THE CONTROL OVER THE DE-IDENTIFICATION OF DATA

INTRODUCTION: THE INFORMATIONAL PRIVACY DEBATE

With increasing technological advances, and worries about big brother watching over our shoulders, there is a continuing debate about our right to privacy, its scope, and the danger of losing it.

Privacy is a very broad concept with many different aspects. The ability to use computers to organize and manipulate data in ways never before possible has spurred a debate about whether the courts and Congress should recognize a right to informational privacy. While a constitutional right to decisional privacy has been recognized by the Supreme Court,[1] there is no federally recognized right to informational privacy.[2] People concerned with protecting informational privacy want to restrict the dissemination of personal information and prohibit any unauthorized use of it.[3] Legislation enacted to address these concerns affords different types of information varying levels of protection,[4] as not all personal information is recognized as requiring the same level of privacy protection.[5] In the United States, personally identifiable medical and financial information, and child-related information is often recognized as more sensitive than other types of information and given stronger protection.[6] The European Union affords a very strict informational privacy right based on personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[7]

---

1 *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965); Roe v. Wade, 410 U.S. 113 (1973).

2 *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1413 n. 118 (2001) (contrasting decisional privacy with informational privacy); Sandra Byrd Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163, 164 (1995).

3 *See* Petersen, *supra* note 2, at 164.

4 *See* RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 179-82 (1st ed., corrected 1993) (discussing disapprovingly the way informational privacy statutes have been constructed, in particular their approach to "sensitive information").

5 *See id.* at 22-25. Wacks defines when information should be considered personal. Wacks' definition of personal information applies specifically to what I refer to as "sensitive" information. *See id.* at 179-80.

6 *See* Letter from Donald S. Clark, Secretary, Federal Trade Commission, to John McCain, Chairman, Committee on Commerce, Science and Transportation, United States Senate (July 31, 1997), at http://www.ftc.gov/os/1997/9707/privac9b.pdf (last visited March 25, 2002) [hereinafter McCain Letter]; *see also* Stephen F. Ambrose, Jr. & Joseph W. Gelb, *Consumer Privacy Regulation and Litigation*, 56 BUS. LAW. 1157, 1157 (2001).

7 Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection

Attempting to address some of the growing informational privacy concerns, Congress has passed privacy legislation addressing a variety of areas, including financial, medical, and cable TV subscriber information.[8] This piecemeal approach has been deemed inadequate by commentators due to both its reactive instead of proactive nature, and heavy lobbying from both businesses and credit reporting agencies.[9] Congressional statutes and related administrative agency regulations typically exclude information from protection once the information has been modified in such a way that the data subject[10] can no longer be identified.[11] For example, Subtitle A of Title 5 of the Gramm-Leach-Bliley Act ("GLBA")[12] protects consumers from disclosure of their nonpublic personal information by requiring financial institutions to provide consumers with the opportunity to opt out of having their nonpublic personal information shared with third parties.[13]

Although personally identifiable information cannot be disclosed by a financial institution to a third party if the consumer objects, de-identified information is treated differently. While promulgating regulations in accordance with the GLBA, the Federal Trade Commission's ("FTC") final rule[14] noted that "[i]nformation that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses" should not be considered personally identifiable information, and therefore not covered by the statute.[15] The Commission's final rule appeared to follow the trend of other privacy legislation exempting de-identi-

---

of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 8.1, 1995 O.J. (L 281) 31, 40 [hereinafter European Directive].

[8] *See, e.g.*, Gramm-Leach-Bliley Act, Disclosure of Nonpublic Personal Information, 15 U.S.C. §§ 6801-10 (2000); Health Insurance Portability and Accountability Act of 1996, Administrative Simplification, 42 U.S.C. §§ 1320d, -1 to -8 (Supp. V 1999); Cable Communications Policy Act of 1984, Protection of Subscriber Privacy, 47 U.S.C. § 551 (1994).

[9] *See* Petersen, *supra* note 2, at 180-83; *see also* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2000) (arguing that since there is not yet any "meaningful" informational privacy legislation, informational privacy would be better treated as a property right).

[10] Data subject refers to the person whom the information is about. *See* European Directive, *supra* note 7, art. 2(a), at 38.

[11] I will refer to this process as both de-identification and anonymization.

[12] 15 U.S.C. §§ 6801 - 6810. Only Subtitle A of Title V of this act, the Disclosure of Nonpublic Personal Information, is covered by this note. Pursuant to the authority granted in 15 U.S.C. § 6804(a)(1), the Federal Trade Commission promulgated a final rule implementing the GLBA. *See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313).

[13] *See* 15 U.S.C. § 6802(b).

[14] Final rules are drafted by administrative agencies and other regulatory authorities under authorization from Congress. *See* discussion *supra* note 12.

[15] 16 C.F.R. § 313.3(o)(2)(ii)(B) (2001).

fied information from statutory coverage.[16] The final rule is silent, however, on the transformation of regulated personally identifiable information into non-regulated de-identified information. I will argue that this transformation should not be regulated by the GLBA.

However, in a recent case, *Individual Reference Services Group, Inc. v. Federal Trade Commission*,[17] a district court found that the GLBA creates a privacy interest in the de-identification of data.[18] While admitting that the regulation expressly prohibits any privacy interest in de-identified data, the court noted that there is a distinction between whether there is a privacy interest in de-identified data and whether "consumers have a privacy interest in the initial use of their nonpublic personal information for the creation of [de-identified] data . . . ."[19]

This note will argue that this statement by the *Individual Reference Services Group* ("IRSG") court was an incorrect interpretation of the GLBA and is inconsistent with the current state of the law on informational privacy.[20] By focusing on the GLBA, this note will show that the informational privacy interest for a data subject[21] should extend only to the use and sharing of personally identifiable information with unauthorized persons. Since no privacy interest is retained in de-identified information, there should be none in the de-identification process. This note presents the issue in four parts.

Part I of this note will provide the framework for *IRSG* and explore the use of de-identified information in the financial industry. This part will describe the growth of the credit reporting industry from generating credit reports to developing additional uses for the information disclosed to them in order to generate those reports. Part I further examines the privacy provisions in the Fair Credit Reporting Act ("FCRA")[22] and the GLBA, both of which ad-

---

16 *See, e.g.*, Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.502(d) (2001); Telecommunications Act of 1996, 47 U.S.C. § 222(c)(3) (Supp. V 1999).

17 145 F. Supp. 2d 6 (D.D.C. 2001).

18 *See id.* at 38.

19 *Id.* The court in this case was specifically referring to the creation of aggregated data, where personally identifiable financial information for a group of individuals is added and then divided by the number of individuals to obtain the characteristics for an "average" consumer in an average area. Individually identifiable characteristics no longer remain after aggregation. *See* In the Matter of Trans Union Corp., No. 9255 at 12 (Fed. Trade Comm'n Mar. 1, 2000), *petition for review denied*, 245 F.3d 809 (D.C. Cir. 2001).

20 Whether this statement is dicta or a holding is subject to debate.

21 A consumer in the context of the GLBA.

22 *See* 15 U.S.C. §§ 1681, 1681a-1681u (2000).

dress credit reporting agencies[23] ("CRAs") and provide increasing privacy protections for consumers. Finally, Part I will conclude by exploring the *IRSG* decision.

Part II will compare Congress' approach to de-identified, anonymous data in other statutes with the approach taken in the GLBA. Examining this approach may shed light on Congressional intent when promulgating the GLBA. This part will address how other privacy statutes treat de-identified information, and whether they mention if notice is required before de-identification. Part II will be divided into two sections: the first will examine the Congressional approach to sensitive personal information, and the second will examine the approach to non-sensitive personal information.[24]

Part III will focus on the European Community and examine the European Directive[25] and its approach to de-identified data. The European Directive is important domestically because in order for United States businesses to be able to receive personally identifiable information from a European company, they must be found to be in compliance with the United States Safe Harbor Principles,[26] approved by the European Commission as meeting the Directive requirements.[27] Examination of the Directive and relevant case law will show that while the European Directive has strict privacy standards, those standards do not regulate the de-identification of personally identifiable information.

Part IV concludes with two sections. The first section suggests ways for Congress to improve existing statutory language to provide a clear and uniform approach to personally identifiable nonpublic information. The second section presents a model statute incorporating the congressional recommendations from the first section. Model "legislative history" is also included to aid in interpreting "congressional" intent.

---

[23] CRA can refer to either a credit reporting agency, or a consumer reporting agency. While these titles are often used interchangeably, some credit reporting agencies provide only commercial credit information and not consumer credit information. *See* ROBERT ELLIS SMITH, PRIVACY, HOW TO PROTECT WHAT'S LEFT OF IT 65 (1979) (noting that Dun & Bradstreet is known for its credit reports on businesses, not consumers, and that these commercial credit reports are not subject to the FCRA).

[24] *See* discussion *supra* p. 1 (distinguishing sensitive from non-sensitive information).

[25] *See* European Directive, *supra* note 7.

[26] *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).

[27] *See* Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, 2000 O.J. (L 215) 7; *see also* European Directive, *supra* note 7, art. 25, at 45-46.

I. BACKGROUND AND ASSOCIATED FINANCIAL ACTS

A. *The Rise of Credit Reporting Agencies and the Evolving Need for Privacy Protection*

Credit reporting agencies started developing approximately 150 years ago.[28] During the early years of American business operations, credit was infrequently granted to consumers and there were no agencies devoted to investigating consumer credit.[29] It was only after the Panic of 1837 that companies began to recognize a need for an ordered process of granting credit.[30] The first mercantile agency was founded in New York in 1841 and grew into the modern credit reporting agency of Dun and Bradstreet, Inc.[31]

In the ensuing 150-plus years, CRAs have grown so greatly in size that Congress acknowledged that "[c]onsumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers."[32] The purpose of the CRA is to collect consumer credit information from credit grantors, among others, and then assemble this information about a specific consumer into a credit report.[33] The credit report is then sold to banks and other lenders, possibly the same credit grantors who provided information to the CRA.[34] Insurance companies and employers are also purchasers of these credit reports.[35] As a result of such an extensive gathering of credit information, CRAs possess extensive databases containing sensitive credit and financial information about millions of consumers.[36]

Looking to develop a way to use this information beyond the creation of credit reports for banks and loan grantors, CRAs became aware that if they could share this information with third parties, such as marketing agencies, this sensitive financial information could provide a wealth of information to the marketers and increased revenue to the CRA.[37] With access to specific

---

28 *See* JOHN M. SHARP, CREDIT REPORTING AND PRIVACY 8-10 (1970) (providing a look into the history of the rise of the credit bureau in both the United States and Canada).

29 *See id.*

30 *See id.*

31 *See id.* at 9. Dun & Bradstreet is known for its commercial credit reports. *See* SMITH, *supra* note 23.

32 15 U.S.C. § 1681(a)(3) (2000) (noting this in the congressional findings of the FCRA).

33 *See* In the Matter of Trans Union Corp., No. 9255 at 1 (Fed. Trade Comm'n Mar. 1, 2000), *petition for review denied*, 245 F.3d 809 (D.C. Cir. 2001).

34 *Id.*

35 *Id.*

36 *Id.*

37 *See* SMITH, *supra* note 23, at 46. Smith, in 1979, described the process of "prescreening" where a credit card company or bank could have the CRA tailor a mailing list to the credit, age, family size or other characteristics desired. *Id.* As technology has increased,

credit and financial information, the marketers could more easily determine to whom they should target their products.

B. *Congress Passes the Fair Credit Reporting Act to Protect Private Financial Information*

Aware that information intended for generating credit reports could be misused, Congress passed the FCRA with one of its main goals being to "protect the privacy of individuals whose sensitive credit and financial data are collected, used, reviewed and transmitted by [credit reporting agencies]."[38] The intention of the FCRA was to protect the privacy of a person's financial information, but not a person's identity.[39]

The FCRA restricted the dissemination of a consumer report except if it is being disseminated for a permissible purpose such as (1) the extension of credit; (2) employment purposes; (3) underwriting insurance; (4) determination of license eligibility; (5) risk assessment for an existing credit obligation; and (6) a legitimate business need for the information.[40] The FCRA prohibited the distribution of credit information to people that did not have a statutorily authorized purpose for using that information,[41] such as target marketers.[42]

Credit reporting agencies have extensive databases. For example, Trans Union's consumer reporting database contains both personally identifiable financial and non-financial information.[43] Trying to make use of this information, while staying within the confines of the FCRA by not releasing credit-related information,

---

CRAs have created databases containing information from credit reports and sold mailing lists generated from these databases to direct marketers for target marketing purposes. *See* H. JEFF SMITH, MANAGING PRIVACY 2 (1994). Some aspects of this process are no longer permitted, though other aspects of direct marketing still are. *See* discussion *infra* pp. 10-12.

38 In the Matter of Trans Union Corp., No. 9255 at 1 (citing the REPORT OF THE COMMITTEE ON BANKING AND CURRENCY, S. REP. NO. 91-517 (1969)).

39 *See id.* Information not covered by the FCRA would not be restricted from dissemination to target marketing agencies. The court did note that the age of a person cannot be distributed because that information is sometimes used in credit decisions, unlike a person's name, telephone number, etc. *Id.*

40 *See* 15 U.S.C. § 1681b (2000) (cited in In the Matter of Trans Union Corp., No. 9255 at 2).

41 *See id.* § 1681a(d)(1). This section of the FCRA states that information cannot be distributed to non-statutorily authorized individuals if it is to be "used or expected to be used" in credit eligibility decisions. *Id.*

42 Target marketing is not a permissible purpose for using a consumer report under the FCRA. *See* In the Matter of Trans Union Corp., No. 9255 at 14 (citing Trans Union Corp. v. Fed. Trade Comm'n, 81 F.3d 228, 230 (D.C. Cir. 1996)).

43 *See* Trans Union, 81 F.3d at 229. The non-financial information consisted of "name (and aliases), social security number, addresses, phone numbers, occupation, gender, ethnic background, marital status and education." *Id.* The financial information consisted of the credit history on any credit account. *Id.*

Trans Union, one of the three CRAs involved in target marketing,[44] used the database it had to generate mailing lists which it provided to target marketing agencies.[45] Trans Union sold the lists to companies that sold catalogs, sweepstakes entries, or other types of solicitations.

The marketing lists were composed of names and addresses of people the companies felt would be receptive to their products.[46] While they did not specifically include any credit information, in order to be included on a list, a person needed at least two credit accounts and possibly had to meet other certain sub-criteria, based on either family size, ethnic origin, or place of residency as specified by the company desiring the list.[47]

In 1992, the FTC brought suit against Trans Union claiming that these target marketing lists were consumer reports, and as such, were governed by the FCRA and could not be distributed to people not authorized by the statute.[48] On remand from the D.C. Circuit,[49] the FTC held that Trans Union's target marketing lists should be considered consumer reports because they contain information that relates to "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living."[50]

C. *The Use of De-identified Data is Sanctioned by the FTC*

The Commission's ruling ended the sharing of personally identifiable financial information with target marketers, but left two alternate uses for CRA databases. Noting the purpose of the FCRA was only to protect the privacy of financial information, the Commission stated that non-financial information such as a person's name, mother's maiden name, generational designator, telephone number, and social security number are not covered by the FCRA, and can be disclosed.[51]

---

[44] Following a wave of consolidation in the 1970s and 1980s, basically only three CRAs remain that provide consumer credit reports: Trans Union, Experian, and Equifax. *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 24 (2000). All three of these CRAs are involved in target marketing practices. *See* In the Matter of Trans Union Corp., No. 9255 at 11.

[45] *See* In the Matter of Trans Union Corp., No. 9255 at 11.

[46] *See* Trans Union, 81 F.3d at 229.

[47] *See id.* at 229-30.

[48] *See* In the Matter of Trans Union Corp., No. 9255 at 2 (quoting the administrative complaint filed by the FTC).

[49] *See* Trans Union, 81 F.3d 228.

[50] In the Matter of Trans Union Corp., No. 9255 at 30 (quoting 15 U.S.C. § 1681a(d)(1) (2000)).

[51] *See id.* Information not covered by the FCRA would not be restricted from dissemination to target marketing agencies. The court did note that the age of a person cannot be

In addition, the Commission indicated that de-identified financial information contained in these credit databases could be disclosed and used for target marketing purposes.[52] While Trans Union's products did not de-identify data before being sold to marketers, violating the FCRA, the Commission cited approvingly the products of two of Trans Union's competitors.[53] These companies provided information to target marketers de-identified by aggregation.[54]

Aggregated information can be looked upon as an "average" of personal information that no longer contains individual identifying characteristics. When CRAs aggregate data, they combine the credit reports for each consumer in a specific geographical area, often based on zip code.[55] This combined data is then divided by the number of consumer reports for the area, resulting in an average consumer report for a consumer within that area.[56] The data provides a window into the financial properties of an average consumer, but not a specific consumer.[57] Instead of knowing an individual's credit characteristics, a target marketer can only find out the characteristics of individuals residing within the specific geographic area.[58] Data is often aggregated at the zip-plus-four level, which covers five to fifteen households.[59] The target marketer would then solicit all residents within a certain zip-plus-four area instead of select people. While the marketer would not have the precision available with the marketing lists prohibited by the FCRA, the marketer would know that the average person within a certain zip-plus-four area meets the marketer's desired financial criteria.

By contrasting the competitor's products with the Trans Union product which released personal financial information, the Commission gave implicit approval to the use of aggregated financial information for target marketing purposes. Before it remanded to the Commission, the D.C. Circuit indicated that disclosure of zip code information was not permissible under the FCRA when it noted that zip code alone could be a factor that had

---

disclosed because that information is sometimes used in credit decisions, unlike a person's name, telephone number, etc. *Id.*

52 *See id.* at 12.

53 *See id.* The two competitors were Experian and Equifax. *Id.*

54 *Id.*

55 *Id.*

56 *Id.*

57 *Id.*

58 *Id.*

59 *See id.* Zip-plus-four is the standard five-digit zip code with four additional digits, providing increased geographic resolution. *Id.*

creditworthiness.[60] The Commission rejected that notion stating that "[r]egardless of whether this information might bear on credit worthiness, nothing in the record before us establishes that zip codes are actually used, or expected to be used as a credit eligibility factor in scoring or as a credit criterion in prescreening."[61] Since zip codes are not used as a factor in creditworthiness decisions, their release for non-FCRA-authorized purposes is permitted by the FCRA.

D. *The Gramm-Leach-Bliley Act Strengthens Privacy Information on Personally Identifiable Information, But Does it Change the View on De-identified Information?*

While the FCRA prohibited the disclosure of personally identifiable financial information, the disclosure of non-financial personally identifiable information by CRAs was still permitted.[62] This practice was halted with the enactment of privacy provisions within the GLBA.[63] The GLBA restricted the dissemination of "nonpublic personal information"[64] unless a consumer was given the opportunity to opt out of the disclosure.[65] Information not covered by the FCRA, such as name and address, was included by the FTC final rule in the definition of nonpublic personal information.[66] The GLBA exempted financial institutions from providing an opt out prior to disclosing nonpublic personal information to a CRA.[67] This permits a CRA to continue generating credit reports without having to ask a consumer for disclosure of his or her information.[68] While CRAs can receive this nonpublic information, they cannot

---

60 *See* Trans Union Corp. v. Fed. Trade Comm'n, 81 F.3d 228, 232 (D.C. Cir. 1996) ("Zip codes (*e.g.* Beverly Hills 90210 and kindred upscale zip codes around the country) . . . seem to have at least as much creditworthiness value as knowing simply that a person once borrowed money . . . .").

61 In the Matter of Trans Union Corp., No. 9255 at 30 (Fed. Trade Comm'n Mar. 1, 2000).

62 *See* discussion *supra* note 51.

63 *See* 42 U.S.C. §§ 6801 - 6810 (2000); Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2001). In the supplementary information submitted with the final rule, the FTC explicitly stated that while some commentators had indicated otherwise, a CRA cannot re-disclose nonpublic information it receives from a financial institution unless it is in the form of a consumer report. *See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646, 33,668 (May 24, 2000).

64 Nonpublic personal information is a subset of personally identifiable information that has been made available to a financial institution through its interactions with the consumer. *See* 15 U.S.C. § 6809(4). Personally identifiable information that is publicly available is not covered by this statute. *See id.* § 6809(4)(B).

65 *See id.* § 6802(b).

66 *See* Privacy of Consumer Financial Information, 65 Fed. Reg. at 33,668 & n.36.

67 *See* 15 U.S.C. § 6802(e)(6)(A).

68 The FTC noted that this "permits the continuation of the traditional consumer reporting business . . . ." Privacy of Consumer Financial Information, 65 Fed. Reg. at 33,668.

give it to a third party unless it is in the form of a consumer report, as permitted by the FCRA.[69] Aggregated information was specifically excluded from the definition of nonpublic personal information.[70] Since aggregated information is not considered nonpublic personal information, its use does not fall within the scope of the GLBA.[71] While nonpublic personal information is covered by the GLBA, and aggregate data is not, the statute and FTC final rule are silent on whether the process turning nonpublic personal information into aggregate data is covered by the GLBA.

The FTC final rule contains language concerning the release of GLBA-covered information, but not de-identified information. While the Commission noted that a non-affiliated third party (such as a CRA) receiving nonpublic personal information cannot re-disclose that information,[72] it also noted that credit header information[73] does not "lose[ ] its status as 'nonpublic personal information' when the consumer reporting agencies combine it with other information in their databases."[74] Both Commission comments address data which has not been de-identified. However, the Commission does not expressly address whether financial information can be aggregated and then disclosed to a third party, without providing any type of notice to the consumer.[75] The creation of this aggregate information and subsequent disclosure should be allowed without providing notice to the original data subject.[76]

---

69 *See supra* note 63.

70 *See* 16 C.F.R. § 313.3(o)(2)(ii)(B) (2001). The Commission stated that aggregate information is not considered personally identifiable information. *Id.* Personally identifiable information was earlier defined as nonpublic personal information. *See id.* § 313(n)(1)(i).

71 *See* 15 U.S.C. § 6801(a) ("[E]ach financial institution has an affirmative and continuing obligation to . . . protect the security and confidentiality of those customers' *nonpublic personal information.*") (emphasis added).

72 *See* Privacy of Consumer Financial Information, 65 Fed. Reg. at 33,668 (discussing 16 C.F.R. pt. 313.11).

73 Information located on the top of a credit report containing identifying information such as the name, address, and social security number of the individual is referred to as "credit header" information due to its location at the "head" of the credit report. Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 14 (D.D.C. 2001).

74 *See* Privacy of Consumer Financial Information, 65 Fed. Reg. at 33,668. When this information is combined with other information, it does not lose its identifying characteristics. When information is aggregated, the result is void of nonpublic personal information.

75 If a CRA was already in possession of aggregate information, there should be no question that information could be disclosed as it is expressly excluded from the definition of nonpublic personal information.

76 This note will only focus on whether data could be de-identified through aggregation under the GLBA without requiring consent of the consumer. In its final rule, the FTC states that in addition to aggregate information, "blind data that does not contain personal identifiers such as account numbers, names, or addresses" is also excluded from the definition of personally identifiable financial information. 16 C.F.R. § 313.3(o)(2)(ii)(B). If con-

Yet, in one of the first cases interpreting the GLBA, a district court disagreed.[77] In a statutory challenge by the Individual Reference Services Group, the court noted that while the creation of aggregated data and its dissemination is not prohibited by the GLBA, "the rules simply prevent [CRAs] from doing so without first giving the consumer the chance to opt out."[78] The court continued, noting that there is a distinction between whether there is a privacy interest in this aggregated data and whether "consumers have a privacy interest in the initial use of their nonpublic personal information for the creation of aggregate data . . . ."[79]

This case dealt primarily with the disclosure of credit header information, disclosure of which was permitted by the FCRA, but not the GLBA.[80] Since the court focused on credit header information, it is difficult to determine if the court's statements on aggregate data were dicta or a holding.

The comments by the *IRSG* court indicate that at least in the realm of financial information, consumers should have a privacy interest in the use of their nonpublic personal information, including the act of de-identifying data. The *IRSG* court agreed that the consumer does not have an interest as to how his or her information is used once he or she is rendered anonymous.[81] While the aggregate data could be used without notice or permission from the consumer, the consumer would have to be provided notice and the opportunity to opt out before the data could be aggregated.[82]

This view is inconsistent with the GLBA. The intention of the Act was to ensure that financial institutions "respect the privacy of its customers and . . . protect the security and confidentiality of those customers' nonpublic personal information."[83] Once the

---

sent is required before personally identifiable financial information is aggregated, by the same reasoning, consent would be required when data is made "blind" through removal of its identifying traits. The relevant issue is whether the data becomes de-identified either through aggregation or removal of personal identifiers. Since the D.C. Circuit has addressed this issue with the GLBA only concerning aggregate information, the focus on this note will be to show that this aggregate information can be de-identified without consumer consent. *See Individual Reference Servs. Group*, 145 F. Supp. 2d 6. Examples will be shown concerning blind data, but they will be used to show that the *Individual Reference Services Group* court was in error on its statement concerning the de-identification of data through aggregation.

77 *See Individual Reference Servs. Group*, 145 F. Supp. 2d 6.

78 *Id.* at 38.

79 *Id.*

80 The court noted that only one of the two plaintiffs, Trans Union, was challenging the effects of the FTC regulations on the disclosure of aggregate data. *See id.* at 16.

81 *See id.* at 38.

82 *See id.* (noting that an opt-out opportunity needs to be provided before data aggregation).

83 15 U.S.C. § 6801(a) (2000).

data has been rendered anonymous by aggregation, the consumer's information is no longer personally identifiable and no longer considered nonpublic personal information by the regulation.[84] Since the act of de-identifying the data only serves to prevent a consumer from being individually identified, this process should not violate a consumer's "security and confidentiality" of his or her nonpublic personal information.[85] The argument that this note asserts rests on the assumption that this de-identified data is truly de-identified and that an individual in the aggregate pool does not risk re-identification.

An act that specifically excludes aggregate data from the definition of nonpublic consumer information should not be interpreted as requiring consumer notice before data relating to him or her is de-identified by aggregation. If the *IRSG* court is correct that consumers have a privacy interest in the de-identification process, though not the resulting de-identified data, consumers may need to be provided a second opt-out notice, posing logistical problems not addressed by the GLBA.

A consumer normally has a relationship with the financial institution obligated to issue the opt-out notice. If a financial institution was interested in disclosing nonpublic personal information to a non-authorized entity, the consumer would be provided the opportunity to opt out of that disclosure.[86] Whether or not a consumer decides to, the financial institution is permitted to disclose the consumer's nonpublic personal information to a CRA.[87] Following the logic of the *IRSG* court, in order for a CRA to be permitted to de-identify the data, which would remove the data from coverage by the statute, a second opt-out opportunity would need to be provided.[88]

If this result was intended by the GLBA, the Act would have covered the mechanics of the process. Financial institutions that have a direct relationship with the consumer and provide the opt-out notice for their purposes could include additional language covering data aggregation. However, these financial institutions have no interest in providing an opt-out notice solely for the bene-

---

84 *See supra* note 70.

85 *See* 15 U.S.C. § 6801(a).

86 The opt-out is required by 15 U.S.C. § 6802(b).

87 *See* 15 U.S.C. § 6802(e)(6)(A).

88 Of course, if the consumer does not opt out of the first notice, thereby permitting disclosure of his or her personally identifiable financial information to unauthorized third parties, this opt-out should be inclusive of the additional opt-out for data aggregation called for by the *IRSG* court. If a consumer is not concerned about the release of personally identifiable financial information, the consumer should not be worried about taking that information and rendering it de-identifiable.

fit of a CRA. This information is already disclosed to CRAs for the generation of credit reports and financial institutions are not affected by whether or not CRAs can aggregate this data and use it for marketing purposes.

That would leave the CRA to provide notice of the opt-out opportunity. The CRA, deemed a financial institution for purposes of the GLBA,[89] would be required to provide an opt-out notice to a consumer with whom the CRA has no relationship. While consumers may be familiar with their bank, and would not be surprised to receive from it a privacy notice containing an opt-out provision, receiving one from a CRA, of whose existence they may not have even been previously aware, would be unusual.

While the *IRSG* court arrived at the idea of an opt-out provision to permit the aggregation of data, the statute's opt-out provision deals with the disclosure of nonpublic personal information, not with rendering nonpublic personal information into a de-identified form.[90] CRAs are now left not knowing whether or not they can legally aggregate this information without providing an opt-out. Due to this uncertainty, companies that license and/or use target marketing products may now be reluctant to license the databases that are the basis of these products.

II. The Approach of the United States to De-identified Information

Unlike Europe, where privacy legislation has been implemented broadly, the United States Congress has passed narrowly focused statutes covering various subject areas.[91] If the United States had a broad privacy statute in effect for all data, that one statute would be dispositive on privacy issues and Congressional intent. Since the United States has multiple statutes and administrative regulations concerning privacy, the intent of the GLBA drafters may only be understood by examining several of these. In addition, since the FTC drafted the final rule implementing the GLBA, looking at prior FTC approaches to privacy issues not contained in a rule or regulation can also shed insight into the GLBA approach to de-identified data.

While examining the statutes, it is important to remember that not all nonpublic personally identifiable information merits the

---

89 *See* Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 14 n.2 (D.D.C. 2001).

90 *See* 15 U.S.C. § 6802(b)(1).

91 *See* Solove, *supra* note 2, at 1440.

same level of protection. In the United States, information pertaining to children, or medical and financial issues has been considered more sensitive than other types of information.[92]

Part II will be divided into three sections. Section A will examine how the FTC has handled the privacy of sensitive information. Section B will examine a Department of Health and Human Services ("DHHS") final rule concerning medical privacy and Section C will examine privacy legislation passed by Congress concerning less-sensitive personally identifiable information.

A. *FTC Positions Concerning the Privacy of "Sensitive Information"*

1. Credit Guides: FTC Comments Suggest No Notice Required for De-identification

The FTC has previously allowed data de-identification without providing notice to the data subject. To aid interpretation of the FCRA, the FTC issued a policy statement clarifying what types of documents qualify as a consumer report.[93] Noting that the FCRA lists seven criteria upon which a communication could be considered a consumer report,[94] the FTC addressed the classification of credit guides.[95] Credit guides are grouped consumer reports supplied by CRAs to credit grantors that rate how well consumers might pay their bills.[96] If these guides are treated as consumer reports, they would fall within the scope of the FCRA, which prohibits its distribution to a credit grantor.[97] The FTC stated that credit guides are consumer reports because "they contain information which is used for the purpose of serving as a factor in establishing the consumers' eligibility for credit."[98] A way to get around this FCRA prohibition would be to code the credit guides, so that the identity of the data subject is not disclosed.[99] Coded credit guides are not considered consumer reports by the FTC until they are decoded.[100]

---

92 *See* McCain Letter, *supra* note 6, at 4; *see also* discussion *supra* p. 1 distinguishing sensitive from non-sensitive information.

93 *See* Statements of General Policy or Interpretations Under the Fair Credit Reporting Act, 16 C.F.R. § 600.1 (2001).

94 15 U.S.C. § 1681a(d)(1) (2000).

95 *See* 16 C.F.R. § 600, app. § 603(d), item 4.

96 *Id.*

97 *See id.* app. § 604(3)(A), item 8. Credit grantors do not have a permissible purpose to obtain a consumer report on each consumer. *Id.*

98 *Id.* app. § 603(d), item 4.

99 *See id.*

100 *See id.* The commentary suggests using identification such as social security number, driver's license number, or bank account number. *See id.* These items would likely be considered nonpublic personal information under the GLBA. *See* Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(m)-(n) (2001). Credit guides should still be permissible

Coded credit guides are a type of de-identified consumer report. The coding of a credit guide and subsequent release to a credit grantor, a non-FCRA-authorized third party, is analogous to de-identifying personally identifiable financial information through aggregation and then releasing that information, expressly considered not-personally identifiable information, to a non-GLBA-authorized third party.

By sanctioning the use of the coded credit guide, without requiring notice to the data subject before the credit guide is coded and made available to a non-FCRA-authorized third party, the FTC appears to be indicating that it has no concerns with the act of de-identification.[101] Rather, the main concern is the identification of the data subject. If this is so, then it should follow that the FTC in drafting the GLBA implementation regulations did not intend a consumer to be provided notice before data de-identification. What is important is that the consumer would remain unidentifiable following the de-identification process.

2. Children's Privacy: The FTC Approves a Plan with Stricter Privacy Protections than the GLBA

Beyond issuing final rules and guidance concerning the FCRA and GLBA, the FTC is charged with monitoring operations on the Internet for unfair or deceptive practices.[102] The FTC was petitioned in 1996 by the Center for Media Education ("CME") to investigate whether a website operated by SpectraCom called "KidsCom" was being operated using unfair and deceptive practices.[103] At the time, the web site collected personal information from children such as name, sex, and birthday without providing adequate notice of the collection or subsequent use to the children's parents.[104] Another section of the website collected information on children's preferences for specific products.[105] This information was sold to marketers on an aggregate and anonymous

---

provided they are coded in a different manner, or rendered anonymous so that the credit grantor cannot re-identify the subjects of the consumer reports.

101 This differs from the GLBA only because the de-identification occurs via coding, as opposed to aggregation.

102 *See* 15 U.S.C. § 45(A)(2) (2000) (empowering the FTC to prevent corporations from using "unfair or deceptive acts or practices in or affecting commerce.").

103 *See* Letter from Jodie Bernstein, Director, Federal Trade Commission Bureau of Consumer Protection, to Kathryn C. Montgomery, President and Jeffrey A. Chester, Executive Director, Center for Media Education 1 (July 15, 1997), *at* http://www.ftc.gov/os/1997/9707/cenmed.htm (last visited Mar. 25, 2002) [hereinafter Bernstein Letter].

104 *Id.* at 1-2.

105 *Id.* at 2.

basis.[106] While the FTC ultimately did not recommend action against the operators of the KidsCom website, the FTC did set out in a response letter to the CME the "relevant legal standard" for how children's Internet privacy should be handled.[107]

KidsCom, in response to the FTC investigation, took measures to improve the privacy of the collected information and its notice provisions. KidsCom modified its website so that personally identifiable information collected from a child could not be released to third parties except under written consent from the parents of the child.[108] This requirement is a stricter standard of disclosure than the opt-out standard established by the GLBA for the disclosure of personally identifiable financial information to third parties.[109]

Parents were also provided the opportunity to object to the release of aggregate information to third parties.[110] This is also a stricter standard than the one set by the GLBA, which expressly excludes aggregate information from any notice provisions.[111] Even the *IRSG* court, which proposed requiring an opt-out opportunity before data aggregation, acknowledged that de-identified data cannot be withheld from unauthorized third parties.[112] The FTC did not develop the KidsCom rules, it only accepted what was submitted to them. It is unclear whether the FTC would have proposed the same standard for the control of aggregate information that KidsCom proposed.

In its response to the CME, similar to its views on credit guides, the FTC appears mainly concerned with the release of personally identifiable information, not the creation or release of anonymous aggregate information. One reason the FTC recommended that enforcement action not be taken against KidsCom is that "there is no evidence that KidsCom at any time released any personally identifiable information to third parties for commercial marketing . . . ."[113] The FTC noted that "[h]ereafter, staff may recommend law enforcement proceedings against marketers who . . .

---

106 *See id.*

107 *Id.* at 4.

108 *See id.* at 4. In contrast to an opt-out provision, this is an opt-in provision, where there cannot be disclosure unless a person opts in.

109 *See* 15 U.S.C. § 6802(b) (2000).

110 *See* Bernstein Letter, *supra* note 103, at 4. Whether this data can be aggregated without consent is not addressed. KidsCom seems to only be concerned with the release of personally identifiable information, or aggregate information and does not place emphasis on the process of converting the personally identifiable information to aggregate information.

111 *See* 16 CFR § 313.3(o)(2)(ii)(B) (2001).

112 *See* Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 38 (D.D.C. 2001).

113 Bernstein Letter, *supra* note 103, at 4.

unfairly use personally identifiable information collected from children."[114] The FTC letter did not address aggregate information.

While KidsCom included protection of aggregate information from disclosure, there is no evidence it was a necessary response to the FTC investigation. Though no personally identifiable information was sold, KidsCom did sell some aggregate and anonymous information to companies, but the FTC did not focus on this action and did not recommend sanctions for it. It appears from the FTC comments, that the main issue was the potential release of personally identifiable information without the prior consent of the parent.[115] Had the FTC been left to develop its own approach to the handling of the data, it is possible that it would not have required any notice before data is rendered anonymous and sold to other companies.

B. *The Approach to Medical Privacy*

Congress addressed the privacy of individually identifiable health information by enacting provisions within the administrative simplification section of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[116] Pursuant to Congressional authorization within this section, the DHHS promulgated the Standards for Privacy of Individually Identifiable Health Information ("Medical Privacy Standards").[117] These regulations established a set of privacy standards which ensure a patient access to his or her information while also protecting it from use by others.[118] The regulation covers "all individually identifiable health information in any form . . . that is held or transmitted by a covered entity."[119] The regulation specifically addresses the creation and use of de-identified protected health information.[120] It permits a covered entity to take protected personally identifiable information and de-identify it so that it can be removed from the scope of the regulation.[121] In addition, the covered entity does not have to de-

---

114 *Id.* at 5.

115 *See id.* at 4 (noting that a release of personally identifiable information by KidsCom would have been of particular concern "in light of the absence of adequate disclosure and prior parental consent").

116 *See* 42 U.S.C. § 1320d, -1 to -8 (Supp. V 1999).

117 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

118 *See id.* at 82,464. The DHHS notes that this protection is required to allow a patient to have peace of mind and to participate fully in his or her care by not being afraid to disclose medically sensitive information. *Id.*

119 *Id.* at 82, 488; *see also* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501 (2001) (defining "protected health information").

120 *See* 45 C.F.R. § 164.502(d); *see also id.* § 164.514.

121 *See id.* § 164.502(d).

identify the data in-house. A covered entity can give protected health information to a business associate for that purpose.[122] While de-identifying data, a covered entity is permitted to de-identify it in such a way that it may be able to re-identify the data at a later time.[123] The de-identified records can be marked, or the covered entity can use codes for later re-identification.[124] This information will be considered de-identified and outside the regulations, provided the covered entity does not disclose the de-identifying methodology which would enable another party to re-identify the data.[125] If re-identified, the data is subject to the regulation.[126]

Patient consent is not required by the Medical Privacy Standards before his or her information can be de-identified.[127] The preamble to the final rule notes that while many individuals believe they "own" their health records and must consent before their information can be released, the current law and practice is not supportive of this view.[128] This was noted in the context of providing consent to a release of individually identifiable information.[129] Release of de-identified information should raise even less privacy concerns.

When a health care provider wants to disclose protected health information (including individually identifiable information), the consent of the individual is required in most cases.[130] More relevant to this discussion is that the final rule generally provides that when a covered entity wants to disclose protected health information for marketing purposes, the individual's consent is

---

122 *See id.*

123 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,543.

124 *Id.*

125 *See id.*

126 45 C.F.R. § 164.502(d)(2)(ii).

127 While similar to the GLBA and the FTC final rule, there is no place in the Medical Privacy Standards where the DHHS states that "consent is not required prior to the de-identification individually identifiable health information." However, patient authorization is only discussed with regard to the disclosure of protected health information. *See* 45 C.F.R. § 164.508. De-identified data is not considered protected health information. *See id.* § 164.502(d)(2).

128 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,472.

129 *See id.*

130 *See* 45 C.F.R. § 164.508; *see also* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,473. The consent requirements under this regulation may change. The DHHS has proposed removing consent requirements regarding uses and disclosures of protected health information for the purposes of treatment, payment and health care operations. *See* Press Release, U.S. Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information B Proposed Rule Modification (Mar. 21, 2002), *at* http://www.hhs.gov/news/press/2002pres/20020321.html (last visited Mar. 25, 2002) [hereinafter Medical Rule Modification].

required.[131]

Unlike the GLBA, which requires a consumer to be provided with an opt-out opportunity before personally identifiable information is disclosed, the Medical Privacy Standards require an authorization.[132] Individually identifiable medical information therefore receives greater protection than personally identifiable financial information.

Yet, if the *IRSG* court was correct in its interpretation of the GLBA opt-out requirements, a consumer who has less privacy protection for personally identifiable financial data than medical data would have more privacy protection for non-identifiable financial information than non-identifiable medical information.

Since de-identified information is removed from coverage by the Medical Privacy Standards, the DHHS commented extensively on how the regulation must be structured in a way that the information is truly de-identifiable.[133] The standard for adequate de-identification of medical information is if it "does not identify the individual, or if the covered entity has no reasonable basis to believe it can be used to identify the individual."[134] The DHHS acknowledged that there is no way to truly de-identify information, but that there must be a "reasonable balance between risk of identification and usefulness of the information."[135]

The Medical Privacy Standards provide two ways for which medical information can be de-identified.[136] One way is by an expert who will alter the data so there remains only a very small risk that the information could be used to identify a patient.[137] Covered entities concerned the expert may unsatisfactorily de-identify the data can take advantage of a safe harbor alternative available by

---

131 *See* 45 C.F.R. § 164.514(e); *see also* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,545. The medical rule modifications would require a specific authorization from the individual before being sent marketing information. *See* Medical Rule Modification, *supra* note 130.

132 *See* 45 C.F.R. § 164.508 (containing details on the authorization for disclosure of protected health information).

133 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,708-12.

134 *Id.* at 82,543; *see also* 45 C.F.R. § 164.514(a).

135 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,708.

136 *See* 45 C.F.R. § 164.514. In addition to these two ways for de-identification, the DHHS is considering an alternative approach to de-identification which would create a "limited data set" of not directly individually identifiable information, yet would contain more identifiers than remain under the current safe harbor method described *infra* pp. 33-34. Stricter re-disclosure provisions would apply to data in this limited data set, than with de-identified information. *See* Medical Rule Modification, *supra* note 130.

137 *See* 45 C.F.R. § 164.514(b)(1).

removing eighteen individually identifying criteria.[138] The data identifiers range from name and telephone number to Internet protocol address numbers and voice prints.[139]

The regulation contains significant safeguards to ensure that the medical information is truly de-identified. An example is the zip code and age restrictions required to obtain the safe harbor protection.[140] While the age of the data subject does not need to be removed, if the individual is over 89 years old, the age must be "aggregated into a single category of age 90 or older."[141] The DHHS noted that while generally "age is sufficiently broad to be allowed in de-identified information . . .[e]xtreme ages—90 and over—must be aggregated further . . . to avoid identification of very old individuals (because they are very rare)."[142]

Regarding geographical origin, de-identified data can only retain the first three digits of the zip code when the population size within this geographic area is greater than 20,000 people.[143] When the total population of a geographic area representing a three-digit zip code is less than 20,000 people, the initial three digits are changed to "000," forming a new geographic area with a population greater than 20,000 people.[144]

While a medical record may be identifiable only to the first three digits of a zip code, the FTC has looked approvingly to data aggregation at the zip-plus-four level, covering five to fifteen homes.[145] Claritas, a company that supplies target marketing products, provides a "confidentiality edit" when only one record is available in a zip-plus-four area so that one household is not identified.[146] However, a confidentiality edit when an individual household is in danger of being identified is quite different than being concerned when there are less than 20,000 individuals in a geographic area.

Perhaps with the FTC financial regulations containing such a brief reference to aggregate information, the possibilities of re-identification were not considered. With a sample aggregated to

---

138 *See id.* § 164.514(b)(2)(i).

139 *See id.*

140 *See id.*

141 *Id.* § 164.512(b)(2)(i)(B).

142 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,710.

143 *See* 45 C.F.R. § 164.514(b)(2)(i)(B)(1).

144 *Id.* § 164.514(b)(2)(i)(B)(2). *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,711.

145 In the Matter of Trans Union Corp., No. 9255 at 12 (Fed. Trade Comm'n Mar. 1, 2000), *petition for review denied*, 245 F.3d 809 (D.C. Cir. 2001).

146 *Id.* at 11-12.

the zip-plus-four level, it may be possible to re-identify the data subject. If so, then perhaps that information should remain covered by the GLBA.

However, that concern is only reached after addressing the threshold issue of whether the data subject has a privacy interest in preventing his or her personally identifiable information from being de-identified. Only after deciding that there is no privacy interest in preventing de-identification of this personally identifiable information, would it be necessary to ensure that the resulting data is truly de-identified.

In light of the strict de-identification criteria of the Medical Privacy Standards, it is important to question whether information has been de-identified in such a way that the data subject can not be re-identified. The FTC has looked approvingly to aggregation by CRAs on a zip-plus-four basis.[147] If Congress (or the FTC) felt the zip-plus-four aggregation was too focused, providing insufficient anonymity, it could require a broader aggregation than the zip-plus-four level. Congress could also add a "reasonable basis to believe" standard similar to the Medical Privacy Standards, stating that aggregate information is not considered personally identifiable information provided the financial institution has no "reasonable basis to believe it can be used to identify the individual."[148]

C. *The Handling of Personally Identifiable Information in Non-sensitive Areas*

Examining statutes covering less-sensitive types of personal information can also lend insight into Congressional views on privacy issues. For example, if Congress takes a restrictive view on non-sensitive personal information, this would support a more restrictive interpretation of the GLBA, which covers sensitive personal information.

1. The Telecommunications Act of 1996

a. Act permits de-identification without notice

Section 702 of the Telecommunications Act of 1996 restricted telecommunications carriers the use of customer proprietary network information ("CPNI").[149] This information is analogous to

---

147 *See id.*

148 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,543.

149 *See* 47 U.S.C. § 222 (Supp. V 1999). CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications car-

the nonpublic personal information covered in the GLBA.[150] Without providing notice to the customer, the disclosure of CPNI by a telecommunications carrier can only be for a use pertaining to the telecommunications service.[151] Similarly, under the GLBA, a financial institution cannot disclose financial information to a non-affiliated third party without providing the required notice.[152] While the GLBA permits the disclosure of nonpublic personal information once the consumer has been provided the opportunity to opt out of the disclosure, the Telecommunications Act of 1996 only permits the disclosure if a customer opts in.[153] Opt-in provisions provide much stronger privacy protection. If a customer does not respond to an opt-in request, the customer's data will not be shared, in contrast to an opt-out provision where the customer's data will be shared if the customer does not respond to the request. Comparing the GLBA opt-out with the Telecommunications Act opt-in, the Telecommunications Act seems to have stronger privacy protections, while dealing with "less-sensitive" data.[154]

Yet, the Telecommunications Act specifically excluded aggregate information from coverage.[155] Not only does the Act state that the telecommunications carriers can use aggregate data without the approval of the consumer,[156] the Act appears to permit aggregation of CPNI without notice or permission of the data subject. The Act allows a telecommunications carrier that "receives or ob-

---

rier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier . . . ." *Id.* § 222(h)(1).

150 *See* 15 U.S.C. § 6802(b) (2000).

151 CPNI can also be provided to the consumer upon request. *See* 47 U.S.C. § 222 (c)(2).

152 *See* 15 U.S.C. § 6802(a).

153 *Compare* 15 U.S.C. § 6802(b) (stating that a consumer's nonpublic personal information can be disclosed only after the consumer has been provided notice as to how the information will be used and also has been provided an opportunity to opt out of this disclosure) *with* 47 U.S.C. § 222(c)(1) (stating that customer approval must be received if a customer's CPNI is to be used for any purpose beyond one directly related to a telecommunications carrier's providing of telecommunications services). While the Telecommunications Act of 1996 is ambiguous as to what type of consumer notice is required, the FCC interpreted the act as requiring an opt-in provision. *See* 47 C.F.R. § 64.2007(b) (2001). The FCC acknowledged in *U.S. West, Inc. v. Federal Communications Commission* that it could have chosen other means of receiving consumer approval, including an opt out approach. 182 F.3d 1224, 1230 (10th Cir. 1999), *cert. denied,* Competition Policy Inst. v. U.S. West, Inc., 530 U.S. 1213 (2000).

154 The majority of the items defined as CPNI by the act do not apply to medical, financial, or child-related information which often is afforded a higher level of privacy protection. *See* discussion *supra* p. 1.

155 *See* 47 U.S.C. § 222(c)(3).The Telecommunications Act described aggregate information as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." *Id.* § 222(h)(2).

156 *See id.* § 222 (c)(3).

tains customer proprietary network information by virtue of its provision of a telecommunications service [to] use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1) [which require approval of the customer before CPNI was used]."[157] The Telecommunications Act of 1996 covers aggregate information prominently within the statute. By contrast, the GLBA presents the opt-out requirement concerning the disclosure of nonpublic personal information; the aggregate information exception is not mentioned.[158] Aggregate information is discussed only in the FTC final rule as being excluded from the definition of personally identifiable information, a subcategory of nonpublic personal information.[159]

In contrast, aggregate information is expressly mentioned in the Telecommunications Act of 1996.[160] Here, the subsection "[c]onfidentiality of customer proprietary network information" addresses (1) disclosure of CPNI, (2) disclosure of CPNI to the customer, or the customer's designee, and (3) the use of aggregate customer information.[161] While these first two items both have express provisions for what action the customer must take to permit the telecommunications carrier to disclose the CPNI,[162] there is no customer action required before a telecommunications company can "use, disclose, or permit access to aggregate customer proprietary network information."[163] If Congress wanted the customer notified before the CPNI was aggregated, it would have been mentioned here. Since stricter privacy provisions were implemented for CPNI under the Telecommunications Act of 1996 than for nonpublic personal information under the GLBA, there should not be a stricter standard for the creation of aggregate information under the GLBA as called for by the *IRSG* court.

b. The impact of *U.S. West* on *IRSG*

The privacy objectives of the Telecommunications Act of 1996 may have a direct bearing on those of the GLBA. In fact, it is possible that the GLBA opt-out provision was based in part on *U.S. West, Inc. v. Federal Communications Commission,*[164] a decision that vacated

---

157 *Id.*
158 *See* 15 U.S.C. § 6802(b).
159 *See* 16 C.F.R. §§ 313.3(o)(2)(ii)(B), (n)(1)(i) (2001).
160 *See* 47 U.S.C. § 222(c).
161 *Id.*
162 *See id.*
163 *Id.* § 222(c)(3).
164 182 F.3d 1224 (10th Cir. 1999), *cert. denied,* Competition Policy Inst. v. U.S. West, Inc., 530 U.S. 1213 (2000).

the FCC's final rule implementing CPNI provisions of the Telecommunications Act of 1996.[165] This case was cited by the defendants in *IRSG* in an attempt to invalidate provisions of the GLBA.

Impacted by the Telecommunications Act of 1996, U.S. West filed suit against the FCC questioning the constitutionality of the FCC's regulations concerning CPNI.[166] The case did not address the aggregate information provisions of the statute.[167] In fact, the court noted at the beginning of the case how CPNI was afforded the most sensitive level of protection due to its potentially sensitive nature but how "Congress afforded [aggregate customer information] substantially less privacy protection under [47 U.S.C.] § 222."[168]

Agreeing with some of the constitutionality questions raised by U.S. West, the *U.S. West* court, after concluding that the FCC's CPNI regulations constitute a government restriction on commercial speech,[169] invalidated them in part because they were not narrowly tailored to serve the interests of the federal government.[170] The court indicated that an opt-out strategy for the disclosure of CPNI may have been an acceptable alternative to the chosen opt-in.[171]

The plaintiffs in *IRSG* tried to raise a similar constitutional challenge citing *U.S. West.*[172] The *IRSG* court distinguished *U.S. West* because in *U.S. West* "neither the Congress nor the FCC explicitly stated what 'privacy' harm [the statute or regulations sought] to protect against."[173] The *IRSG* court noted that Congress articulated this harm in the GLBA when it stated "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal account information."[174] The *IRSG* court stated that the harm to the consumer is not a specific use and disclosure of the consumer's nonpublic in-

---

165 *Id.*

166 *See id.* at 1228.

167 The court notes that the central provision being dealt with is 47 U.S.C. § 222(c)(1). *Id.* One can only wonder if the district court in *IRSG* would have addressed aggregate information had IRSG not included aggregate information in their statutory challenge of the GLBA.

168 *U.S. West,* 182 F.3d at 1228.

169 *See id.* at 1232.

170 *See id.* at 1238-39.

171 *See id.* The court points out that the FCC should have considered an opt-out strategy as an option, calling it an "obvious and substantially less restrictive alternative." *Id.* at 1238.

172 *See* Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 42 (D.D.C. 2001).

173 *Id.* at 42 (quoting *U.S. West,* 182 F.3d at 1235) (brackets in original).

174 *Id.* (quoting 15. U.S.C. § 6801(a) (2000)).

formation, but instead "it is the use and disclosure of that information without the consent of the consumer."[175]

While the *IRSG* court is able to distinguish the GLBA from the Telecommunications Act of 1996 because the privacy harm in the latter act was not expressly stated by the FCC or Congress,[176] it was clear in the Telecommunications Act of 1996 that aggregate information was not considered part of a consumer's nonpublic information and that its use or disclosure did not require consumer consent.[177] While the GLBA required only an opt-out provision for the disclosure of information,[178] its privacy goals seem analogous to the Telecommunications Act of 1996.[179] There is no indication that Congress intended telecommunications carriers to get permission from customers before aggregating CPNI.

If the key privacy goal of the GLBA is to "protect the security and confidentiality" of a consumer's nonpublic personal information,[180] the aggregation of this data is not a violation of these privacy goals. Once aggregated, data remains secure, confidential, and de-identified. It should no longer be associated with the consumer from which it originated.[181]

2. Governmental Disclosure of Data (Privacy Act and Freedom of Information Act)

Examining statutes regulating government policy on personally identifiable information reveals that the main governmental concern is not the ultimate control of personal information, but protection of the data subject's privacy. Section 3 of the Privacy Act of 1974[182] governs how federal agencies collect, use, or disseminate records.[183] The Privacy Act prohibits the disclosure of information contained in its records subject to several exemptions.[184] One ex-

---

175 *Id.* at 43.

176 *See U.S. West*, 182 F.3d at 1235; *see also Individual Reference Servs. Group*, 145 F. Supp. 2d at 42.

177 *See* 47 U.S.C. § 222(c)(3) (Supp. V 1999).

178 It may even be that the *U.S. West* court suggested the opt-out procedure based on the GLBA's provision.

179 The FCC could have interpreted the Federal Telecommunications Act differently and decided to require an opt-out provision for CPNI. If that had happened, then the privacy requirements for the disclosure of CPNI/nonpublic personal information would have been the same, and the *U.S. West* court may have found the regulations constitutional.

180 *See Individual Reference Servs. Group*, 145 F.2d at 42.

181 If the aggregate information was found to not be truly de-identified, then it should not be removed from coverage by the statute. *See* discussion *supra* pp. 34-35.

182 *See* 5 U.S.C. § 552a (2000).

183 *See* Yaron F. Dunkel, *Medical Privacy Rights in Anonymous Data: Discussion of Rights in the United Kingdom and the United States In Light of the Source Informatics Cases*, 23 LOY. L.A. INT'L & COMP. L. REV. 41, 58 (2001).

184 *See* 5 U.S.C. § 552a(b)(5).

emption allows a record in the government agency's files to be disclosed if it is in a form that is "not individually identifiable" and will be "used solely as a statistical research or reporting record."[185] In addition, the Freedom of Information Act[186] ("FOIA") supports a policy "to open public business to public view when no 'clearly unwarranted' invasion of privacy will result . . . ."[187]

In *Department of Air Force v. Rose*,[188] the Court held that information could be distributed under the FOIA if the deletion of personal references and other identifying information proves sufficient to protect the privacy of the people mentioned in the sought-after information.[189] While these acts cover the public, and not the private sector, they illustrate that the privacy interest involved does not concern the use of information containing personal information, but whether that use is a "clearly unwarranted invasion of personal privacy."[190] Neither act questions whether personal references can be deleted from the information without consent of the data subject. As long as the privacy of the data subject is protected, both the FOIA and the Privacy Act permit the release of de-identified data,[191] and since there is no mention of contacting the data subject before this de-identification, it is implicit that no privacy interest exists in preventing the de-identification of this data.

3. The Cable Communications Policy Act of 1984

Section 631 of the Cable Communications Policy Act of 1984[192] prohibits cable operators from collecting and disseminating personally identifiable information without subscriber consent.[193] Except under limited circumstances,[194] a cable operator cannot disclose personally identifiable information about a cable subscriber unless the subscriber has previously provided his or her consent.[195] The names and addresses of cable subscribers cannot be disclosed unless the cable subscriber has had an opportunity to

---

185 *Id.* § 552a(b)(5).
186 5 U.S.C. § 552.
187 Department of Air Force v. Rose, 425 U.S. 352, 381 (1976).
188 425 U.S. 352 (1976).
189 *Id.*
190 *Id.* at 371 (quoting with approval Department of Air Force v. Rose, 495 F.2d 261, 266 (2d Cir. 1974)).
191 The *Rose* court stated that the disclosure of information which did not contain personal references would not be an invasion of privacy. *Id.* at 381.
192 47 U.S.C. § 551(a)(2)(A) (1994).
193 *See id.* § 551(b),(c).
194 *See id.* § 551 (c)(2).
195 *See id.* § 551(c)(1).

opt out.[196] The Act expressly excludes aggregate data from being considered personally identifiable information.[197] Since aggregate data is not personally identifiable information, the statute does not prohibit a cable company from using any information it has compiled so long as the identity of the cable subscriber is not revealed. The Cable Communications Policy Act of 1984 does not call for notifying cable subscribers if their non-identifying information is being collected or used.

The nature of the cable business provides an interesting twist to the *IRSG* holding. The *IRSG* court acknowledged that a consumer only has a privacy interest in data aggregation.[198] Unlike the financial industry, where financial institutions receive financial information in a personally identifiable form, what if it were possible to set up a system that recorded non-identifiable aggregate data of cable subscribers? This information would not need to be de-identified and is expressly excluded from the Act.[199] There is no substantive difference between de-identifying data already in a company's possession and collecting de-identified data in the first place. The net result is the same de-identified data, though collecting the aggregate data would circumvent the *IRSG* court's privacy concerns, while obtaining the same result with the data. Would the *IRSG* court then claim in this instance that collecting the aggregate data, expressly excluded by statute, is a breach of privacy? Even if it thought so, it would be bound to adhere to the Act.[200] This hypothetical circumvention of the de-identification process demonstrates that it was not intended in any of these statutes to provide the data subject notice before personally identifiable data was de-identified.

III. THE EUROPEAN COMMUNITY'S APPROACH TO DATA DE-IDENTIFICATION

The European Data Directive[201] provides a common level of protection for the processing of personal data for all EU member countries.[202] Personal data which is or is intended to undergo processing may only be transferred to non-European Community countries that provide an "adequate level of [privacy] protec-

196 *See id.* § 551(c)(2)(C)(i).
197 *See id.*
198 Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 38 (D.D.C. 2001).
199 *See* 47 U.S.C. § 551(a)(2)(A).
200 Of course, the court could always find the statute unconstitutional.
201 *See* European Directive, *supra* note 7.
202 *See id.* art. 1, at 38.

tion."[203] In order for United States companies to be permitted to receive personal information from companies within the European Community, the United States Department of Commerce promulgated the Safe Harbor Privacy Principles.[204] The European Commission accepted these principles as providing an adequate level of protection.[205]

The European Directive provides that under ordinary circumstances, any time personal data is to be processed, the data subject must give his or her unambiguous consent.[206] Since de-identifying or aggregating data would involve destruction and erasure of certain parts of the data, something expressly considered processing by the Directive,[207] it would appear that de-identification may be a process prohibited by the Directive unless the data subject provides consent. The issue is more complicated, however, because the Directive specifically references de-identified data in recital 26 which states that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."[208]

This precise issue was addressed by the English Court of Appeal in *Regina v. Source Informatics Ltd.*,[209] where pharmacists de-identified prescription information and then sold it to Source Informatics. The British Department of Health issued a policy document stating that it was a breach of confidence to de-identify the prescription data without the consent of the data subject.[210] The Court of Appeal reversed a lower court ruling upholding the British Department of Health policy document.[211] This case is quite helpful in understanding the relevant issues due to the lack of case law concerning data de-identification, and Source Informatics' sub-

---

203 *See id.* art. 25.1, at 45.

204 *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).

205 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82486 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

206 *See* European Directive, *supra* note 7, art. 7(a), at 40. The Directive defines data processing as "any operation or set of operations which is performed upon personal data . . . such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, clocking, erasure or destruction[.]" *Id.* art. 2(b), at 38.

207 *See id.* art. 2(b), at 38.

208 *See id.* recital (26), at 33.

209 2001 Q.B. 424 (Eng. C.A.).

210 *Id.* at 431.

211 *See id.* at 444. For an article contending that this case was wrongly decided, and that patients in both the United States and the United Kingdom should maintain control over anonymous medical data, see Dunkel, *supra* note 182. Dunkel does not address the de-identification of medical data, but instead argues that the medical patient's right to privacy should extend to anonymous information. *See id.* at 44.

sequent use of the data for marketing purposes.[212]

While the controversy originated before the European Directive became effective, the Directive was raised on appeal by both parties with each side using it to support their view.[213] The Department of Health argued that de-identifying the data was a form of processing which required the explicit consent of the data subject.[214] The appellants argued that the Directive "can have no more application to the operation of anonymising data than to the use or disclosure of anonymous data."[215] While the court acknowledged that erasure or destruction of data is considered a form of processing "for good reason . . . it by no means follows, however, that [anonymization] should be held to fall within the definition: on the contrary, recital (26) [of the European Directive] strongly suggests that it does not."[216] This statement by the court on the European Directive was not meant to be a definitive ruling,[217] but the court felt that this judgment was supported by both "commonsense and justice."[218]

This case is directly on point and illustrates how the *IRSG* court should have held concerning the anonymization of nonpublic personal information. As seen in *Source Informatics*, under the European Directive, any data rendered anonymous is no longer subject to protection, and the rendering process does not require consent. The GLBA should be interpreted similarly.

The GLBA's opt-out provisions concerning the release of personally identifiable information to a third party for the use of target marketing are also consistent with the European Directive. The Directive specifically addresses direct marketing on two fronts. When personal information is to be processed with an anticipated use of direct marketing, the data subject needs to be provided the right to "object, on request and free of charge, to the processing . . . ."[219] Even if data is not being processed, if it is to be released to a third party for the use of direct marketing, the data

---

212 *See* Regina v. Source Informatics, Ltd, 2001 Q.B. 424, 434 (Eng. C.A.). The court notes "the striking paucity [concerning] the anonymisation of confidential information and its subsequent use in anonymised form." The court could only find two cases in the case law which were at all relevant to the issue. *Id.*

213 *See id.* at 440-41.

214 *See id.* at 441 (citing the European Directive, *supra* note 7, arts. 2, 8.1, 8.2(a),8.3, at 38, 40-41).

215 *Id.* at 442. The court noted that the appellant placed great reliance on the European Directive, *supra* note 7, recital (26), at 33. *Id.*

216 2001 Q.B. at 442.

217 In fact, the court stated that "this is clearly not the appropriate occasion to attempt a definitive ruling on the [European Data Directive]." *Id.*

218 *Id.*

219 *See* European Directive, *supra* note 7, art. 14(b), at 43.

subject needs "to be expressly offered the right to object free of charge to such disclosures or uses."[220]

CONCLUSION

A. *Congressional Advice*

Congress must make clear that an entity covered by a statutory privacy provision has the authority to de-identify data without providing notice to the data subject, when the resulting de-identified data is no longer covered by the statute.

Regulation of an individual's personally identifiable nonpublic information, whether by the domestic piecemeal approach, or the comprehensive European approach, has been similar.[221] Data has been considered either personally identifiable, thus requiring protection, or anonymous, removing it from statutory coverage. If the resulting anonymized information is no longer covered by statute, it does not make sense to find an informational privacy interest in protecting data from the de-identification process.

With the data subject retaining no privacy interest in the de-identification, Congress must ensure that data which has been de-identified is truly de-identifiable. Excluding aggregate information or blind data from coverage without providing a standard for de-identification suggests that this subject has been poorly thought through.

The privacy sections of the appropriate statutes should be amended to contain language similar to the Medical Privacy Standards. Congress should establish a reasonable basis standard for data de-identification,[222] and should consider safe harbor alternatives for complying with this provision. Congress may decide that medical information requires greater protection than financial or other types of information. Regardless, the courts should not be required to determine which information warrants a higher level of protection.

Aggregation to the zip-plus-four level has been looked at favorably in the context of interpreting the FCRA.[223] It is unclear

---

220 *Id.* The final rule implementing the GLBA stipulates that a financial institution must disclose to the consumer if nonpublic personal information is shared with non-affiliated third parties, and if so the consumer needs to be provided with the option to opt out, and be instructed on how he or she may do so. *See* Privacy of Consumer Financial Information, 16 C.F.R. § 313.6(a)(6) (2001).

221 The approach is only similar, of course, in the areas the United States has decided should be covered by privacy regulation.

222 *See* 45 C.F.R. § 164.514(a) (2001).

223 *See* In the Matter of Trans Union Corp., No. 9255 at 12 (Fed. Trade Comm'n Mar. 1, 2000), *petition for review denied*, 245 F.3d 809 (D.C. Cir. 2001).

whether the *IRSG* court thought this aggregation was inappropriate. The *IRSG* court only stated that a consumer needs to be notified before his or her data can be identified.[224] The level of aggregation permitted should turn on whether or not a data aggregator feels that there is a reasonable basis to believe the data can be re-identified. It is possible that once even a small amount of data is aggregated, re-identification becomes extremely difficult and an individual's confidentiality would be maintained. That is a decision that should be left to Congress or the administrative agencies.

B. *Model Statutory Language*

Using language from the GLBA and Telecommunications Act of 1996, and incorporating the recommendations stated in Section A of this note's conclusion, model statutory language is presented for Congress to use when addressing individually identifiable nonpublic personal information. The model statute includes a de-identification standard and specifically excludes the de-identification process from any notice requirements. Individually identifiable nonpublic personal information remains protected and not subject to disclosure without a level of notice being provided to the individual. The model language is designed to be used for one comprehensive privacy statute but can also be adapted for use with the existing piecemeal statutory scheme.

§ 1 Protection of Individually Identifiable Nonpublic Personal Information.

(a) In General.

Every business entity has a duty to protect the confidentiality of individually identifiable nonpublic personal information disclosed to it.

(b) Definition.

As used in this section:

(1) Individually identifiable nonpublic personal information

The term "individually identifiable nonpublic personal information" means information —

(A) provided by an individual to a business entity;

(B) resulting from any transaction with the individual or any service performed for the individual; or

(C) otherwise obtained by the business entity.

(2) Such term does not include publicly available information.

---

224 *See* Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 38 (D.D.C. 2001).

(c) Confidentiality of Individually Identifiable Nonpublic Personal Information.

(1) Privacy requirements for business entities.

Except as required by law or with the approval of the individual, a business entity that receives or obtains individually identifiable nonpublic personal information by virtue of its business interactions shall not use, disclose, or permit access to individually identifiable nonpublic personal information beyond the scope for which the information was originally collected.

(2) Disclosure on request by individuals.

A business entity shall disclose individually identifiable nonpublic personal information, upon affirmative written request by the individual, to any person designated by the individual.

(3) De-identified nonpublic personal information.

(A) Information that does not identify an individual is not subject to the provisions of this statute.

(B) A business entity may render individually identifiable nonpublic personal information de-identifiable either through the creation of aggregate information or blind data without providing notice to the individual. This de-identified information shall remain exempt from the provisions of this statute, provided the business entity that created such de-identified information has no reasonable basis to believe that the information can be re-identified by any other person.

(d) Rulemaking, Regulatory Authority.

(1) Rulemaking.

The administrative agencies and authorities that regulate business entities that receive individually identifiable nonpublic personal information shall each prescribe such regulations as may be necessary to carry out the purposes of this section with respect to the business entities subject to their jurisdiction.

(2) Coordination, consistency, and comparability.

Each of the agencies and authorities required under Paragraph (1) to prescribe regulations shall consult and coordinate with the other such agencies and authorities for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities.

Legislative History

The following comments address specific issues which may arise during interpretation of the model statute. These comments are arranged by section and subsection.

§ 1(c)(1) Privacy requirements for business entities.

This statute allows for the disclosure of individually identifiable nonpublic information if the individual has given approval. The language of this statute has been intentionally left vague to permit the use of an opt-in or opt-out requirement prior to disclosure.[225] When an administrative agency tailors the privacy statute to differing types of information, the agency should decide what type of notice is required, providing stricter notice requirements for more sensitive information.

§ 1(c)(3) De-identified nonpublic personal information.

(A) The goal of this privacy statute is to "protect the confidentiality of individually identifiable nonpublic personal information . . . ." § 1(a)(1). Exempting de-identified nonpublic personal information from statutory coverage is consistent with this intent. Since de-identified information is not covered by this statute, it follows that the process of de-identification of this data is permitted without providing notice to the individual.

(B) If the resulting de-identified data is not covered by the statute, there should be no privacy interest in the de-identification process since there is no danger of a breach of the individual's confidentiality with the disclosure of the resulting de-identified data. This is consistent with the goal of the statute.

To ensure the confidentiality of the individually identifiable nonpublic personal information, a "reasonable basis to believe" standard has been chosen for the business entity to follow when determining if the blind or aggregate data meets the requirements of being de-identified. The administrative agency implementing this rule for a specific type of data may want to provide a safe harbor alternative to provide a business entity with an option that ensures data has been adequately de-identified.[226] It is possible that blind data may require a greater amount of de-identification than aggregate data since blind data pertains to one individual while aggregate data is an average of multiple individuals. Depending on the size of the aggregate pool, varying standards of de-identification may be required.

§ 1(d) Rulemaking, Regulatory Authority

While this model statute proposes a comprehensive approach to data coverage, it is understood that each data type may require specific safeguards within the framework proposed by this statute.

---

225 *See* discussion *supra* note 153. This ambiguous language was taken from the Telecommunications Act of 1996. *See* 47 U.S.C. § 222(c)(1) (1994).

226 *See* 45 C.F.R. § 164.514(b)(2)(i) (2001).

The administrative agencies are left with the task of developing specific final rules and regulations which will address privacy needs on a subject-by-subject basis, and tailoring the privacy provisions as appropriate for that type of data, while remaining consistent with the goals of this statute.

*Benjamin Charkow**

* Production Editor, *Cardozo Arts & Entertainment Law Journal*; J.D., 2003, Benjamin N. Cardozo School of Law.