate defendants, including Metromail,[144] alleging violations of privacy.[145]

The *Dennis* class plaintiffs argue that the corporate defendants[146]

---

you as you moaned in my ear . . . It can only be in letters at the moment; maybe later, I can get over to see you." *Id.*

[142] *See id.* at 4 (stating that hundreds of inmates process data for private entities as part of prison industry work program); *Prime Time Live, supra* note 1 (showing inmates entering data, telemarketing, and filing).

[143] *See* Plaintiff's Fifth Amended Class Action Petition at 10, *Dennis* (No. 9604451) (stating that Texas prisoners routinely processed personal information).

[144] *See id.* Dennis filed a class action suit on April 18, 1996, after searching for almost two years for a lawyer who would represent her free of charge in her unusual case. *See* Bernstein, *supra* note 8, at A1 (discussing Dennis's struggle for redress).

[145] *See* Plaintiff's Fifth Amended Class Action Petition at 3, 27-36, *Dennis* (No. 9604451) (describing third cause of action for invasion of privacy by common law torts of "misappropriation" and "public disclosure of private facts" and fourth cause of action for negligent invasion of privacy). However, Dennis's complaint pleads fraud as the first cause of action, alleging that Metromail failed to disclose that (1) the actual purpose was requesting consumers' personal information; (2) such information would not be used for sending coupons and product samples; (3) such information would be maintained in Metromail proprietary database; (4) such information would be provided to entities other than national grocery product manufacturers who did not send any coupons, samples, or offers of consumer goods anyway; (5) such information would be used for purposes other than to send coupons, samples, or offers of consumer goods; and (6) prisoners would have access to such information. *See id.* at 16-18; Interview with Robert M. Long, *supra* note 16 (acknowledging that privacy is not heart of complaint, but fraud because Metromail solicited personal information under false pretenses by failing to disclose that convicted felons would have access to such information). Other allegations include negligent misrepresentation, negligence, gross negligence, negligent entrustment, breach of implied contract, and unjust enrichment. *See* Plaintiff's Fifth Amended Class Action Petition, at 27-46, *Dennis* (No. 9604451). The class-action suit is on behalf of all citizens whose privacy interests, safety, and physical and emotional well-being are being injured. *See id.* at 3. In addition to compensatory and punitive damages for class members' injuries and expenses, the lawsuit seeks equitable relief so that defendants (1) return their wrongfully acquired profits, (2) are prohibited from continuing their wrongful conduct, (3) take reasonable steps to eliminate future harm, (4) redress future inquiries through a monitoring system, (5) establish a fund for victims, and (6) are prohibited from using prisoners to process personal information. *See id.* at 3-4.

[146] *See* Plaintiff's Fifth Amended Class Action Petition, at 7-9, *Dennis* (No. 9604451). In addition to Metromail, Dennis is suing R.R. Donnelley & Sons, Inc. and Computerized Image & Data Systems, Inc., who were also involved in the use of prison labor to process the consumer surveys. *See id.* Dennis previously sued the Texas Department of Criminal Justice ("TDCJ") for negligence in misusing Texas prison facilities and equipment to process personal information of consumers without their knowledge or consent. *See* Plaintiff's Third Amended Class Action Petition at 2, 11-13, 16, Dennis v. Metromail (Tex. Dist. Ct., Apr. 14, 1997) (No. 9604451) (on file with author). Dennis's third amended complaint alleged that State defendants failed to (1) prevent Parfait's letter from being sent, (2) take reasonable steps to safeguard the foreseeable misuse of personal information by prisoners, and (3) disclose to consumers that prisoners would have access to such information. *See id.* at 16. However, the Texas district court dismissed claims against TDCJ and its representatives

wrongfully deceived consumers into disclosing personal information through a coupon offer, used cheap prison labor to process the information, and then sold the information for commercial gain.[147] Specifically, they claim an invasion of privacy under the common law "misappropriation" and "public disclosure of private facts" torts.[148] They allege that corporate defendants misappropriated and wrongfully disclosed their personal and private information without their knowledge or consent to hundreds of convicted felons.[149] The *Dennis* class members argue that providing personal information for the purpose of receiving "Free coupons" with "No gimmicks" does not constitute permission for other uses.[150] Metromail's questionnaires failed to disclose that the company would (1) use personal and private information for any purpose other than to mail coupons and samples; (2) provide such information to parties other than the companies sending the coupons and samples; and (3) give the information to convicted felons.[151]

In response to the class's allegations, Metromail[152] and its parent

---

under government immunity of the Texas Torts Claims Act. *See* TEX. CIV. PRAC. & REM. CODE ANN. §§ 101.001-.021 (West 1997 & Supp. 1998). The court found that solicitation, misuse, and disclosure of information was not actionable against a state entity. *See generally* Defendants Texas Department of Criminal Justice, Wayne Scott, and Alan Polunksy's Motion for Summary Judgment and Severance, Dennis v. Metromail (Tex. Dist. Ct., Jan. 9, 1997) (No. 9604451) (on file with author) (claiming plaintiffs do not have reasonable expectation of privacy); Plaintiff's Response to Defendants' Motion for Summary Judgment, Dennis v. Metromail (Tex. Dist. Ct., Apr. 7, 1997) (No. 9604451) (on file with author) (alleging defendant used private information and allowed state prisoners to view it); Defendants Texas Department of Criminal Justice, Wayne Scott, and Alan Polunksy's Motion Reply to Plaintiff's Response to Motion for Summary Judgment and Severance, Dennis v. Metromail (Tex. Dist. Ct., Apr. 11, 1997) (No. 9604451) (on file with author) (refuting plaintiff's claims); Order on Motion for Summary Judgment and Severance, Dennis v. Metromail (Tex. Dist. Ct., Apr. 14, 1997) (No. 9604451) (on file with author) (granting summary judgment and severance).

[147] *See* Plaintiff's Fifth Amended Class Action Petition at 2, *Dennis* (No. 9604451) (alleging defendants' wrongdoing). Plaintiffs alleged that corporate defendants intentionally deceived working class and elderly American consumers. *See id.* at 2-3.

[148] *See id.* at 27-33 (discussing privacy cause of action).

[149] *See id.* Under the TDCJ work program, hundreds of prisoners from six prison work factories called record conversion units enter data into computers and prepare data for microfilm for state and local government, and, in this instance, for private business. *See id.* at 14. Dennis's complaint documents a known history of at least 12 incidents of misconduct by Texas prisoners in the record conversion units of TDCJ. *See id.* at 14, 20-21, 39-44.

[150] *See id.* at 16 (describing advertisement for Metromail questionnaire).

[151] *See id.* at 18-19 (claiming consumers did not consent to prisoner access to information).

[152] *See General Counsel Says Metromail Expects to Prevail in Lawsuit; Condemns Misinformation in PR Campaign by Plaintiffs' Lawyers*, PR NEWSWIRE, Apr. 28, 1997, *available in* LEXIS, News Library, Prnews File (noting that Metromail's counsel has stated that company has implemented "industry leading controls over collection, management and dissemination of con-

company, R.R. Donnelley, claim they did not know prisoners performed the data processing for them because another defendant, Computerized Image & Data Systems, subcontracted the work to the Texas prison system.[153] However, discovery documents reveal that Metromail and the prison shipped the consumer surveys back and forth.[154] Records show that three shifts of prisoners regularly handled thousands of Metromail consumer questionnaires and surveys for Seventeen magazine, L'Oreal, Six Flags, Days Inn, Phillip Morris, R.J. Reynolds, Time-Life, and Coca-Cola[155] and continued to do so for at least three months after Parfait's letter became public in 1994.[156] The corporate defendants in Dennis counter that the consumers were not guaranteed a reasonable expectation of privacy because they voluntarily disclosed their personal information.[157] While *Dennis* is still in its pretrial stages, Texas law-

---

sumer information"). As a leading provider of direct marketing with 3200 employees, Metromail has information on more than 146 million individuals and 90% of U.S. households. *See id.* Metromail integrates consumer information into a market database, including a "Behavior Bank" of consumer spending habits, preferences, and activities. *See* Plaintiff's Fifth Amended Class Action Petition at 12, *Dennis* (No. 9604451).

[153] *See* Miller, *supra* note 12, at B5 (discussing corporate defendants' alleged ignorance of prison data processors); *see also Class Action Expands Against Metromail and Donnelley over Privacy Violations; Broader Focus, New Plaintiffs Target Deceptive Collection and Sale of Data; Return of Profits Sought*, BUSINESS WIRE, Apr. 30, 1997, *available in* LEXIS News Library, Bwire File (stating that Computerized Image handled work for Texas prison in past).

[154] *See Class Action Expands Against Metromail and Donnelley Over Privacy Violations, supra* note 153.

[155] *See A Prison in a Growth Industry, supra* note 65, at A1 (naming corporate clients for whom Metromail has processed information in Texas prison facilities).

[156] *See id.* (noting that Metromail received $150,000 for handling surveys).

[157] *See Prime Time Live, supra* note 1 (summarizing corporate defendants' defense to *Dennis*); Ericson, *supra* note 17 (citing Metromail's argument in motion to dismiss that plaintiffs in *Dennis* lacked basis for privacy claim because they voluntarily disclosed their personal information). Corporate defendants have invoked the defense of consent similar to that used in the unrelated 1985 decision of *Douglass v. Hustler Magazine, Inc.*, 769 F.2d 1128 (7th Cir. 1985). In that case, an actress successfully sued Hustler magazine because it published nude photos taken only for Playboy without her consent. *See id.* at 1137-39. The magazine argued that plaintiff consented to have her photos appear in any lawful setting, thus removing any reasonable expectation of privacy. *See id.* at 1137. However, the court found that plaintiff signed a limited release for Hustler's use of her photographs, which she intended for publication only in Playboy. *See id.* at 1137-39; *see also R.R. Donnelley, Biggest Kids' Data Firm, Cites "Hustler" Magazine Defense, Says Families Lose Privacy Rights in Consumer Surveys; Giant Class Action Suit Targets Company that Gave Information on at Least 1.3 Million U.S. Families to Sex Offenders in Texas Prison*, BUSINESS WIRE, June 13, 1996, *available in* LEXIS, News Library, Bwire File (discussing Donnelley's and Metromail's defense to their practice of collecting and selling information on millions of children and use of prison labor).

Metromail has since discontinued the use of prison labor because of the *Dennis* case. *See* Ericson, *supra* note 17 (stating that Metromail no longer uses prison labor). Instances of inmate abuse of personal information also occurred prior to the *Dennis* case. *See Prime Time Live, supra* note 1 (noting problems in Texas prison). While the *Dennis* case is still pending

makers have not hesitated in responding to the privacy concerns arising out of convicted felons' access to personal consumer information, passing legislation in 1995 and 1997.

(2) Statutory Data Privacy Protection

Texas, which does not have any constitutional protections for privacy, recognizes three of the four common law privacy torts.[158] Unlike most states, Texas has several statutes that specifically restrict prisoners' contact with personal information. In 1995, responding to news accounts of Parfait's letter to Dennis, the Texas Legislature added section 38.111 to the Texas Penal Code to prohibit prisoner misuse of information gained through any work program.[159] Any violation constitutes a third degree felony.[160] The Texas Legislature also enacted two new statutes. One eliminates or reduces good time credit for convicted felons in state prison who have misused personal information[161] and the other prohibits such

---

as of this writing, the TDCJ has acknowledged problems in the past with prisoner access to personal information. *See* Plaintiff's Fifth Amended Class Action Petition at 20-21, 39-44, *Dennis* (No. 9604451). For example, prisoners inserted obscene messages while mailing out brochures for the Texas tourist department. *See Prime Time Live, supra* note 1 (noting problems in Texas prison). Prisoners also smuggled at least one thousand motor vehicle titles in a car theft ring headquartered at the prison. *See id.*

[158] *See* Matthews v. Wozencraft, 15 F.3d 432, 436 (5th Cir. 1994) (holding that life story does not constitute "name" or "likeness" under Texas "misappropriation" tort); Cain v. Hearst Corp., 878 S.W.2d 577, 578 (Tex. 1994) (holding that Texas does not recognize "false light" tort); Hogan v. Hearst Corp., 945 S.W.2d 246, 250 (Tex. Ct. App. 1997) (holding that newspaper's publication of arrestee's name, birthday, and reason for arrest obtained from public records does not rise to "public disclosure of private facts" tort under Texas law); Farrington v. Sysco Food Services, Inc., 865 S.W.2d 247, 253 (Tex. Ct. App. 1993) (noting that plaintiff's consent negates claim of "intrusion upon seclusion" tort under Texas law); *see also* Billings v. Atkinson, 489 S.W.2d 858, 859 (Tex. 1973) (holding that Texas recognizes common law right of privacy).

[159] *See* TEX. PENAL CODE ANN. § 38.111 (West 1998). Under this section, a prisoner who discloses or uses personal information with the intent to benefit, harm, or defraud another prisoner or another individual is guilty of committing a felony of the third degree. *See id.* As a result of this statute, one Texas prison lost 187 sex offenders from its record-entry work program. *See A Prison in a Growth Industry, supra* note 65, at A1 (quoting director of state prison industries, "We lost some damn good programmers — pedophiles. Some of our best computer operatives were sex offenders."). Another new measure placed restrictions on prisoner access to personal information, such as home address, telephone number, and names and social security numbers of family members, but did not get enacted into law. *See* S.B. 354, 74th Leg., 1994-1995 Reg. Sess. (Tex. 1995).

[160] *See* TEX. PENAL CODE ANN. § 38.111.

[161] *See* TEX. GOV'T CODE ANN. § 498.0041 (West 1996) (authorizing director of correctional facility to forfeit or reduce prisoners' time for good conduct for violation of Texas Penal Code § 38.111).

felons from participating in similar work programs again.[162]

In 1997, the Texas Legislature enacted another law which expanded the scope of Texas's data privacy laws to include all prisoners, not just those convicted of violating the privacy laws.[163] The Texas Legislature acted after a strip search revealed that a prisoner was in possession of a phone number and address of an individual.[164] Because the prisoner had not yet misused the information, he could not be prosecuted under the 1995 law. Therefore, Texas lawmakers amended section 38.111 of the Texas Penal Code to make it a felony for a prisoner to possess, for certain prohibited uses, the personal information of another individual obtained through a prison work program.[165] Moreover, the Texas Legislature enacted a statute which bans all prisoners convicted of violating section 38.111 from participating in such work programs again.[166]

(3) Current Policy and Practice

In 1997, the Texas Department of Criminal Justice ("TDCJ") implemented security measures to prevent the kind of misconduct that resulted in Parfait's 1994 letter to Dennis. The TDCJ also announced a plan to phase out the use of prison labor in its record conversion programs to comply with current Texas law.[167] Nevertheless, the TDCJ renewed a one-year contract with the Texas Department of Transportation, which allegedly needed more time to secure an alternative to processing vehicle registrations and license renewal records.[168] The information on the vehicle registration

---

[162] *See* TEX. GOV'T CODE ANN. § 507.028 (West 1996) (stating that defendants convicted under Texas Penal Code § 38.111 are barred from work programs that provide them with access to personal information of third parties).

[163] *See* TEX. PENAL CODE ANN. § 38.111 (prohibiting possession of personal information by prisoner).

[164] *See* Telephone Interview with Rhett Barniff, Research Assistant, Texas Senate Committee on Criminal Justice (Feb. 4, 1998) (notes on file with author) (discussing impetus for legislation).

[165] *See* TEX. PENAL CODE ANN. § 38.111.

[166] *See* TEX. GOV'T CODE ANN. § 497.098 (West 1997) (prohibiting prisoners convicted of Penal Code § 38.111 from participating in work programs that give them access to personal information in future).

[167] *See* Letter from Wayne Scott, Director, Texas Department of Criminal Justice, to the Texas Senate Criminal Justice Committee (Oct. 23, 1997) (on file with author) (noting that TDCJ eliminated two of four record conversion units). As of September 1, 1997, TDCJ discontinued all contracts with private companies for data entry work which granted prisoners access to personal information. *See id.*

[168] *See id.* (stating that TDCJ is phasing out use of inmate labor); *see also* Plaintiff's Fifth

forms included the owner's name, address, and make and model of car.[169] Texas prisoners manufactured inspection and registration stickers and operated the machines that placed renewal notices into envelopes. They also transferred data from microfilm to computer disks.[170] However, they did not have any writing materials with which to keep information for their own use.[171] As of September 1998, the TDCJ terminated all record conversion contracts and Texas prisoners concluded data entry work for the state transportation department in October 1998.[172]

Additionally, Texas implemented another oversight measure to investigate the potential problems of prisoner data entry. Texas Lieutenant Governor Bob Bullock called on a state senate committee to study the effectiveness of prohibiting prisoner access, usage, possession, and disclosure of the personal information of third parties, and to make recommendations to prevent prisoner abuse of information.[173] The committee published its findings in an October 1998 report.[174]

The Texas Legislature has responded to the *Dennis* class plaintiffs by enacting statutes that deny prisoners access to the personal information of third parties.[175] However, the TDCJ did not have to enter into a one-year renewal contract, and even after it did, a court should have declared the contract void as against public policy for endangering the safety and well-being of its citizens.[176] The risk of another *Dennis* incident is too great. The *Dennis* plaintiffs

---

Amended Class Action Petition at 32, Dennis v. Metromail (Tex. Dist. Ct., Jan. 9, 1998) (No. 9604451) (on file with author) (noting that Texas prisoners process public information 99% of time while information processed in Dennis's case was for private business).

[169] *See* Moritz, *supra* note 63, at 7 (listing personal information accessible to Texas prisoners).

[170] *See id.* The prisoners did not have access to online services. *See id.*

[171] *See id.* (indicating daily tasks in processing motor vehicle registrations).

[172] *See* SENATE COMMITTEE ON CRIMINAL JUSTICE, INTERIM REPORT, 76th Legis. 1997-1998 Reg. Sess. (Tex. 1998), at 37-38 [hereinafter INTERIM REPORT].

[173] *See* Moritz, *supra* note 63, at 7 (reporting that state lawmakers called for investigation on safeguards implemented to prevent prisoners from gaining access to personal information); *Prisoner Data Access Questioned*, *supra* note 73, at B5 (explaining that while it is important for prisoners to work to help repay their debt to society, safety must always come first).

[174] *See* INTERIM REPORT, *supra* note 172, at 37-38. However, the committee did not make any recommendations on prisoner access to personal information because administrative and legislative action has cured the problem. *See id.*

[175] *See* TEX. PENAL CODE ANN. § 38.111 (West 1998) (making felonious crime for prisoners to possess, access, and use personal information).

[176] *See* Plaintiff's Fifth Amended Class Action Petition at 2, 37-44, Dennis v. Metromail (Tex. Dist. Ct., Jan. 9, 1998) (No. 9604451) (on file with author) (alleging grave danger to public safety through use of prison labor).

consented only to receiving coupons, not prisoner access to their personal information.[177] Metromail failed to notify the 1.3 million consumers who completed surveys of these "waivers" of their privacy expectations.[178] Even though the Texas prisoners saved taxpayers more than three million dollars last year processing documents for government agencies,[179] the savings came at the expense of public safety.

b. California Law

(1) The Right to Privacy in the Public Sector

California has three primary sources of law that prevent the government from invading an individual's right to data privacy. First, the state constitution guarantees the right to informational privacy.[180] Second, the California Public Records Act prohibits state agencies from disclosing personal information contained in government records, such as employee and medical information, to the public.[181] Under the "public interest balancing test," a government agency may not disclose information if the invasion of an individual's privacy outweighs the public's need for the information.[182] Finally, the California Fair Information Practices Act ("IPA") requires state agencies to maintain records with information that is "relevant and necessary to accomplish a purpose of the agency required by or authorized by the California Constitution or

---

[177] *See id.* (claiming Metromail misrepresented purpose of consumer questionnaire).

[178] *See R.R. Donnelley, Biggest Kids' Data Firm, supra* note 157 (stating Metromail believes consumers have no reasonable expectation of privacy when completing questionnaires). Additionally, the president of Computerized Image described the prison work program giving felons access to sensitive consumer information as "a really wonderful, worthwhile program" even after he learned of Parfait's obscene letter to Dennis. *See* Plaintiff's Third Amended Class Action Petition at 20, Dennis v. Metromail (Tex. Dist. Ct., Apr. 14, 1997) (No. 9604451) (on file with author). Moreover, Metromail's vice president of marketing told the Houston Mayor's Office that there was no disclaimer on the questionnaires because the public was not entitled to know who would screen their personal information. *See id.*

[179] *See* Moritz, *supra* note 63, at 7 (citing taxpayer savings).

[180] *See* CAL. CONST. art. I, § 1; Central Valley Chapter v. Younger, 214 Cal. App. 3d 145, 165-72, 262 Cal. Rptr. 496, 508-12 (Ct. App. 1989) (holding that state Department of Justice unconstitutionally distributed criminal history information to non-law enforcement public and private employers for employment, licensing, and certification purposes).

[181] *See* CAL. GOV'T CODE §§ 6250-6255 (West 1998).

[182] *See* CAL. GOV'T CODE § 6255 (creating balancing test by which state agency justifies nondisclosure of requested records by demonstrating that privacy interests of individual outweigh public interest served by disclosure); Wilson v. Superior Court, 51 Cal. App. 4th 1136, 1144, 59 Cal. Rptr. 2d 537, 542 (Ct. App. 1997) (concluding application should not be made public under balancing test).

statute or mandated by federal government."[183] It also allows individuals to inspect and correct errors in their personal information.[184] Furthermore, the IPA limits secondary uses of information that agencies can collect subject to twenty-three disclosure exceptions.[185]

(2) Protections Against Private Sector Intrusions Upon an Individual's Right to Privacy

Unlike Texas, California has several means of protecting individuals from intrusion upon the right to privacy by the private sector. First, courts can use an explicit provision in the California Constitution to protect the right to data privacy against both public and private encroachment.[186] Second, California courts have adopted Prosser's four common law privacy torts and applied them in the context of private sector violations of privacy.[187] Third, the California Legislature has enacted laws applicable to the processing of personal information by private entities.

(a) The Privacy Initiative of 1972

In contrast to the constitutions of the federal government and the other forty-nine states, the California Constitution contains an explicit right to privacy, the Privacy Initiative of 1972. The Privacy Initiative, among other things, protects personal information.[188] Drafters of the initiative intended the term "privacy" in the state constitution to include data protection.[189] Generally, the California

---

[183] CAL. CIV. CODE § 1798.14 (West 1998).

[184] *See id.* § 1798.32.

[185] *See id.* § 1798.24. The five most important exceptions are the following: (1) to the individual to whom the record pertains, (2) to a person representing the individual or his guardian or conservator, (3) to others with no more than 30 days prior written consent of the individual or in the time limit to which the individual agrees to in the prior written consent, (4) to an agency upon compelling health or safety reasons of the individual, and (5) pursuant to a search warrant. *See id.* § 1798.24(a)-(c), (i), (*l*).

[186] *See* CAL. CONST. art. I, § 1 (providing that right to privacy states, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); *see infra* notes 188-92 and accompanying text.

[187] *See infra* notes 193-97 and accompanying text (discussing application of Prosser's common law privacy torts in California).

[188] *See* CAL CONST. art. I, § 1.

[189] *See* Cal. Proposition 11, *reprinted in* CALIFORNIA BALLOT PAMPHLET: GENERAL ELECTION NOV. 7, 1972, at 26-27 (1972); *see also* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 480-84 (1992) (citing proponent's argument that lack of

Constitution requires state action.[190] However, the California Supreme Court has held that an individual can enforce this right against a private entity.[191] For this reason, California has the strongest constitutional data privacy protection in the United States.[192]

(b) The Common Law Right to Privacy

When the California Supreme Court extended the constitutional right to privacy to the private sector, it underscored the unifying theme of Prosser's common law torts.[193] California courts have used each of the common law privacy torts to protect an individual's right to be let alone in cases involving defamation based on language,[194] misuse of confidential business information,[195] the definition of newsworthy,[196] and the unauthorized publishing of

---

effective restraints on information activities of government and businesses justifies legal and enforceable right of privacy for all Californians).

[190] *See* White v. Davis, 120 Cal. 2d 94, 105, 533 P.2d 222, 233-34 (1975) (finding that undercover police agents recording classroom discussions in university established prima facie violation of constitutional right to privacy).

[191] *See* Hill v. NCAA, 7 Cal. 4th 1, 20, 865 P.2d 633, 644 (1994) (holding that individuals may assert constitutional right to privacy against private entities). The court cited a ballot argument to support the application of the Privacy Initiative to nongovernmental entities: "The right of privacy . . . prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us." *Id.* at 642; *see also* Heda v. Superior Court, 225 Cal. App. 3d 525, 527, 275 Cal. Rptr. 136, 137 (Ct. App. 1990) (holding that defendant's constitutional right to privacy for medical records outweighed plaintiff's motion for trial preference in medical malpractice case). Other decisions have held the Privacy Initiative applicable to private entities. *See Cutter v. Brownbridge*, 183 Cal. App. 3d 836, 843, 228 Cal. Rptr. 545, 549 (Ct. App. 1986) (holding that psychotherapist violated patient's constitutional right to privacy by disclosing details of therapy); *Park Redlands Covenant Control Committee v. Simon*, 181 Cal. App. 3d 87, 97, 226 Cal. Rptr. 199, 205 (Ct. App. 1986) (holding that restrictive covenant for number of residents in homes regardless of square footage abridged unit owner's constitutional right to privacy).

[192] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 135.

[193] *See Hill*, 7 Cal. 4th at 22, 865 P.2d at 647 (discussing applicability of Prosser's common law torts to California).

[194] *See, e.g.*, Fellows v. National Enquirer, Inc., 42 Cal. 3d 234, 251, 721 P.2d 97, 109 (1986) (holding that "false light" tort based on language requires proof of special damages when defamatory meaning does not appear on its face).

[195] *See, e.g.*, Pillsbury, Madison & Sutro v. Schectman, 55 Cal. App. 4th 1279, 1286, 64 Cal. Rptr. 2d 698, 703 (Ct. App. 1997) (noting that direct business competitor could misappropriate confidential business information because "misappropriation" tort involves "pirating of the fruits of another's labors and passing them off as one's own").

[196] *See, e.g.*, Dora v. Frontline Video, Inc., 15 Cal. App 4th 536, 543, 18 Cal. Rptr. 2d 790, 793 (Ct. App. 1993) (noting that relevant factors for "public disclosure of private facts" tort when defining "news worthiness" include social value of facts published, depth of intrusion, and degree individual voluntarily took position of public notoriety).

private matters.[197] However, California courts have not applied Prosser's torts in a factual setting involving intrusions upon an individual's right to protect his personal information by private entities.

(c) Statutory Privacy Law

In response to the *Dennis* case in Texas, the California Legislature recently enacted legislation that bans prisoners convicted of specified offenses from having access to personal information in most work programs.[198] Assembly Bill 2649, which added sections 4017.1 and 507.1 to the California Penal Code and section 219.5 to the California Welfare and Institutions Code, prohibits prisoners from having access to personal information if they have been convicted of, or adjudicated to have committed, any offense (1) involving forgery or fraud, (2) involving misuse of a computer, (3) requiring registration as sex offenders pursuant to section 290 of the California Penal Code, or (4) involving the misuse of personal or financial information of another person.[199]

Those prisoners who have not committed the specified offenses may have access to the personal information of third parties, subject to certain conditions. The new law creates a two-tiered system of prisoners. Adult prisoners who may have access to personal information must disclose the fact of their confinement before taking such information. In contrast, juvenile prisoners with access to personal information are required to disclose their status only if

---

[197] *See, e.g.*, People v. Brown, 88 Cal. App. 3d 283, 290 n.4, 151 Cal. Rptr. 749, 754 n.4 (Ct. App. 1979) (citing example of "intrusion upon seclusion" tort when photographer takes picture of hospital patient who earlier refused interview).

[198] *See* A.B. 2649, 75th Leg., 1997-1998 Reg. Sess. (Cal. 1998) (to be codified at CAL. PENAL CODE §§ 4017.1, 5071 and CAL. WELF. & INST. CODE § 219.5) (defining personal information to include social security numbers, addresses, driver's license numbers, and phone numbers of private individuals). State Assemblywoman Liz Figueroa introduced A.B. 2649 after the *Dennis* case brought to her attention a California prison work program that gives juvenile prisoners working as airline reservationists access to credit card information. *See* Dan Bernstein, *Lawmakers Target High-Tech Intrusions on Private Lives*, SACRAMENTO BEE, Dec. 8, 1997, at A14. California lawmakers have introduced other legislation that would curb abuses by information vendors and marketing companies. *See id.* The California Legislature enacted a related measure that creates misdemeanor crimes for list brokers and others who use personal information about children. *See* A.B. 1792, 75th Leg., 1997-1998 Reg. Sess. (Cal. 1998) (to be codified at CAL. PENAL CODE § 637.9). This is a state version of the federal Children's Privacy Protection and Parental Empowerment Act, which is still pending before Congress. *See supra* notes 114-15 and accompanying text (discussing impetus for federal Children's Privacy Protection and Parental Empowerment Act).

[199] *See* A.B. 2649.

asked.[200] Moreover, this measure mandates random monitoring of telephone calls and constant supervision of the juveniles' other activities that provide access to personal information to assure the sanctity of such information.[201] This new law does not apply to those situations where prisoners have only incidental contact with personal information.[202]

Although California law now regulates the use of prison labor to perform data entry work, citizens are still vulnerable to potential abuses of their personal information for four reasons. First, the new law does not prohibit prisoners from merely possessing personal information.[203] Second, unlike the Texas statutes, which bar all prisoners from contact with personal information, California permits prisoners to process personal information so long as they have not committed certain specified offenses. California should at least prevent prisoners convicted of violent felonies from having access to personal information. Yet, the law fails to specify the penalty for prisoners convicted of the enumerated offenses who manage to access personal information. It also fails to specify a penalty for prisoners who are permitted to access personal information, but did not disclose their confinement, as mandated by law.[204] Finally, California law permits the current practice of permitting juvenile prisoners to process personal information.

(d) Current Policy and Practice

In 1990, California voters approved the Prison Inmate Labor Initiative which permits state prisons to enter into contracts with public entities and businesses for the use of prison labor.[205] The

---

[200] *See id.*

[201] *See id.*

[202] *See* Catherine Bridge, *New Prison Bill a Real Piece of Work*, RECORDER, July 21, 1998, at 5 (noting that A.B. 2649 exempts 4100 prisoners in firefighting work camps who may pass mailboxes or homeowners' property).

[203] *But see, e.g.*, TEX. PENAL CODE ANN. § 38.111 (West 1997) (prohibiting prisoners from possessing, accessing, disclosing, and using personal information).

[204] *See* A.B. 2649 (prohibiting prisoner access to personal information without imposing penalty for violation).

[205] *See* Cal. Proposition 139, *reprinted in* CALIFORNIA BALLOT PAMPHLET: GENERAL ELECTION NOV. 6, 1990, at 65 (establishing joint venture between government and nonprofit or for-profit entity for purpose of employing inmate labor). Since the 1890s, the sale of prison-made goods on the open market has been illegal in California, and prisoners only produced commodities for sale to the government. *See* Telephone Interview with Reggie Drew, Chief Assurance Officer, California Department of Corrections (Jan. 30, 1998) (notes on file with author).

initiative, however, did not address the privacy interests of third parties.[206] Under this initiative, private companies can arrange an in-house correctional facility at the prison to train and hire prisoners as their own employees.[207] This private-public partnership is called the Joint Venture Program in the California Department of Corrections ("CDC") and the Free Venture Program in the California Youth Authority ("CYA").[208]

Through the CYA, the initiative allows juvenile prisoners to answer telephone calls and handle personal information for several state agencies and private businesses.[209] For example, since 1986, juvenile prisoners have been processing personal information for Trans World Airlines ("TWA") as contingency airline reservations

---

[206] *See* Cal. Proposition 139, *supra* note 205, at 65 (permitting companies to set up work facility inside prison).

[207] *See id.*; CALIFORNIA DEPARTMENT OF CORRECTIONS, JOINT VENTURE BROCHURE (1997) (describing prison work program in various state correctional facilities). Tasks include assembling furniture, making license plates, paper products, and shoes, making steel tanks for microbreweries, and making plastics and faucets. *See* Parenti, *supra* note 54, at 11. Currently, the Joint Venture Program operates in 23 correctional institutions. *See* Interview with Reggie Drew, *supra* note 205. One CDC program involves 430 prisoners who manufacture glasses for Medi-Cal recipients where federal law mandates the social security number of the eye wearer on the Medi-Cal form. This form also contains the prescription that prisoners need to make the glasses. CDC stated that it has taken preventative steps to ensure prisoners are "screened" from social security numbers. *See* SENATE COMM. ON PUB. SAFETY ANALYSIS OF A.B. 2649, as amended on June 17, 1998, 75th Legis., 1997-1998 Reg. Sess. (Cal. 1998) [hereinafter A.B. 2649 ANALYSIS]. Ten years ago in Mule Creek, inmates sorted, stacked, and bundled by zip code mail for delivery to the post office, saving the state millions of dollars. *See* Interview with Reggie Drew, *supra* note 205. The department discontinued postal sorting by inmates for public safety reasons. *See id.* Nevertheless, California adult prisoners do perform data entry services for nonsensitive information for private businesses. *See* Parenti, *supra* note 54, at 11. Parenti cites as an example DPAS, a private company in San Francisco, which set up a data processing operation inside San Quentin State Prison. *See id.* DPAS employs 18 prisoners to assemble literature for Chevron, Bank of America, and Macy's Department Store. *See id.*

[208] *See* Parenti, *supra* note 54, at 11; CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, *supra* note 11.

[209] *See* Cal. Proposition 139, *supra* note 205 (allowing private companies to hire juvenile prisoners as employees); CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, *supra* note 11 (describing work programs). Since 1990, juvenile prisoners in the Preston Youth Correctional Facility in Ione, California work as consumer hotline operators for the Department of Consumer Affairs, Bureau of Automotive Repair. *See id.* The juvenile prisoners answer toll-free calls from consumers who need to obtain smog devices to repair and register late model cars. *See id.* When callers give the make and model number of the vehicle and year, juvenile prisoners search the listing of parts suppliers in a computer. *See id.* Currently, five juvenile prisoners are participating in the program, earning $5.15 an hour with incentive raises. *See id.* According to the Administrator of the Free Venture Program, the prisoners do not receive any personal information from the caller under this automotive program. *See* Telephone Interview with Heyman Matlock, Administrator, Free Venture Program, (Jan. 30, 1998) (notes on file with author).

agents at the Ventura Youth Correctional Facility in California.[210] They key into the computer the name, address, phone number, credit card number, and dates of travel of callers.[211]

In its twelve years of existence, the CYA received one reported incident of prisoner abuse. Upon release from the youth facility in 1991, a former prisoner who worked as a TWA reservations agent used a customer's credit card number to charge more than $4400 in women's lingerie and $9000 in computers.[212] Police also found that the juvenile possessed credit card numbers of more than sixty other customers.[213]

However, numerous safeguards are in place to prevent juvenile prisoners from misusing personal information.[214] For example, TWA and the CYA have implemented several security measures in their joint program to use juvenile prisoners. First, CYA screens applicants to ensure that they have no record of fraud, embezzlement, check cashing, or computer hacking.[215] Furthermore, TWA employees supervise all juvenile prisoners while they work.[216] In addition, the facility can only receive incoming calls, which are monitored.[217] After they enter flight arrangements, the information is immediately deleted from the screen and the confirmed reservation is sent to corporate offices in St. Louis, Missouri.[218] Prison authorities also strip search the juveniles before and after they enter the work facility and living quarters.[219] Lastly, they are not permitted to have any writing materials[220] and must be forthright if a caller asks if the reservationist is a prisoner.[221]

---

[210] *See* Parenti, *supra* note 54, at 11; Telephone Interview with Heyman Matlock, *supra* note 209 (explaining details of airline reservation agents' program).

[211] *See* CALIFORNIA DEPARTMENT OF YOUTH AUTHORITY, *supra* note 11 (describing daily tasks as airline reservations agent). Juvenile prisoners handle more than one million overflow calls every year. *See id.* The project can accommodate up to 70 juvenile prisoners full-time and 24 part-time. *See id.* Currently, 44 juvenile prisoners work as TWA airline reservationists and receive $5.33 an hour. *See id.*

[212] *See Prime Time Live*, *supra* note 1 (interviewing TWA passenger whose credit card number was misused by former CYA prisoner).

[213] *See id.*

[214] *See* Telephone Interview with Heyman Matlock, *supra* note 209 (discussing safeguards to deter potential abuse by juvenile prisoners).

[215] *See id.*

[216] *See id.*

[217] *See id.* (noting that supervisors cannot monitor TWA employees in private sector offices because union regulations prohibit such practice).

[218] *See id.*

[219] *See id.*

[220] *See id.*

[221] *See id.*

Such security measures, the CYA contends, adequately protect against prisoner misuse of personal information. Moreover, CYA officials argue that one security breach in twelve years is far less than the abuse found in the private sector.[222] Furthermore, the Free Venture Program with TWA has contributed an average of $170,000 to the state's general fund over the past three years in taxes on wages, reimbursement for room and board, and victim restitution contributions.[223]

The California law, which requires juvenile prisoners to disclose that they are prisoners if asked, does not eliminate the TWA youth reservations program.[224] Although the CYA has received only one reported incident of prisoner abuse with a customer's credit card number in the TWA program,[225] the potential for abuse is still present. While security measures have improved, such as deleting credit card numbers, addresses, and phone numbers immediately after the transaction, particularly adept juvenile prisoners may still memorize such personal information.[226] Moreover, requiring them to disclose to callers that prisoners are handling their flight reservations only if asked is an unrealistic safeguard. Absent widespread publicity of these prison work programs, few callers are apt to think that reservationists are convicted criminals and, thus, are unlikely to ask reservationists if they are prisoners. Therefore, consumers may inadvertently and unknowingly disclose unrelated personal information to potential abusers.

C. Industry Standards

Data privacy protection is also lacking in the American business community, which has avoided the imposition of legal rules for almost twenty years through a lobbying effort demanding self-regulation.[227] The direct marketing industry, which includes companies such as Metromail,[228] is virtually self-regulating on privacy

---

[222] *See id.*

[223] *See* A.B. 2649 ANALYSIS, *supra* note 207.

[224] *See id.*; Cal. Proposition 139, *supra* note 205, at 65 (establishing joint venture between government and nonprofit or for-profit entity for purpose of employing prisoner labor).

[225] *See* A.B. 2649 ANALYSIS, *supra* note 207 and accompanying text (describing incident of prisoner misuse of personal information from TWA work program).

[226] *See* Reidenberg, *supra* note 14, at 518 (enumerating various safeguards against misuse of personal information in TWA work program).

[227] *See id.* at 498-99 (discussing lack of fair information practices in United States).

[228] *See* Bernstein, *supra* note 8, at A1 (noting that Metromail maintains "Behaviorbank"

issues.[229] No privacy law, in fact, specifically targets the direct marketing industry.

The direct marketing industry, which has grown tremendously in the United States,[230] operates without any public accountability.[231] For example, companies can adopt informal industry codes of conduct for the treatment of personal information. These, however, are voluntary benchmarks which lack enforcement provisions.[232] Similarly, company policies which express a commitment to consumer privacy in brochures or annual reports have no legal force or effect.[233] Consumers do not have the ability to know when, why, how, and to what extent these companies are using their personal information.[234] Even assuming, arguendo, that individuals are aware of company practices, they lack the bargaining power to contract for privacy protections with businesses.[235] In some cases, political pressure from consumer advocacy groups, public opinion polls, academia, government, and the media can encourage businesses to handle personal information with

---

that sells names, addresses, and personal characteristics of consumers for between 4 and 25 cents to other direct marketers, financial institutions, manufacturers of goods, governmental entities, reporters, politicians, magazines, and newspapers).

[229] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 309 (discussing policy and practices of direct marketing industry). The telecommunications, financial services, and entertainment fields have addressed privacy issues in their direct marketing campaigns. *See* Reidenberg, *supra* note 14, at 518.

[230] *See* Bernstein, *supra* note 8, at A1 (noting that direct marketing sales were $630 billion in 1990).

[231] *See id.* (quoting spokesperson for Direct Marketing Association as saying that unrestricted marketing of personal information is beneficial to economy); Ericson, *supra* note 17 (stating that Direct Marketing Association has no policy regarding what kind of personnel should process data).

[232] *See* Reidenberg, *supra* note 14, at 510 (noting that industry codes are weak); *see, e.g.*, DIRECT MARKETING ASS'N, GUIDELINES FOR PERSONAL INFORMATION PROTECTION (1994) [hereinafter GUIDELINES] (listing guidelines for industry).

[233] *See* Reidenberg, *supra* note 14, at 511 (noting that corporate policies are voluntary and not legally binding). To promote a sound business reputation and goodwill, companies like Equifax and Dun & Bradstreet have declared commitments to privacy in their annual reports. *See* DUN & BRADSTREET CORP., ANNUAL REPORT TO STOCKHOLDERS 22 (1993) (acknowledging privacy concerns); EQUIFAX INC., ANNUAL REPORT TO STOCKHOLDERS (1992) (expressing commitment to privacy). Similarly, American Express has included an annual privacy notice to cardholders. *See* Reidenberg, *supra* note 14, at 511 n.66 (noting that wording of notice is found in assurance made by American Express to the Bureau of Consumer Frauds and Protection of New York Attorney General's Office).

[234] *See* Reidenberg, *supra* note 14, at 533 (noting that consumers are ignorant about the treatment of their personal information absent notice, consent, and access requirements).

[235] *See id.* at 510 (indicating that individual's protection of personal information is merely incidental to contract between corporation and client).

fairness.[236]

The industry generally uses personal information for two purposes: (1) constructing profiles of individuals by assembling their personal characteristics and habits, and (2) commercializing the profiles by selling their information to other marketers.[237] Notably, the Direct Marketing Association ("DMA"), the industry trade association for direct marketers, has developed a code of conduct[238] and created a Privacy Task Force[239] to advocate the adoption of voluntary, self-regulatory standards within the sector.

Despite these two hallmarks, the industry's policies and enforcement thereof are weak for a number of reasons. First, the DMA's definition of "personal information" does not include data in public records or observable data, which refers to physical characteristics such as race.[240] Second, the DMA Guidelines specify that direct marketers should collect personal data lawfully and only for direct marketing purposes.[241] However, the DMA opposes restrictions on the secondary use of personal information and loosely permits direct marketers to disclose personal information to each other.[242] Some direct marketers claim that consumers who volunteer information are not forbidding secondary use; however, such surveys usually do not state the intended uses of personal information nor do they offer an opt-out provision.[243] Finally, the industry lacks safeguards for especially sensitive data such as health conditions and sexual preferences.[244]

Less than twenty-five percent of the industry complies with these

---

[236] *See id.* at 511 (arguing that public pressure may influence business practices).

[237] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 311.

[238] *See* GUIDELINES, *supra* note 232 (defining obligations and responsibilities of direct marketers to public).

[239] *See* DIRECT MARKETING ASS'N, FAIR INFORMATION PRACTICES MANUAL (1994) (establishing committee to study privacy concerns).

[240] *See* GUIDELINES, *supra* note 232, at 2.

[241] *See id.* (requiring collection of information for specific marketing purpose); SCHWARTZ & REIDENBERG, *supra* note 67, at 309 (pointing out that direct marketing industry ignores its own guidelines); *see also* Plaintiff's Fifth Amended Class Action Petition at 32, Dennis v. Metromail (Tex. Dist. Ct., Jan. 19, 1998) (No. 9604451) (on file with author) (alleging that Metromail violated industry standards despite DMA Guidelines which state that "[e]ach direct marketer should be responsible for the security of personal data. Strict measure should be taken to assure against unauthorized access, attention, or dissemination of personal data.").

[242] *See* GUIDELINES, *supra* note 232 (listing various positions of industry on treatment of personal information); *see also* SCHWARTZ & REIDENBERG, *supra* note 67, at 321 (stating that DMA criticizes limitations on secondary use of personal information).

[243] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 323.

[244] *See id.* at 335.

self-regulation policies.[245] These guidelines are meaningless because businesses have an abundance of personal information and do not hesitate to use it for marketing purposes.[246] The direct marketing industry has so much personal information about individuals that even the FBI approached the industry to obtain certain data.[247]

Standards for the treatment of personal information are, however, slowly evolving due to two phenomena. First, the American public has little confidence in the way the private industry treats personal information.[248] Second, companies realize that they will suffer from this lagging confidence if they do not change their data processing practices, or at least alert consumers of them.[249] Their long-term survival depends on consumer satisfaction with the way they conduct business and use personal information.

III. PROPOSED SOLUTION

A. The European Directive

Unlike U.S. privacy laws, their European counterparts are comprehensive in both coverage and scope.[250] They can serve as a model of data privacy legislation that the United States should follow. For sixteen years, the European Parliament, the European Union's legislative body,[251] has demanded regulation restricting the processing of personal data by government and business.[252] Four

---

[245] *See* LOUIS HARRIS & ASSOCS. & WESTIN, *supra* note 18, at 98-103 (discussing attitude of industry toward protecting personal information).

[246] *See* Reidenberg, *supra* note 14, at 520 n.122 (citing typical response from companies when faced with request for access to profile information as "it's proprietary" or "we won't tell you").

[247] *See* Ray Schultz, *FBI Said to Seek Compiled Lists for Use in Its Field Investigations*, DM NEWS, Apr. 20, 1992, at 1. However, the industry did not provide the FBI with any information. *See* Ray Schultz, *Big Compilers Say No to the FBI*, DM NEWS, May 4, 1992, at 1.

[248] *See New Public Views on Business and Privacy . . . Whom Do They Trust?*, 1 PRIVACY & AM. BUS. no. 3, at 1-2 (1994) (finding that 40% of Americans think business poses greater threat to privacy than government).

[249] *See* Reidenberg, *supra* note 14, at 511.

[250] *See generally* Symposium, *Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 IOWA L. REV. 431 (1995) (analyzing European Directive and commenting on free flow of data and privacy protection).

[251] *See* Fred H. Cate, *The EU Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 432 n.14. The body consists of 518 members elected by party, not country. *See id.*

[252] *See* Spiros Simitis, *Foreword* to PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW at v (1996) (providing background information on European Directive's history).

years after the European Commission first proposed a draft, the European Union enacted the "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" ("European Directive") in October 1995.[253]

The European Directive obligates the sixteen member states of the European Union to revise existing laws or enact new laws embodying the principles enunciated in the European Directive.[254] Signatory countries to the European Directive must adopt the necessary provisions within three years of the Directive's enactment.[255]

The European Directive has three important objectives: (1) to ensure the right of privacy of individuals in an information-oriented society, (2) to promote the free flow of personal information within the European Union by virtue of a uniform legal scheme protecting such information, and (3) to deter the misuse of personal information by third countries with insufficient data protection.[256] In essence, the European Directive harmonizes the privacy protections of individual member states.

Four main principles govern comprehensive data protection under the European Directive.[257] The first is the creation of fair information practices that define the obligations and responsibilities of the data processor.[258] The European Directive requires that a specific purpose must accompany the commercialization of personal information. It further prohibits the secondary use of per-

---

[253] *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter European Directive] (providing rights of privacy to individuals, promoting free circulation of personal data, and preventing abuse of personal data).

[254] *See id.* arts. 4(1), 27. For example, France, Germany, Sweden, and the United Kingdom must amend their respective national privacy laws to conform to the principles of the European Directive while Italy and Greece must adopt new national regulations for the first time. *See* Simitis, *supra* note 252, at v.

[255] *See id.* art. 32(1) (imposing deadline on states to adopt new regulations of directive).

[256] *See id.* arts. 1(1)(2), 25, 26. Moreover, the European Directive requires its signatories to prevent the transfer of personal information to third countries determined to have inadequate protections for the privacy of personal information. *See id.* art. 25(4). The Directive permits the transfer of personal information if the receiving country has "adequate" privacy regulation. *See id.* art. 25(1), (2). The Directive lists exceptions to the rule of adequacy for everyday business transactions. *See id.* art. 26(1)(a)-(f), (2). The European Union's duty to protect personal information goes beyond its borders. *See* Simitis, *supra* note 252, at vi.

[257] *See generally* European Directive, *supra* note 253, arts. 5-21 (structuring treatment of personal information around four main principles).

[258] *See id.* art. 6(1)(b) (stating that member states shall collect personal data for "specified, explicit, and legitimate" purposes and not for incompatible purposes).

sonal information.[259] Such fair information practices would also restrict the collection of unnecessary data[260] and impose time limits on the storage of personal information beyond a specified period.[261] The European Directive mandates that consumers have access to their personal information and the right to correct inaccuracies.[262] It also regulates the security of information to guard against its unauthorized alteration or destruction.[263] Thus, the European Directive obligates member states to "provide that processing of personal data is lawful" only if carried out in accordance with the aforementioned rules.[264]

The second European principle is transparency in the processing of personal information.[265] This element requires data processing to be open and accessible because "secret" processing infringes upon an individual's civic participation in political and social life.[266] The European consensus is that individuals must be able to understand how others treat their personal information in order to participate actively and effectively in society. Because a person is entitled, on request, to know of the existence of a processing operation,[267] the European Directive requires notice to individuals of the collection of personal information, consent for certain kinds of processing, and whether third party disclosures are planned.[268]

The third principle in the European Directive affords special protections to particularly sensitive data.[269] Processing such highly personal information, including that concerning health, race, and religion, is subject to greater protection.[270] However, the European Directive exempts processing of highly personal information for

---

[259] *See id.*

[260] *See id.* art. 6(1)(c) (prohibiting collection of inadequate, irrelevant, and excessive information).

[261] *See id.* art. 6(1)(e) (requiring expiration for collection of data and safeguards for historical, scientific, and statistical personal information which may require extended storage).

[262] *See id.* arts. 6(1)(d), 12 (requiring accurate and complete information on data subject and providing data subject's right of access to information).

[263] *See id.* art. 17 (providing against unlawful or accidental destruction or loss of personal information).

[264] *See id.* art. 5.

[265] *See id.* arts. 7(a), 11(1) (requiring consent of individual for entity to process personal data).

[266] *See id.*

[267] *See id.* art. 10.

[268] *See id.* arts. 11, 12.

[269] *See id.* art. 8 (applying extra protection to special categories of data processing).

[270] *See id.*

certain statistical, historical, scientific, national security, journalistic, literary, or artistic purposes.[271]

The final principle embodied in the European Directive involves the enforcement of the Directive's mandate and continuing oversight of the treatment of personal information.[272] It requires oversight through the "controller," a central registry or public supervising authority who oversees such uses as the commercialization of consumer lists and global information transfers.[273] Independent monitoring of data processing is also necessary to provide expertise to government, business, and citizens during the Information Age.[274] Additionally, a data protection commission offers research and development regarding information transfers.[275] Furthermore, the European Directive advocates the creation of an independent body to serve as a forum for debate regarding the use of data processing activities.[276]

In contrast to the narrowly tailored American laws aimed at specific industries, many European countries already had comprehensive omnibus laws to regulate the use of personal information even before the enactment of the European Directive.[277] As a result, European laws tend to place greater emphasis on privacy. While U.S. data protection laws generally focus on trade secrets, European countries use the term "data protection" in the context of legal rules governing the collection and use of personal information.[278] Another stark difference between European and American law is the role of the state. U.S. privacy laws aim to prevent unreasonable government intrusion. However, because European countries generally require the state to take a more active role in protecting personal information,[279] European data privacy laws apply

---

[271] *See id.* arts. 8, 9 (listing exemptions from special protections).

[272] *See id.* arts. 28-30 (requiring supervising authority over those who monitor and process personal information).

[273] *See id.* art. 28 (enumerating responsibilities of supervising official).

[274] *See* Schwartz, *supra* note 44, at 565.

[275] *See id.*

[276] *See id.*

[277] *See* Reidenberg, *supra* note 42, at 199-200, n.15, 236, nn.232-38 and accompanying text (citing examples of privacy protection laws of individual European countries).

[278] *See* European Directive, *supra* note 253, arts. 3-21 (listing rights of individuals and responsibilities of data processor).

[279] Austria, Belgium, Denmark, France, Germany, Ireland, Luxembourg, the Netherlands, Spain, Sweden, and the United Kingdom have such laws. *See* Reidenberg, *supra* note 42, at 238 nn.234-35.

equally to both the public and private sectors.[280]

The United States lacks omnibus data protection laws and comprehensive industry-specific data protection laws because of the historical development of our legal system. The ad hoc nature and emphasis on minimal government regulation involving the flow of information in the private sector stems from a historical focus on restraining the state. In order to minimize government intrusion, the United States regulates fair information practices through discrete and industry specific regulations.[281] American political philosophy essentially reflects a hostility toward government regulation of private conduct while Europeans view government more as a protector.

Federalism is another reason for the lack of omnibus data protection in the United States. Laws establishing fair information practices for the protection of personal information come from several different sources, including the U.S. Constitution, state constitutions, federal and state statutes, and the common law of state courts. Self-regulation in the private sector also contributes to the patchwork of American data protection laws. Furthermore, unlike the European Directive, which embodies core principles of data processing for its member states, a common set of accepted standards for the treatment of personal information is not contained in any single source in the United States.[282] Although the U.S. Department of Health and Welfare promulgated one of the first sets of guidelines for the treatment of personal information,[283] they are only voluntary. Thus, the American desire for minimal regulation is a cause of inadequate data protection.

B. The Prohibition on Prisoner Processing of Personal Information Act of 1999

Because the piecemeal approach to data privacy rights at the federal and state levels in the United States offers little protection to individuals, we should look to the European Directive as a model for comprehensive data privacy protection. There is some

---

[280] *See* European Directive, *supra* note 253, preamble §§ 5, 12, art. 3 (discussing scope of European Directive as applying to processing of personal data within European community).

[281] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 512.

[282] *See id.*

[283] *See* Reidenberg, *supra* note 14, at 512.

consensus in the United States on commonly accepted standards for data privacy in the private sector,[284] although businesses have not necessarily implemented them.[285] This consensus and the principles of the European Directive form the basis for this Comment's proposed federal statute, entitled the Prohibition on Prisoner Processing of Personal Information Act of 1999, found in the Appendix.

The proposed federal statute generally prohibits prisoners from possessing, accessing, and processing personal information. However, it allows states that meet certain requirements to employ prisoners.[286] The statute has several attributes. First, it balances an individual's right to privacy, private industry's need to process information for commercial gain, government's right to process information for administrative reasons, and the benefits that prisoners receive from such work programs.[287] For example, individuals will receive notice of the use of prison labor.[288] The proposed statute also restricts the permissible purposes for collecting information, limits its storage time, and grants individuals access for the purposes of correcting misinformation.[289]

Second, the proposed statute preserves the concepts of liberty and identity in American democracy by allowing states to elect to use prison labor to process personal information.[290] While the statute borrows many concepts from the European Directive, Europe's wholesale approach would not work in the United States. Unlike Americans, Europeans have historically been more willing to regu-

---

[284] *See id.* at 511-12 (discussing common benchmark standards such as lawful collection of data for specific purpose and determination of use of data prior to collection). The U.S. government also supported similar voluntary guidelines adopted some years later by the Organization for Economic Cooperation and Development ("OECD"). *See* Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. (C. 58 final) (Oct. 1, 1980). Likewise, many American companies expressed a commitment to these OECD principles. *See* Reidenberg, *supra* note 14, at 512 n.70 (citing list of companies who support privacy principles).

[285] *See* DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306 (1989) (arguing that federal statutory protection against government surveillance is inadequate).

[286] *See* APPENDIX: PROPOSED FEDERAL STATUTE: PROHIBITION ON PRISONER PROCESSING OF PERSONAL INFORMATION ACT OF 1999, §§ 3, 4 (a)(1)-(a)(7), 4(b)(1)-(b)(5), 4(c) (Sandra T.M. Chong 1999) [hereinafter PROPOSED FEDERAL STATUTE].

[287] *See id.* §§ 4 (a)(1)-(a)(7), 4(b)(1)-(b)(5), 4(c), 4(d), 5(a)-(d).

[288] *See id.* § 4(b)(1).

[289] *See id.* § 4(b)(2)-(b)(5). Additionally, private businesses can still enter into partnerships with states that choose to use prison labor, subject to certain restrictions, and still receive financial benefits. *See id.* § 4 (a)(1)-(a)(7). Also, specified prisoners can be paid while receiving work training and learning valuable skills. *See id.* §§ 1(c), 4(a)(1).

[290] *See id.* §§ 3-4.

late commercial activities; several European countries have even adopted comprehensive legislation on data processing by private businesses.[291] Americans do not view government regulation with as much benevolence as their European counterparts, and this statute reflects such sentiment.[292] Finally, the proposed statute allows individuals to pursue a cause of action and receive damages or an injunction for unfair information practices based on dignitary and social violations of the right to be let alone.[293]

The proposed federal statute is necessary and improves upon existing approaches in the United States, Texas, and California for several reasons. First, there is currently no federal law that specifically regulates the use of prisoners to process personal information or that otherwise addresses the privacy concerns of third parties.[294] Yet Congress has the capability to pass comprehensive federal legislation and the authority to regulate the use of prison labor under both the Interstate Commerce Clause[295] and the congressional remedial and preventative power to reach private action under Section five of the Fourteenth Amendment.[296] The proposed statute addresses the current gaps of industry-specific data privacy protections. Because the flow of personal information is not particular to state or national boundaries, it is appropriate and even necessary to adopt new legislation at the federal level.[297]

Second, this is an emergency public safety measure.[298] Most people would be surprised to learn that prisoners have access to some of their most private and confidential information and would want

---

[291] *See* Reidenberg, *supra* note 42, at 198 n.15, 20 n.23 (discussing widespread acceptance of privacy rights applicable to private sector's information processing in European countries).

[292] *See* Reidenberg, *supra* note 14, at 500-07 (arguing that American philosophy of limited government and conception of "marketplace of ideas" permits minimum restrictions on data flows).

[293] *See* PROPOSED FEDERAL STATUTE, *supra* note 286, § 5(a)-(d).

[294] *But see* Children's Privacy Protection and Parental Empowerment Act, H.R. 3508 and S. 1908, 104th Cong. (1996).

[295] *See* U.S. CONST. art. I, § 8 (giving Congress power "to regulate foreign Nations, and among the several States, and with the Indian Tribes"); *see also* PROPOSED FEDERAL STATUTE, *supra* note 286, § 1(b). Data processing deals with commercial activities; the data entry work stems from consumer surveys and questionnaires from the direct marketing industry.

[296] U.S. CONST. amend XIV, § 5 (stating that "Congress shall have power to enforce, by appropriate legislation, the provisions of this article"); *see, e.g.*, Katzenbach v. Morgan, 384 U.S. 641, 646-47 (1966) (suggesting that congressional power could be "substantive," not merely remedial, under § 5 of 14th Amendment in finding that New York literacy test for Puerto Ricans violated Voting Rights Act of 1965).

[297] *See* Reidenberg, *supra* note 42, at 238-39.

[298] *See* PROPOSED FEDERAL STATUTE, *supra* note 286, § 1(a).

to take immediate action to prohibit or restrict the practice.[299] The *Dennis* case illustrates the potential for prisoner abuse of personal information. Even if states were to pass legislation banning prison labor for data entry, uniformity among states would likely be lacking. Additionally, individual state legislatures may be slow in acting for political and administrative reasons.

Third, the proposed statute presumes that prisoner access, use, disclosure, and possession of personal information is potentially dangerous[300] and, thus, imposes a burden on the state to explain why the benefits of using prisoners to process personal information outweigh the risks.[301] Because private businesses lack incentives to police themselves, Congress must act.[302]

Critics from the privacy advocates camp may denounce this proposed statute as not going far enough in restricting the use of prison labor to process personal information. They would likely argue that an outright ban of the practice is the only effective solution to prisoner abuse because safeguards are not foolproof.[303] While a complete prohibition on the use of prison labor for data entry would be ideal, the solution is too simplistic and, frankly, unrealistic given the significant financial savings government and private businesses realize,[304] the constructive use of otherwise idle prisoners, and the potential infringement on the rights of states to regulate their own prison population.[305]

---

[299] *See* Bernstein, *supra* note 8, at A1 (explaining consumer outrage upon learning of use of prison labor to process personal information).

[300] *See* PROPOSED FEDERAL STATUTE, *supra* note 286, § 1(a).

[301] *See id.* §§ 4(a)(1)-(a)(7), 4(b)(1)-(b)(5).

[302] *See supra* notes 227-249 and accompanying text (explaining minimal industry standards on how personal information should be handled in private sector).

[303] *See supra* notes 70-76 (outlining position of privacy advocates on use of prisoners to process personal information).

[304] *See supra* notes 50-65 (outlining arguments in favor of using prisoners as resource). Private industry may criticize the statute for going too far. The business sector might be worried that constraints on the use of prisoners to process personal information will impose additional costs and impede the partnership with state prisons. *See* Reidenberg, *supra* note 42, at 239 (acknowledging legitimate concerns of private industry in establishing new framework for fair information practices). The statute presumes that these constraints are simply a cost of business. *See* PROPOSED FEDERAL STATUTE, *supra* note 286, §§ 4(a)(1)-(a)(7), 4(b)(1)-(b)(5).

[305] *See supra* notes 50-65 and accompanying text (discussing benefits to prison labor). Companies have used prison labor to end or avoid strikes. In fact, TWA established a reservations operation in the Ventura Youth Facility during a strike by TWA's unionized flight attendants in the mid-1980s. *See* Cary Spivak, *Behind Bars, a New Frontier for Wisconsin Business: Inmate Labor Sparks Interest, and Some Fierce Controversy in State*, MILWAUKEE J. SENTINEL, June 22, 1997, at 1. With juvenile prisoners acting as reservationists, ticket agents were transferred to flight attendant positions. *See* Parenti, *supra* note 54, at 11. The assistant

In contrast, critics from the prison industry may point out that the proposed statute is premature in light of the isolated incidents of abuse. They may also claim that it is unworkable because it requires states to fulfill numerous and tedious conditions before using prison labor to perform data entry work.[306] Yet the statute merely creates a rebuttable presumption that prisoners who possess, have access to, or process personal information in prison work programs have the potential for abuse.[307] However, most of the states that already allow prisoners to process personal information need only improve, albeit significantly, existing safeguards.[308] The states that do not currently permit the use of prison labor for data processing, on the other hand, will have to satisfy this burden should they change their policy. Such a requirement seems to be a low price to pay given the risks involved.

The proposed statute provides a minimum floor of federal protection for individuals as a supplement to existing state protections.[309] States can still enact their own omnibus protections for fair information practices that establish more stringent requirements.[310] In fact, the proposed federal statute encourages states to enact their own laws that govern the particular circumstances of their prison population, citizenry, and private industry.

CONCLUSION

Few disagree that privacy data deserves protection from unwarranted intrusions.[311] The more difficult issue is how to balance the

---

research director for the California Labor Federation believes that TWA's hiring of juvenile prisoners gave the airline flexibility to replace the flight attendants on strike, and that the state essentially subsidized the strike-breaking effort by permitting the use of prison labor. *See id.* Thus, unions and small businesses oppose the use of prison labor to process information because of unfair competition and job displacement. *See id.* Under the proposed federal statute, states have the option to use prisoners or regular employees. *See* PROPOSED FEDERAL STATUTE, *supra* note 286, §§ 4 (a)(1)-(a)(7), 4(b)(1)-(b)(5), 4(c).

[306] *See* PROPOSED FEDERAL STATUTE, *supra* note 286, §§ 4 (a)(1)-(a)(7), 4(b)(1)-(b)(5), 4(c).

[307] *See id.* § 1(a).

[308] *See* Bernstein, *supra* note 8, at A1 (discussing other states which use prisoners to process personal information for private and public entities); Saul, *supra* note 10, at A35.

[309] *See* Reidenberg, *supra* note 42, at 238-39 (noting that it is appropriate to adopt legislation at federal level because transmittal of personal information is not confined to state or national borders and uniformity of law avoids chaos of 50 different state privacy regulations).

[310] *See* SCHWARTZ & REIDENBERG, *supra* note 67, at 150-51 (arguing in favor of comprehensive state data protections).

[311] *See Hearings*, supra note 43 (statement of Senator Steve Peace) (stating "privacy

individual's right to be let alone with private industry's right to solicit such information in the market, government's need to collect such information for legitimate purposes, and society's need to facilitate commerce and efficiency. Yet businesses must be held accountable for the collection, storage, processing, and dissemination of personal information that harms individuals. Accountability should also extend to state and federal governments that allow prisoners to process personal information.[312]

Congress needs to address the problems of data privacy associated with prison labor before the potential abuses become more rampant. The proposed statute allocates the accountability for misuse of personal information and provides safeguards to prevent the kind of abuse that confronted Beverly Dennis. Specifically, the statute protects individuals against unwarranted intrusions of data privacy,[313] gives states the option of allowing prisoners to process personal information subject to certain constraints, and allows private businesses to use this resource in a safe, efficient, and responsible manner. Finally, the statute provides individuals with a much deserved remedy for the misuse of their personal information. As Hal Parfait, Metromail, and the Texas prison industry would surely realize, under the proposed statute, Beverly Dennis's life is no longer for sale for twenty-five cents.

Sandra T.M. Chong

---

rights is the great civil rights turn of the century").

[312] *See generally* PROPOSED FEDERAL STATUTE, *supra* note 286 (providing individuals with minimum level of protection against privacy violations from use of prisoners to process personal information).

[313] *See Prime Time Live, supra* note 1 and accompanying text (summarizing Parfait's view of Texas's work program).

APPENDIX

PROPOSED FEDERAL STATUTE: PROHIBITION ON PRISONER PROCESSING OF PERSONAL INFORMATION ACT OF 1999

§ 1. Declaration of legislative findings and legislative intent

(a) The practice of using prisoners to process information for public and private entities infringes upon the fundamental rights of individuals, threatening their right to privacy and placing them in danger of their lives or safety.

(b) This Act is not intended to restrict the free flow of information between or among states. It is intended to ensure the fair and safe treatment of personal information.

(c) Notwithstanding (a) and (b), this Act recognizes that prisoners may obtain important job skills and provide valuable services to public and private entities through processing information.

§ 2. Definitions

For the purpose of this Act, the following definitions apply:

(a) "Personal information" shall refer to any information about an identified or identifiable natural person by reference to one or more factors relating to his or her physical, physiological, financial, mental, social, economic, racial, ethnic, or cultural identity. Personal information consists of any facts, preferences, communications, or opinions that an individual would reasonably regard as private, confidential, or sensitive and, therefore, would want to prohibit or restrict from use or dissemination. Personal information includes, but is not limited to, a person's name, home telephone number, address, age, address and place of employment, marital status, spouse's name, children's names and ages, social security number, driver's license number, credit card numbers, bank account numbers, tax records, and medical records.

(b) "Processing of personal information" shall mean any operation(s) performed upon personal information, including but not limited to collection, recording, organization, storage, adaptation, alteration, destruction, retrieval, consultation, use, transmission, and disclosure.

(c) "Controller" shall refer to the prison administrator, the

director of the correctional facility, the supervisor of the prison work program, or any authorized correctional officer.

(d) "Data collector" shall refer to the entity who employs prisoners to process data.

§ 3. Ban on prison labor involving personal information

No prisoner or incarcerated juvenile or adult in any county, state or federal prison, jail, or other correctional facility shall possess, access, or process personal information for private or public use.

§ 4. Exceptions

Notwithstanding the provisions of § 3, states may allow prisoners to process personal information if all of the following conditions are met.

(a) Screening and Oversight of Prisoners

(1) Prisoners selected to process information must never have been convicted of, or adjudicated to have committed, a dangerous, violent, or sexual-related felony or sexual-related misdemeanor as defined in each state's respective penal code. Prisoners selected must never have been convicted of, or adjudicated to have committed, fraud, forgery, embezzlement, crimes involving a computer, counterfeiting, or crimes involving the misuse of personal information.

(2) The controller must still screen nonfelony prisoners. The controller must certify in writing that the prisoners selected to process information have no prior history of violence nor show any propensity to commit violence while serving their sentences.

(3) The controller must strip search the prisoners every time they enter and leave the data processing facility and living quarters.

(4) The controller must closely supervise and monitor prisoners processing personal information at all times.

(i) Safeguards include, but are not limited to, random monitoring of phone calls and work stations.

(ii) The controller shall ensure that no writing instruments or materials are accessible to prisoners.

(5) The controller must file biannual reports to the Federal Bureau of Prisons outlining the prison work program, indicating the number of participants, describing the data processing activity involved, the controls implemented to prevent potential abuse of information, and corrective actions taken against prisoners in regard to abuse of information.

(6) Each state's work program is subject to random unannounced visits or inspections of the prison work program to ensure compliance with federal law.

(7) A victims' fund shall be established to compensate individuals injured by prisoner misuse of personal information. Prisoners shall contribute no more than twenty percent of their earnings.

(b) Consumer Protections

(1) Individuals must be given reasonable prior notice that prisoners will be handling their personal information. Individuals must give written consent to allow prisoner processing of personal information for the stated intended purpose of its collection.

(2) Personal information can only be collected lawfully for a specific purpose. The data collector must determine the use(s) of each piece of personal information prior to its collection and shall acquire such information only through lawful means. Such information collected for a specific use necessarily prohibits secondary or other use of information unless otherwise mandated by law.

(3) Personal information must be relevant for the intended lawful purpose of the collection of data. Extraneous or excessive information is prohibited, unless it can be shown that the information was reasonably necessary for the purpose of collection.

(4) Personal information collected must not be stored for any period of time longer than necessary to accomplish the purpose of collection.

(5) Personal information must be accurate. Individuals must have reasonable access to their personal information and the ability to correct inaccurate data. Security measures should be in place to guard against the unauthorized destruction or alteration of personal information.

(c) Special Protections for Sensitive Data

Prisoners shall not possess, access, process, disclose, or use personal information relating to particularly sensitive facts, including but not limited to racial or ethnic origin, political opinion, religion, occupation, income, credit worthiness, health, sexual practices, security, or criminal activity.

(d) Penalties

Any prisoner who possesses, accesses, processes, discloses, or

uses personal information while confined in a correctional facility, with the intent to obtain a benefit or harm another person shall be prohibited from participating in any subsequent work program which provides access to personal information. A prisoner who violates this section is also subject to a forfeit of all or part of his work time credit.

§ 5. Enforcement of fair information practices

(a) An individual has a private cause of action against the controller, data collector, and prisoner for violation of data privacy.

(b) An individual may recover compensatory and punitive damages.

(c) An individual is entitled to a trial by jury where the value of the controversy exceeds twenty dollars.

(d) An individual or the Federal Bureau of Prisons may obtain an injunction against any work program that fails to comply with the terms of this Act.