NOTE
PERSONAL DATA SPEECH: TOWARD A NEW COMMERCIAL SPEECH
DOCTRINE FOR DATA PRIVACY REGULATIONS

David H. Chan

I. Introduction

“[T]he Internet [contains] ‘the largest information database’ in the world. You
may find it hard to imagine, the vast resources we have made available to you, to dig up
information on anybody . . . in a 100% legal and efficient way . . . . You will be surprised
as to the information available on anybody including yourself.”

--advertisement from socialsecurity-numbersearch.com

Welcome to the $5 billion-a-year personal data industry, a legal wild-west
frontier where legitimate and illegitimate players collect, aggregate, and exchange large
amounts of personal data without regulation. For example, anyone can click on the
internet ad referenced above and buy a person’s information including social security
number for only $34.95. In recent years, our increased reliance on electronic
transactions has led to an abundance of digitized personal data, greatly fueling the
industry’s growth. These transaction histories are often aggregated with other private and
public sector data to create behavioral profiles, primarily for marketing.

1 Social Security Lookup, http://www.socialsecurity-numbersearch.com/social-security-number-
lookup.htm (last visited February 14, 2006).
3 Jonathan Krim, Pentagon Creating Student Database, WASH. POST., June 23, 20005, at A1.
4 Social Security Lookup, http://www.socialsecurity-numbersearch.com/social-security-number-
lookup.htm (last visited February 14, 2006).
5 A Pew research in 2004 found that 83 million people had shopped online, and overall online sale
was estimated to be $120 billion in 2004. Bob Tedeschi, No Longer a Niche Marketing Outlet, The Internet Is
6 See DANIEL SOLOVE, THE DIGITAL PERSON 22-26 (2004) (DoubleClick, a company that profiles people
online browsing and shopping habits, has already amassed profiles for 80 million U.S. household at the end
of 1999).
7 See id. at 16-20.
In 2005, in the midst of increased identity thefts and data security breaches, Congress began to tackle the lack of oversight in the data industry, and proposed twenty-two bills addressing identify theft. Because there is no comprehensive federal legal framework to address data privacy, these proposed bills aim to shore up holes in a patchwork of federal laws that each addresses a narrow area of data privacy. For example, some federal laws regulate the collection and use of records by federal agencies, while others regulate access to education records, the sale of state Departments of Motor Vehicles data, and privacy in credit reporting.

While it is unclear what privacy legislation Congress will eventually pass, any new legislation that restricts the transfer of data will likely face challenges on First Amendment grounds. In recent years, companies that collect and sell personal data, as well as corporations that use and share their own customers’ data, have fought regulation as a restriction on free speech. Courts have just begun to address this First Amendment defense, and often classify the collection and exchange of personal data as commercial speech. Thus, how the courts apply the commercial speech doctrine to the use and sale of personal data will directly impact whether the government may regulate in this area.

See, e.g., Tom Zeller Jr., *The Scramble to Protect Personal Data*, N.Y. TIMES, June 9, 2005, at C1 (detailing public and congressional reaction to recent breaches at data brokers Choicepoint and LexisNexis).


SOLOVE, *supra* note 6, at 67.

Id.

Privacy Act of 1974. SOLOVE, *supra* note 9, at 67-72, provides this listing in more details.


This argument has been raised, e.g., Trans Union Corp. v. FTC, 245 F.3d 809 (D.C. Cir. 2001). See infra Part III.B for a discussion of the arguments raised in the case.

Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1409 (citing U.S. West, Inc. v. FCC, 182 F.3d 1224, 1232-33 (10th Cir. 1999) and United Reporting Publ’g Corp. v. California Highway Patrol, 146 F.3d 1133, 1136-37 (9th Cir. 1998), *rev'd sub nom. u, 120 S. Ct. 483 (1999)* as examples).
This article will outline this emerging area of the commercial speech doctrine, analyze the courts’ difficulties in applying the doctrine to data privacy laws, and propose a new structural approach to determine the constitutionality of data privacy laws. Part II of this article sets forth the background on privacy issues arising from the use of personal data. Part III outlines two main problems with applying the commercial speech doctrine to data privacy laws. In particular, it discusses the problem of categorizing personal data as commercial speech and the problem of determining the proper level of scrutiny to evaluate the constitutionality of data privacy regulations. In light of these problems, Part IV proposes a new multi-tiered approach to the commercial speech doctrine for personal data speech. The proposed approach eliminates the difficult inquiry of whether personal data is commercial speech. Instead, under the proposed approach, categorical bans of personal data speech will receive strict scrutiny while privacy regulations that aim to address the issue of data control will receive intermediate scrutiny. The proposed approach also includes a separate tier for data privacy legislation that provides for private rights of action.

II. Background

A. Personal Data: The Beginning of a New Portable Commodity

In the 1970s, both corporations and government entities began using computer databases to store records and made data portable for the first time. The transition from paper to electronic records made it feasible for private parties to obtain data,

19 See COMM. ON INNOVATIONS IN COMPUTING AND COMMUNC’NS, NAT’L RESEARCH COUNCIL, FUNDING A REVOLUTION: GOVERNMENT SUPPORT FOR COMPUTING RESEARCH 159-64 (1999) [hereinafter Funding a Revolution].

analyze it, and sell it as a commodity. Indeed, government databases were the seed
data sources for many private commercial databases.\textsuperscript{21}

In the last decade, unprecedented increases in both supply and demand for data
triggered an explosive growth of the personal data industry. On the supply side,
increased internet use led to an explosive growth in the amount of available data.\textsuperscript{22} For
example, one data profiler claims they have information on 90 million U.S. households.\textsuperscript{23}
On the demand side, corporations began utilizing the new data commodity to target
advertisements to selected customers who would be interested in their products and
reaped improved returns on their advertising investments.\textsuperscript{24} The promise of better returns
led to a huge appetite for consumer data, which in turn fed the growth of the “data
mining” or “data profiling” industry, a group of companies that “aggregate information
contained in private databases to create consumer profiles that are then offered for sale to
interested parties.”\textsuperscript{25}

Such profiles often include personal information ranging from information in
public records (e.g. name, social security number, race, gender, and home ownership) to
habitual information (e.g. shopping habits and utility usage) to private and potentially
embarrassing information (e.g. arrest records, lifestyle preferences, hobbies, religion, and
medical information).\textsuperscript{26} Such information is available for as little as $65 per thousand

\textsuperscript{21} Neil M. Richards, \textit{Reconciling Data Privacy and the First Amendment}, 52 UCLA L. REV. 1149, 1156
(2005).
\textsuperscript{22} Bob Tedeschi, \textit{supra} note 5.
\textsuperscript{23} Abacus Alliance Data, http://www.abacusus.com/products\_&\_services/abacus_alliance_data/default.asp
(last visited Nov. 1, 2005).
\textsuperscript{24} SOLOVE, \textit{supra} note 6, at 17.
\textsuperscript{25} Richards, \textit{supra} note 21, at 1157. For purpose of this article, the “profiling industry” is treated as a
segment of the data broker industry.
\textsuperscript{26} Electronic Privacy Information Center, Privacy and Consumer Profiling,
names, categorized by the type of consumer sought by marketers.\(^\text{27}\) For example, the profiling company Focus USA boasts on its web site that it has profiling information on “virtually every household in the country.”\(^\text{28}\) Their product offerings include such creatively named lists such as “In Style Women,” “Born to Shop,” and “Gardening Buffs.”\(^\text{29}\)

B. “The heart of a surveillance system that will turn society into a transparent world.”

Even as far back as 1974, Supreme Court Justice William Douglas, quoting Arthur Miller, noted that the computer has become “the heart of a surveillance system that will turn society into a transparent world.”\(^\text{30}\) In Douglas’ time, George Orwell’s novel \textit{1984} depicted a future where “Big Brother” uses computer databases to track every member of society.\(^\text{31}\) Three decades later, due to the availability of personal data, the fictional and prophetic fears of surveillance, control, and loss of anonymity have become alarmingly real.

For example, a recent GAO survey indicated 52 federal agencies had or planned on having data-mining programs in 2004.\(^\text{32}\) Both the FBI and the Department of Defense have used commercial databases for terrorist surveillance post 9/11.\(^\text{33}\) The military has also tried to contract a marketing firm to create a customized database of teenagers to

\(^{27}\) \textit{Id.}  
\(^{31}\) \textit{SOLVE}, supra note 6, at 31-35.  
\(^{33}\) See Jeffery Rosen, \textit{The Naked Crowd: Balancing Privacy and Security in an Age of Terror}, \textit{ARIZ. L. REV.} 607, 610-611 (2004) (discussing for example the Total Information Awareness system, a data mining operation used to detect terrorist activities).
bolster sagging recruitment efforts.\textsuperscript{34} Besides the concerns of potential improper uses by the government, there is also concern that such commercial databases can be used to process sensitive information and cause potentially embarrassing or highly personal information to float freely from database to database.\textsuperscript{36} For example, public arrest records that are legitimately collected may be passed from one database to another and end up illegitimately denying one’s employment or housing.

The dearth of meaningful legal requirements that such personal data be kept securely\textsuperscript{37} means it can fall into wrong hands that can exploit it for illegal and harmful purposes. For example, consumer profiles can facilitate crimes such as identity theft, stalking, or harassment.\textsuperscript{38} To make matters worse, “uber-databases” can be created, composed of non-sensitive information in such enormous quantities that they contain detailed dossiers of each individual’s entire existence.\textsuperscript{39} While there may be legitimate uses to these personal dossiers, their existence makes governmental and other illegitimate uses more likely and damaging.

Despite these problems, there is currently no federal legislation that regulates the sale of personal data or aggregated profiles. Instead, federal laws cover specific types of personal data in specific contexts.\textsuperscript{40} Some notable legislation include older privacy laws such as Privacy Act of 1974 and the Fair Credit Reporting Act of 1970. Both have data privacy provisions applicable to the present problem.\textsuperscript{41} In recent years, for example, Congress has enacted the Gramm-Leach-Bailey (GLB) Act of 1999 to mandate opt-out

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{34} Jonathan Krim, \textit{Pentagon Creating Student Database}, WASH. POST, June 23, 2005, at A1.
\item\textsuperscript{36} Richards, supra note 21, at 1158.
\item\textsuperscript{37} \textit{Id.}
\item\textsuperscript{38} \textit{Id.}
\item\textsuperscript{39} \textit{Id.}
\item\textsuperscript{40} SOLOVE, \textit{ supra} note 6, at 71.
\item\textsuperscript{41} SOLOVE, \textit{ supra} note 6, at 67-68.
\end{itemize}
\end{footnotesize}
mechanism when corporations share “nonpublic personal information.” Congress also enacted the Fair and Accurate Credit Transactions Act (FACTA) of 2003 to strengthen the Fair Credit Reporting Act’s privacy provisions.

However, viewed in the expansive space where data can be collected and exchanged, these federal laws cover only a small geography of the personal data problem. Furthermore, these laws address privacy in certain contexts but ignore it in others. Thus, critics have described the federal government’s response to privacy issues as haphazard, mosaic and unsatisfactory.

III. The First Amendment Defense and the Commercial Speech Doctrine

Even with their limited coverage, federal data privacy laws have been the subjects of free speech litigation when they have been enforced. In particular, companies argue that the First Amendment protects the free collection, use and exchange of personal data. In the late 1990s, both the Ninth and the Tenth Circuits examined this First Amendment defense for the first time and held that the commercial speech doctrine governs the use and sale of personal data. However, applying the doctrine in its current form to the area of personal data has proven to be problematic. First, owing to varying definitions in the precedents, courts have difficulties categorizing personal data as “speech” and “commercial speech.” Second, the uneven application of the commercial speech doctrine has generated a haphazard, mosaic and unsatisfactory response.

---

44 SLOVE, supra note 6, at 71.
46 Id.
47 See, e.g., US West v. FCC, 182 F.3d 1224 (10th Cir. 1999); Trans Union Corp. v. FTC, 245 F.3d 809 (D.C. Cir. 2001); Mainstream Marketing Services, Inc. v. FTC, 358 F.3d 1228 (10th Cir. 2004).
48 “Congress shall make no law abridging the freedom of speech....” U.S. CONST. amend. I.
49 United Reporting Publishing Corp. v. California Highway Patrol, 146 F.3d 1133 (9th Cir. 1998), rev’d on other grounds, 528 U.S. 32 (1999); U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999).
speech doctrine and intermediate scrutiny has produced inconsistent results in this area of personal data speech. This section will discuss each of these problems in turn.

A. Is Personal Data Commercial Speech?

Since not all “speech” receives the same treatment under the First Amendment, categorization is an integral part of any First Amendment inquiry. Unfortunately, both the terms “commercial” and “speech” are loaded with multiple meanings and ill-defined implications. In adjudicating data privacy litigation courts will need to first determine whether personal data is “speech” in order to decide whether the First Amendment is applicable. If so, courts will need to decide whether such speech is “commercial” to apply the appropriate level of protection. As discussed below, each step of the analysis is wrought with difficulties and uncertainties.

1. Data as “Speech”

At its core, First Amendment “speech” covers expressions in verbal, written or artistic forms. In addition, the Court has held that “speech” include many actions such as political contributions and wearing of communicative clothing. Given the Court’s expansive definition of “speech,” numerous data privacy scholars have conceded that First Amendment “speech” covers personal data, and the early circuit cases involving data privacy have so held. For example, the Tenth Circuit in U.S. West, Inc. v. FCC

52 Id.
53 Id.
54 See Richards, supra note 21, at 1179.
55 U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999); United Reporting Pub'g Corp. v. California Highway Patrol, 146 F.3d 1133 (9th Cir. 1998).
56 182 F.3d 1224 (10th Cir. 1999).
held that because the FCC prohibited phone companies (the speakers) from freely using and sharing their customers’ personal data and phone records with other parties (the audience), it was restricting speech.\(^{57}\)

However, the Tenth Circuit’s reasoning does not go far enough to complete the inquiry. This is because the First Amendment exempts certain “speech” such as obscenities, as well as certain special areas such as those governed by securities law and attorney-client privilege laws.\(^ {58}\) These laws often restrict the use of acquired information for purposes other than the original permissible one.\(^ {59}\) By analogy, one may argue that FCC in the \textit{U.S. West} can restrict phone companies from collecting customers’ phone usage and personal data for one purpose (maintaining their phone services) and use them later for different purposes (e.g. for marketing purposes). The Tenth Circuit’s analysis does not indicate whether any such exemption applies.

On the other hand, some have proposed that personal data be characterized as an article of commerce.\(^ {60}\) This characterization has some support in \textit{Reno v. Condon},\(^ {61}\) a Supreme Court case involving Congress’ exercise of its Commerce Clause power to restrict sale of drivers’ personal data by state Departments of Motor Vehicles. The Court there characterized such personal data as “articles of commerce.”\(^ {62}\) This type of characterization undoubtedly influences the courts toward categorizing personal data as commercial speech.

2. Personal Data as “Commercial” Speech

\(^{57}\) Id. at 1232.
\(^{58}\) Richards, supra note 21 at 1190.
\(^{59}\) Id.
\(^{60}\) Id. at 1195-1200.
\(^{61}\) 528 U.S. 141 (2000).
\(^{62}\) Id. at 148.
Courts also have difficulties justifying the categorization of personal data as commercial speech because of the Court’s own murky definition of commercial speech. This problem can be traced to the origin of the commercial speech doctrine, which arose from cases involving commercial advertising. In 1975, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, the Court first held that commercial speech was within the scope of First Amendment protection. There, the Court struck down a Virginia professional conduct statute that prohibited pharmacists from advertising the price of prescription drugs. The Court reasoned that a communication proposing a sale of a product X at the Y price is within the scope of First Amendment protection because a free enterprise economy depended on numerous private economic decisions, which in turn relied on the free flow of commercial information. The formulation of proposing a sale of product X at the Y price came to known as the “core notion” of commercial speech. Then in 1980, the Court in *Central Hudson Gas & Electric Corp. v. Public Service Commission* broadly defined commercial speech as any “expression related solely to the economic interests of the speaker and its audience.”

In one of the first personal data speech cases, the Ninth Circuit in *United Reporting Publishing Corp. v. California Highway Patrol* held that the sale of names and addresses of recently arrested individuals by a data publishing company constituted

---

64 *Id.* at 749-50.
65 *Id.* at 761.
66 *Id.* at 765.
69 *Central Hudson*, 447 U.S. at 561.
70 146 F.3d 1133 (9th Cir. 1998), rev'd on other grounds, 528 U.S. 32 (1999).
“commercial speech.” The court there acknowledged that “the precise bounds of the category of expression that may be termed commercial speech” are subject to doubt. However, the Ninth Circuit interpreted the lack of precise bounds as the Supreme Court’s giving broad discretion to the lower courts. The Ninth Circuit thus felt it had the discretion to come to its own conclusion.

The court reasoned that the data speech in question could be reduced to “I [publishing service] will sell you [client] the X [names and addresses of arrestees] at the Y price,” and so was a purely economic transaction. Therefore it would fit comfortably within the narrow definition of commercial speech. However, this characterization is incorrect because it erroneously classified the advertising of the data product as the “speech” in question, when the “speech” subject of the regulation was really the arrestees data. The court might have been confused because so much of the commercial speech precedents involved advertising. Because of this error, the categorization of arrestee’s personal data as commercial speech would only work under Central Hudson’s broader definition of “related solely to the economic interests.” Unfortunately, the Supreme Court later reversed the Ninth Circuit’s decision on standing grounds and did not address the commercial speech issue.

A year after United Reporting, the Tenth Circuit decided the aforementioned U.S. West case. Like the Ninth Circuit, the Tenth Circuit noted that while the use and sale of

---

71 Id. at 1137.
72 Id. (quoting Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio, 471 U.S. 626, 637 (1985)).
73 Id.
74 Id.
75 Id.; see Virginia State Bd., 425 U.S. at 762.
77 U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).
phone company customer data do not fit neatly into the traditional commercial speech
definition of “a speech that proposes a commercial transaction,” the traditional
definition does not comprise the “universe of commercial speech.” Furthermore, the
Tenth Circuit admitted there was much ambiguity in the doctrine as to what exactly
constituted commercial speech. Nonetheless the court assumed, without offering any
justification, that the personal data in question was commercial speech because it was
speech “integral to and inseparable from the ultimate commercial solicitation.”

Due to ambiguity in the commercial speech precedents, it was impossible for the
Tenth Circuit to forward a good justification for classifying customer phone data as
commercial speech. The difficulty of precisely defining “commercial speech” is a
problem that predated United Reporting and U.S. West. In 1990, Ninth Circuit Court of
Appeals Judge Alex Kozinski pointed out it was not unclear just what exactly met the
traditional narrow definition of “proposing a commercial transaction.” For example, a
TV ad could be classified as a very short film, which is a form of speech fully protected
by the First Amendment.

Others have found the Central Hudson’s broader definition of “speech concerning
solely the economic interests of the speakers and audiences” problematic as well.
Examples such as a newspaper article discussing business affairs and an author writing

78 Id. at 1222-23 (quoting Pittsburgh Press Co. v. Human Relations Comm’n, 433 U.S. 376 (1973)).
79 Id. at 1233, n.4.
80 Id.
81 Id.
82 Alex Kozinski & Stuart Banner, Who’s Afraid of Commercial Speech?, 76 VA. L. REV. 627, 638-39
83 Id.
84 Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to
product reviews for pay would technically fall under this definition.\textsuperscript{85} However, such speech receives no less protection than political, religious, and social commentary.\textsuperscript{86} Hence, it is argued that although personal data is being sold for the “economic interests,” it still deserves full First Amendment protection.\textsuperscript{87} Justice Thomas also noted these difficulties in \textit{City of Cincinnati v. Discovery Network, Inc.},\textsuperscript{88} a case involving regulation on news racks on public sidewalks. He said: “[t]his very case illustrates the difficulty of drawing bright lines that will clearly cabin commercial speech in a distinct category.”\textsuperscript{89}

Despite these difficulties, the Court does not seem ready to abandon the commercial speech doctrine.\textsuperscript{90} In the last twenty-five years, the Court has not abandoned the distinction between commercial speech and other types of speech, and only Justice Thomas has indicated a willingness to abandon the distinction.\textsuperscript{91} Therefore, it is unlikely that there will be any satisfying solution to the problem of categorizing personal data.

\textit{B. Development of Intermediate Scrutiny for Commercial Speech Regulation}

Even if the Court were to construe personal data as commercial speech, there is still the problem of applying the appropriate level of constitutional protection. The commercial speech doctrine has undergone major changes in the last several decades, and the shifting doctrine will affect any analysis of personal data as commercial speech cases. This section will examine how the development of commercial speech doctrine has led to difficulties for courts in data speech cases.

\textsuperscript{85} \textit{Id.} at 1081.
\textsuperscript{86} \textit{Id.} Volokh also pointed out that recent cases in the late 1990s including 44 Liquormart have moved away from the \textit{Central Hudson} language and toward the common definition of “proposing a commercial transaction.” \textit{Id.} at 1082, n. 138.
\textsuperscript{87} \textit{Id.} at 1081.
\textsuperscript{88} 507 U.S. 410 (1993).
\textsuperscript{89} \textit{Id.} at 418-20.
\textsuperscript{90} See discussion infra Part III.B.
\textsuperscript{91} 44 Liquormart v. Rhode Island, 517 U.S. 484, 522-23 (Thomas, J., dissenting).
Until the 1970s the Court afforded no constitutional protection to commercial speech. In 1980, in *Central Hudson Gas & Electric Corp. v. Public Service Commission*, the Court first applied intermediate scrutiny and used a four-part test to determine the constitutionality of a commercial speech regulation. Now known as the *Central Hudson* test, it provided that courts should determine: (1) whether the commercial speech is truthful and not misleading, and if so, (2) whether the asserted government interest is substantial, (3) whether the regulation directly advances the governmental interest asserted, and (4) whether the regulation is no more extensive than is necessary to serve that interest.

In 1996, in *44 Liquormart, Inc. v. Rhode Island*, the Court opened the possibility that strict scrutiny may be applied to commercial speech. In unanimously striking down a Rhode Island ban on price advertising for alcohol, the Court said *Central Hudson*’s intermediate scrutiny is only justified when the state regulates commercial messages to protect consumers “from misleading, deceptive, or aggressive sale practices.” Otherwise, “strict review” is appropriate. The Court proceeded to do so because it did not find that the Rhode Island’s total ban of alcohol price information to be motivated by a consumer protection interest that justified intermediary scrutiny. In particular, the majority read the fourth prong of *Central Hudson* to require an evaluation of a ban’s

---

93 447 U.S. 557. The court struck down a state regulation that prohibited electricity companies from sending advertisements promoting the electricity use along with utility bills.
94 *Id.* at 566.
95 *Id.*
97 *Id.* at 501.
98 *Id.*
99 *Id.*
effectiveness and an examination of alternatives to determine a ban’s constitutionality.  

Under the majority’s application of the test, the regulation must be “no more extensive than necessary.” Furthermore, the majority requires the regulation to “directly advance” its purpose “to a material degree” or “significantly.”

Justice O’Connor’s concurrence also appeared to tighten the requirement of the last prong of the Central Hudson test by taking “the availability of less burdensome alternatives” as a signal that narrow tailoring is not met. Furthermore, O’Connor states that there was no need for the majority to apply a more strict version of the Central Hudson test, since the Rhode Island’s regulation would have failed Central Hudson “as is.” In sum, 44 Liquormart signaled the Court’s intention to increase protection for commercial speech. Hence, post-44 Liquormart, a government regulation must meet this searching examination. Therefore, it seems unlikely that a regulation banning commercial speech would ever survive the Central Hudson test as applied by the 44 Liquormart court. It is not surprising that, since 44 Liquormart, the Court has struck down regulations banning casino advertising and billboards for tobacco products.

1. Intermediate Scrutiny Applied: U.S West

Post 44 Liquormart, the Tenth Circuit applied the Central Hudson test in the aforementioned U.S. West case. There, the FCC issued an order requiring telecommunication companies to implement an opt-in procedure before using, disclosing

100 Id. at 505.
101 Id. at 507.
102 Id. at 505.
103 Id. at 529.
104 Id. at 532.
105 Id.
or sharing a customer’s personal information\textsuperscript{109} for marketing purposes.\textsuperscript{110} The “opt-in” procedure required a company to obtain customer consent prior to using or sharing the customer’s information. To the phone companies, this was more restrictive than the opposite “opt-out” procedure, which instead allowed a company to use or share information until a customer decided to voice disapproval. The FCC order, however, did not prohibit companies from contacting their own customers about the services to which they already subscribed.\textsuperscript{111}

In \textit{U.S. West}, the first prong of \textit{Central Hudson} was met because both parties agreed that the data involved truthful and non-misleading information.\textsuperscript{112} The Tenth Circuit then devoted substantial discussion on whether a government asserted privacy interest could sufficiently meet the second prong of \textit{Central Hudson}, which required substantial state interest. While the court acknowledged that privacy may rise to the level of substantial interest, the court looked for, but did not find, a showing of specific harms such as potential for embarrassment or misappropriation of sensitive information.\textsuperscript{113} Nevertheless, the court assumed that the FCC had met the second prong,\textsuperscript{114} because it would fail on the last two prongs.

On the third prong, the court, invoking \textit{44 Liquormart} languages, held that the FCC failed to prove that the regulation “directly and materially advances its interest.”\textsuperscript{115} The court said that the FCC only relied on speculation and did not provide evidence that

\textsuperscript{109} At issue was customer proprietary network information (CPNI), which included information collected over the course of the carrier-customer relationship, such as details on telephone bills as well as records of phone calls placed and received. \textit{U.S. West, Inc. v. FCC}, 182 F.3d 1224, 1228 n.1 (10th Cir. 1999).
\textsuperscript{110} \textit{Id.} at 1228.
\textsuperscript{111} \textit{Id.}
\textsuperscript{112} \textit{Id.} at 1234.
\textsuperscript{113} \textit{Id.}\ The court also observed, “[a] general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial interest.” \textit{Id.}
\textsuperscript{114} \textit{Id.}
\textsuperscript{115} \textit{Id.} at 1237-38.
privacy interests would be harmed. Finally, the court held that the regulation did not meet the fourth prong of *Central Hudson*, which required the regulation to be narrowly tailored. Citing O’Connor’s occurrence in *44 Liquormart*, the court noted that “evidence of an obvious and substantially less restrictive means” indicated “a lack of narrow tailoring.” The court reasoned that the opt-out approach advocated by the phone companies was less restrictive than the FCC’s mandated opt-in approach, citing experimental data presented by the phone companies that only a small percentage of customers granted approval to share their data when contacted under the opt-in approach. The court rejected FCC’s position that opt-out was not as effective as opt-in as an argument based only on “common sense” and speculation, which was sufficient only to meet a rational basis analysis. Hence, the FCC lost under the last two prongs of *Central Hudson* and the Supreme Court did not grant certiorari. Undoubtedly, the *44 Liquormart* decision made the case much more difficult for the FCC.

2. A Novel Approach to Intermediate Scrutiny: *Trans Union Corp. v. FTC*\(^\text{122}\)

Two years later after *U.S. West* was decided, the D.C. Circuit offered a different and conflicting rationale for intermediate scrutiny in *Trans Union Corp. v. FTC*.\(^\text{123}\) The court there upheld a FTC order preventing Trans Union, a credit reporting agency, from selling its target marketing products. The data products consisted of lists of names and addresses of individuals who met specific financial criteria, such as possession of an auto

---

\(^{116}\) *Id.*

\(^{117}\) *Id.* at 1238.

\(^{118}\) *Id.* at 1238-39.

\(^{119}\) *Id.*

\(^{120}\) *Id.*

\(^{121}\) *Id.*

\(^{122}\) *Id.*

\(^{123}\) *Id.*

17
loan, a department store credit card, or two or more mortgages.\textsuperscript{124} The FTC acted under the authority of the Fair Credit Reporting Act (FCRA),\textsuperscript{125} which restricts a credit reporting agency to furnish consumer reports to persons for certain “permissible purposes” only, some of which include determining eligibility for credit and employment.\textsuperscript{126} The FTC determined that the lists that Trans Union sold to target marketers were “credit reports” furnished for an impermissible purpose.\textsuperscript{127}

Unlike the Tenth Circuit, the D.C. Circuit addressed the First Amendment argument last in its opinion, devoting only five paragraphs to it.\textsuperscript{128} Also, instead of applying \textit{Central Hudson}, the D.C. Circuit justified intermediate scrutiny using a rationale from \textit{Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.}\textsuperscript{129} In \textit{Dun & Bradstreet}, the Court held that a plaintiff did not have to meet the \textit{New York Times} actual malice standard\textsuperscript{130} when he brought a defamation suit against a consumer reporting agency who caused harm by issuing erroneous information about the plaintiff to five customers.\textsuperscript{131}

The D.C. Circuit reasoned that \textit{Dun & Bradstreet} stood for the proposition that speech that served only private interests deserved reduced constitutional protection.\textsuperscript{132} Since Trans Union’s lists were “solely of interest to the company and its business customers and relates to no matter of public concern,”\textsuperscript{133} the lists warranted reduced

\textsuperscript{124} Id. at 812.
\textsuperscript{125} 15 U.S.C. § 1681.
\textsuperscript{126} Trans Union, 245 F.3d at 813.
\textsuperscript{127} Id. at 814.
\textsuperscript{128} Id. at 818-19.
\textsuperscript{129} 472 U.S. 749 (1986).
\textsuperscript{130} New York Times v. Sullivan, 376 U.S. 254 (1964) (establishing the requirement for defamation plaintiffs to prove actual malice in cases concerning public figures and matters of public concern).
\textsuperscript{131} Dun & Bradstreet, 472 U.S. at 751-52.
\textsuperscript{132} Trans Union, 245 F.3d at 818.
\textsuperscript{133} Id.
constitutional protection.\textsuperscript{134} Without mentioning Central Hudson,\textsuperscript{135} the D.C. Circuit simply held in two paragraphs that the government had met intermediate scrutiny.\textsuperscript{136}

In its denial for rehearing,\textsuperscript{137} the D.C. Circuit defended its decision to apply Dun & Bradstreet.\textsuperscript{138} The court admitted that Trans Union’s reports did not contain “wholly false” information as with those in Dun & Bradstreet, but still dismissed the distinction as non-critical.\textsuperscript{139} Interestingly, the D.C. Circuit discussed a line of cases decided under the Central Hudson test. The court said that the FTC satisfied narrow tailoring required by intermediate scrutiny because its action was distinguishable from those actions held to be impermissible under various applications of Central Hudson. The D.C. Circuit reasoned that, unlike restrictions on vice advertising (e.g. gambling, alcohol, tobacco), where the government sought to mitigate harms caused by the advertised conduct or product, the government here could not “promote its interest (protection of personal financial data) except by regulating speech because the speech itself cause[d] the very harm the government [sought] to prevent.”\textsuperscript{140} Hence the court implied that the results would have been the same even if Central Hudson, as interpreted by 44 Liquormart, had been applied, and that it was immaterial that the court arrived at intermediate scrutiny from a different rationale. As such, the D.C. Circuit produced an outcome that is directly opposite to that of the Tenth Circuit.

\footnotesize{\textsuperscript{134} Id.\textsuperscript{135} Id.\textsuperscript{136} Id.\textsuperscript{137} Id.\textsuperscript{138} Trans Union Corp. vs. FTC, 267 F.3d 1138 (D.C. Cir. 2001).\textsuperscript{139} Id.\textsuperscript{140} Id. at 1140 (the court merely stated, in a one sentence, “[n]othing in Dun & BradStreet, however, suggests that [the distinction was] critical to the Court’s decision”).}
After the denial for rehearing, Trans Union appealed to the Supreme Court, which denied the petition for writ of certiorari,\textsuperscript{141} with Justices Kennedy and O’Connor dissenting. Kennedy hinted that the D.C. Circuit’s rationale was out of the ordinary, and perhaps incorrect: “[t]his case is of national importance, and the Court of Appeals has adopted a novel approach to commercial speech. I would grant the petition for certiorari.”\textsuperscript{142} Kennedy also correctly distinguished \textit{Dun & Bradstreet} as a case involving false speech and noted that it was only a plurality opinion. This was a controversial case that had been criticized, and transplanting its rationale to a truthful speech context is problematic.\textsuperscript{143} In 2003, the Supreme Court declined an opportunity to clear the confusion when it denied cert in the commercial speech case \textit{Nike v. Kasky}.\textsuperscript{144}

\textbf{IV. Toward a Tiered Approach in Adjudicating First Amendment Challenges to Data Privacy Laws}

In light of the problems with these early commercial speech cases involving personal data, this article proposes a tiered approach unique to data privacy laws. The proposed approach moves the focus away from the debate over whether personal data is “commercial” speech and instead focuses on ensuring effective data privacy laws are made consistent with the speech protection goals of the First Amendment.

There are three reasons why the focus on the debate over whether data is “commercial” speech is misplaced. First, while personal data are sold for commercial purposes, there are instances when they are used for non-commercial purposes such as charity fund-raising, political organizing, and private or police detective work. Hence,

\textsuperscript{141}Trans Union LLC v. FTC, 536 U.S. 915 (denying cert).
\textsuperscript{142}Id.
\textsuperscript{143}Justices Kennedy and O’Connor stated it was “questionable ... whether this precedent has any place in the context of truthful, non-defamatory speech.” Id.
\textsuperscript{144}539 U.S. 654 (2003).
personal data cannot fit into an either-or distinction between commercial speech and non-commercial speech; it is simply in a different category of its own. Second, *US West* and *United Reporting* showed that that courts struggled to categorize personal data as commercial speech. In addition it is clear that the Court is not moving toward a clear, bright-line rule approach in commercial speech.\(^{145}\) It is enough to note that in many instances personal data is analogous to commercial speech, and this can be a basis for supporting intermediate scrutiny for some data privacy regulations. Third and most important, the commercial attribute of personal data is secondary to the primary concern of control. Unlike restriction on political speech or dangerous speech, regulation of personal data is not about suppressing ideas, as personal data is neutral and contains no opinion or idea. The main issue is the control of data -- who gets to use it and how. It is more useful to emphasize the aspect of personal data as property or goods. Based on these concepts of data control and data as property, this article proposes a three-tier approach to evaluating the constitutionality of data privacy laws under the commercial speech precedents. This tiered approach is somewhat similar to the Court’s Time, Place and Manner jurisprudence, which varies the level of constitutional protection based on the regulation scheme in question.

\textit{A. Top Tier: Strict Scrutiny for Categorical Bans}

At the top tier, regulation that bans use or sale of personal data in a categorical way should receive something akin to strict scrutiny in line with the approach taken by the Court in *44 Liquormart*. Just as it is difficult to justify a total ban on alcohol price information to serve a public health purpose, government should not be able to ban any data speech, commercial or otherwise, for privacy purposes unless it meets strict scrutiny.

\(^{145}\) See discussion \textit{supra} Part III.A.
Justices Stevens and Kennedy’s dissent in *United Reporting* pointed out that were
United Reporting to lawfully obtain arrestees’ data from a legal source other than the
state government, California could not have banned United Reporting from using the data
for commercial purposes.\(^{146}\) Even though bans by category may be the most effective
means of privacy regulation, they completely wrestle away control of data from its owner
and heighten the risk of laws running contrary to the principle of free speech.

**B. Second Tier: Intermediate Scrutiny for Regulation Requiring Consent**

The second tier of the proposed approach distinguishes regulations that ban
speech from those that burden speech. When the government is burdening the exchange
of personal data to address the data control issue, intermediate scrutiny should apply.
Regulation requiring an opt-in falls within this category. Indeed, this approach should be
favored because it puts in place a default position in the law that addresses an imbalance
of bargaining power between corporations and individuals. The opt-in requirement is
similar to default contractual provisions that provide that there should be no free use of
data unless the parties have a “meeting of the minds.” For example, users of free email
websites often give up personal information to companies and allow them to share the
information, all in exchange for email services. This exchange is an “opt-in” in action
and fits with the data as property paradigm because personal data is given in exchange for
a benefit.

Requiring opt-in fits with the control paradigm since it requires individuals to
decide when and where to relinquish control of their personal information. Practically
speaking, companies that already have data would be required to obtain consent before
using and selling it. This would go a long way in addressing the privacy problems noted

in Part II. No longer will websites indiscriminately sell data without first getting consent. In addition, if intermediate scrutiny is met, laws should be able to require a default of limited scope consent, so that data are not passed from place from place without explicit consent.

It is true that the “opt-in” default position economically burdens companies, as do regulations that require companies to securely store data. However, regulations that burden data speech are beneficial because they correct the current devaluing of personal data. Opt-in makes “post-consent” personal data valuable again and deters it from being passed carelessly from one place to another. Regulation requiring secure storage also will achieve the same effect. If personal data becomes expensive, companies will make more effort to guard it.

Viewed in this way, the *U.S. West* decision was too harsh in striking down the FCC order. The Tenth Circuit took notice of O’Connor’s *44 Liquormart* concurrence, which stated that, even under *Central Hudson*, the availability of a less restrictive alternative is evidence that a law fails narrow tailoring. The Tenth Circuit gave only this justification: the existence of opt-out was an indication that opt-in was not a least restrictive means, which meant that the Tenth Circuit was essentially applying a least restrictive means analysis. Yet the Tenth Circuit failed to take into account that both opt-in and opt-out are distinguishable from the type of total ban that triggered strict scrutiny in *44 Liquormart*. This distinction is taken into account in the tiered approach.

Another argument for less than strict scrutiny in this area is that *44 Liquormart* justified striking down bans on advertisement by reasoning that narrow tailoring requires

---

147 U.S. West v. FCC, 182 F.3d 1224, 1238-39 (10th Cir. 1999).
148 *Id.*
the government to pursue its interests by directly regulating the harmful conduct or product promoted by the advertisement. On this point, the D.C. Circuit was correct in Trans Union. It follows that, if personal data sold in aggregated form without consent is the “actual” harmful product, then government regulation on the data “product” is exactly the action that the Court requires. Indeed, language in 44 Liquormart seems to allow more leeway when government acts in a consumer protection interest.

Finally, data privacy is an inherently architectural problem that requires an architectural solution. For example, the national Do-Not-Call registry, upheld by the Tenth Circuit in 2004, provided the type of architectural solution that ordinary customers needed to protect their privacy. There, the FCC and FTC provided a tool to help consumers opt-out of telemarketing lists in one national centralized database. The Tenth Circuit, characterizing the Do-Not-Call list as an “opt-in program” that put the choice of whether or not to restrict commercial calls entirely in the hands of the individuals, upheld the regulation. The Do-Not-Call registry example suggests that there is a way in which the government can create a technological solution that allows individual consumers to opt-out/opt-in more easily. This will help the many consumers who are either unaware of privacy concerns or do not have enough savvy to protect their privacy, again putting control of data back where it belongs.

C. The Special Tier: “Data Defamation” Torts

149 For example, in 44 Liquormart, Justice O’Connor suggested that Rhode Island could have increased alcohol taxes or conducted an anti-alcohol campaign. 44 Liquormart v. Rhode Island, 517 US 484, 529-30.
150 Id. at 501 (“When a State regulates commercial messages to protect consumers from misleading, deceptive, or aggressive sale practices, or requires the disclosure of beneficial consumer information, the purpose of its regulation is consistent with the reasons for according constitutional protection to commercial speech and therefore justifies less than strict review.”).
151 SOLOVE, supra note 6, at 97.
152 Mainstream Marketing Services, Inc. v. FTC, 358 F.3d 1228, 1242 (2004).
153 Id. at 1242.
154 SOLOVE, supra note 6, at 97.
Finally, at the third tier is a different type of test altogether, one that would follow the Court’s treatment of defamation torts under the First Amendment. Covered in this tier are statutes that have private rights of action provisions against companies that violate privacy laws. Much like the way that defamation actions are treated differently under the First Amendment, these provisions should also receive a special formulation of scrutiny, since they are analogous to torts laws. Part of the Trans Union opinion undoubtedly took this factor into consideration because the FRCA provided for private right of action against Trans Union for violating the FRCA.¹⁵⁵

This is an evolving area of law, because unlike defamation, privacy harms often involve truthful speech. The law is not ready to abandon this historical distinction of true versus false speech, even though with regard to privacy true speech often causes more damages. For example, fake or incorrect social security numbers and personal information are of no use to identity thieves, or telemarketers. This is another area where personal data’s unique attributes make it a misfit under the traditional notions of the First Amendment.

Moreover, individuals often suffer privacy harm inherent in the aggregation of truthful personal information. This area remains unsettled because of rapid technological changes as well as shifting policy debates.¹⁵⁶ The technological possibility for pervasive harms from truthful data remains not yet fully recognized by the public in the present. If and when the harm caused by truthful personal data is recognized as equal to those of false speech that gives rise to traditional torts actions, Congress or state legislative bodies should be able to codify such harms into statutes. The First Amendment should have a

¹⁵⁵ Trans Union LLC v FTC, 536 U.S. 915, 915 (discussion in dissent denying cert).
¹⁵⁶ This is a controversial topic, and some argues that there is not a privacy right of not having others reveal truthful information about an individual. See Volokh, supra note 84, at 1050-51.
place for such “data torts” along side of defamation torts. Indeed, if one accepts this argument, then the D.C. Circuit’s analogy between the harm in the truthful credit report and that of defamation does not seem so far-fetched.

Conceptually, consumer statutes that allow for private rights of action also helps solve the architectural problem of unequal balancing power in a way similar to the Do-Not-Call registry. These consumer protection statutes provide individuals with tools to take back some control of their own data through litigation. Indeed, individuals are already starting to file suits under state consumer protection laws to protect their data privacy. The first example is *Leadbetter v. Comcast Cable Communications*, a class action suit where cable internet users are suing cable providers over the release of their information for investigation into illegal music downloading. In another case, an America Online (AOL) subscriber sued AOL for giving away his information in response to a simple police request. The First Amendment should not unduly restrict these consumers from pursuing their private rights of action to protect data privacy.

V. Conclusion

Privacy regulations over the use and sale of personal data face constitutional uncertainty. As the commercial speech doctrine continues to govern this area, the Court’s vague formulation of what triggers intermediate scrutiny versus strict scrutiny leaves both opportunities and challenges for regulatory agencies like the FTC and the FCC. The focus on whether personal data constitutes commercial speech is misplaced, and a new category for personal data is needed to allow the courts to better account for

---

157 Case No. 05 2 114115 KNT (King County, Washington, Complaint filed May 3, 2005), removed to federal court as Case No. C05-0892RSM (Western District of Washington).
the distinctive attributes of personal data. Finally, such a new category of data speech can adapt from precedents from the commercial speech area, and the Court should distinguish total bans from other regulatory regimes to accomplish the goals of encouraging effective privacy laws while protecting speech rights. In this manner, the Court will ensure that the commercial speech doctrine as applied to personal data will accord proper weight to the increasingly important interests of data privacy.