University of Dayton Law Review

Volume 35 | Number 3 Article 4

5-1-2010

Model Omnibus Privacy Statute

Scot Ganow

Sam S. Han
University of Dayton

Model Omnibus Privacy Statute

Cover Page Footnote

Many thanks to Ms. Rebecca Greendyke and Mr. Brian Sullivan for their assistance in researching materials and helping to prepare this article for publication.

MODEL OMNIBUS PRIVACY STATUTE

Scot Ganow, J.D., CIPP[1]

Sam S. Han, Ph.D.[2]

---

[1] Certified Information Privacy Professional; J.D., University of Dayton School of Law, 2009. Mr. Ganow is an attorney and former corporate privacy officer, and has worked as Certified Information Privacy Professional consultant to healthcare and technology companies. Many thanks to Ms. Rebecca Greendyke and Mr. Brian Sullivan for their assistance in researching materials and helping to prepare this article for publication.

[2] Assistant Professor, University of Dayton School of Law.

ABSTRACT

One of today's major concerns is how easily digital information can be copied and disseminated. Thus, when one's private information becomes publicly available in digital format, that information can be readily duplicated and distributed across the globe within seconds. If the disseminated information includes credit card numbers or Social Security numbers, then there is a heightened exposure to identity theft and a host of other privacy-related crimes.

Given the existence of such a digital landmine, laws have been promulgated for various sectors (e.g., financial, healthcare, government, etc.) to protect personally-identifiable information. However, due to differing needs of the various sectors, each sector treats its data differently from other sectors.

Compounding to this sector-by-sector discrepancy, several states have enacted their own laws relating to personally-identifiable data. Thus, the treatment of personally-identifiable data can differ from state to state, as well as from sector to sector. This presents numerous compliance challenges to a business should it collect, use, and share personally-identifiable information as part of its business model. A company, even one of modest size with a small customer base, still faces questions as to which compliance structure it must follow: Must it comply with the laws of the state in which its customer resides? Is it governed by an overarching federal framework? Or, does it need to comply with a particular sector in which it does business, such as healthcare? A company can easily be paralyzed attempting to determine which laws govern the personally-identifiable information in its possession. This is to say nothing of the significant increase in its compliance burden should there be a transfer of information to and from a foreign country (or compliance regime), such as the European Union (EU) or countries in the Asia Pacific Economic Conference (APEC).

With these issues in mind, this paper examines whether an omnibus privacy statute can be crafted such that it adequately addresses each sector. While this paper takes no position either for or against an omnibus privacy statute, it shows the feasibility of crafting such a statute should such a privacy statute be deemed necessary.

Specifically, this paper presents a model omnibus privacy statute, which: (1) identifies categories of personally-identifiable data that are common across most sectors and across all states; (2) identifies particular data elements that fall within each of these categories; and (3) prescribes the treatment of these data elements (both in how to collect the data and in how

to protect the data after collection) based on their respective categories. Briefly, this paper proposes three distinct categories, namely: (1) high-risk data elements (which, standing alone, can identify a particular individual or cause harm); (2) mid-risk data elements (which can identify a particular individual or cause harm when combined with other mid-risk data); and (3) low-risk data elements (which cannot identify a particular individual unless used in conjunction with high-risk or mid-risk data).

Lastly, in the spirit of creating solutions through such an omnibus privacy statute, we humbly suggest a model form which a compliant business organization can use in the collection, use, and sharing of personally-identifiable information. A practical privacy-enabling tool, such as a standard universal form for the collection of personally-identifiable information, not only meets the letter of the law, but provides an operational method by which employees and managers of any level of training can follow to ensure that the privacy protections of the statute truly follow the data from the point of collection and beyond.

I. INTRODUCTION

Even before the U.S. Supreme Court found an implied right of privacy in the Fourth Amendment,[3] an individual's right to privacy was an emerging legal issue.[4] At least one aspect of privacy that remains constant over time is that much of the debate revolves around technology. For example, Warren and Brandeis wrote their article on privacy in response to increasing numbers of newspapers and photographs that were made possible by the printing press.[5] While the Gutenberg press may be a distant historical memory for today's on-demand generation, the Internet (and electronic media in general) is fertile grounds for privacy debate.

Academic journals are replete with articles that oppose an omnibus federal privacy statute for various reasons.[6] Similarly, there are articles that advocate for a federal privacy statute to unify the disparate treatment of data elements across different sectors.[7] Given that such scholarly writings exist, and much of the pros and cons of an omnibus privacy statute are discussed by other learned scholars, this paper does not seek to advance one position over the other. In other words, we do not argue the merits or demerits of an omnibus federal privacy statute.

Instead, the goal of this paper is simply to provide a structural

---

[3] *See generally* Katz v. United States, 389 U.S. 347 (1967).
[4] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).
[5] *See, e.g.*, Wikipedia, Privacy, http://en.wikipedia.org/wiki/Privacy (last visited May 3, 2010).
[6] *See, e.g.*, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 902 (2009).
[7] *See, e.g.*, Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 868 (2009); Candice L. Kline, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 443, 443 (2008).

guideline on how an omnibus privacy statute should be written, in the event that Congress chooses to craft such a statute. In short, we do not discuss the "whether" question in this article, but rather the "how" question. This is because few, if any, articles address the "how" issue.

Structurally, we begin with a brief overview of currently-existing privacy-related statutes, both in the federal arena and the state arena.[8] In analyzing these laws, we focus on legislatively-enacted laws that address privacy concerns on a sector-by-sector basis, instead of on the judicial decisions that interpret those laws. The reason for our narrow focus stems from our goal of eventually crafting an omnibus privacy statute for collecting and protecting personally-identifiable information. Additionally, we intentionally limit the depth of our statutory review, because an exhaustive analysis of each statute is unnecessary for our purposes.

Once these federal and state privacy statutes are reviewed for their respective data elements,[9] we attempt to glean concepts that these statutes have in common, despite their applications in different arenas. From that analysis, we propose a model privacy statute that attempts to simplify handling of information across the many different sectors, both business and governmental. Furthermore, we suggest a proposed compliant intake form for the collection of personally-identifiable information that categorizes the information at the point of collection.

With this in mind, we now move to our review of privacy statutes, both in the federal arena and in the state arena.

II. REVIEW OF PRIVACY STATUTES

Many statutes either directly or indirectly implicate privacy. To discuss all of those laws without a specific focus would be both uninteresting and unhelpful. Thus, for purposes of this paper, we select only a handful of privacy-related statutes, which directly address privacy concerns. From these statutes, we attempt to: (a) discern overarching themes in how various entities approach data protection; and (b) identify recognizable categories for different types of data. Once the broad categories of data are identified, we take individual data elements and place them within their respective categories.

---

[8] We acknowledge the existence of the Wiretap Statutes (*e.g.*, 18 U.S.C. §§ 2510-2522 (2006); 47 U.S.C. § 605 (2006)), the Surveillance Statutes (*e.g.*, 47 U.S.C. §§ 1001-1010 (2006)), and the Polygraph Statutes (29 U.S.C. §§ 2001-2009 (2006)). However, those types of statutes are beyond the scope of this paper, because the Surveillance and Wiretap Statutes regulate data-interception techniques, rather than regulating the treatment of different data types. Our paper focuses narrowly on regulating the collection and disclosure of particular data types, rather than on the interception of every data type.

[9] Throughout this paper, unless otherwise specified, we use the phrase "data element" or "data elements" to mean a particular piece of information that is associated with an individual. Some examples of data elements include first name, last name, Social Security number, phone number, physical address, zip code, height, weight, blood type, driver's license number, etc.

A. Data Elements from Selected U.S. Federal Statutes

There are a host of U.S. federal statutes that directly implicate privacy.[10] Each statute seeks to regulate a particular business or governmental sector. For example, some statutes regulate the financial sector,[11] other statutes govern the healthcare industry,[12] and still other statutes restrict the federal or state government.[13] Thus, while these sectors collect overlapping data elements (e.g., name, address, telephone number, Social Security number, etc.), oftentimes each sector treats some of the data elements in a noticeably different manner.

Our goal in this section is to identify, if possible, relevant data elements for each statute. Thereafter, we briefly discuss how data categories or data elements are treated, generally.

1. Right to Financial Privacy Act

The Right to Financial Privacy Act ("RFPA") protects an individual's financial records from disclosure, with certain exceptions.[14] Financial records, according to the RFPA, are broadly defined to include "information known to have been derived from . . . any record held by a financial institution pertaining to a customer's relationship with the financial institution,"[15] and any "disclosure of any financial records or information which is not identified with or identifiable as being derived from the financial records of a particular customer."[16] Thus, while the RFPA does not expressly define each of the data elements that are a part of an individual's "financial records," the RFPA prohibits the disclosure of information that can be identified with a particular individual.

Relevant to our paper, one shortcoming of the RFPA is that it does not specify which data elements, either alone or in combination, are

[10] *See, e.g.*, Administrative Procedure Act, 5 U.S.C. §§ 551-559 (2006); Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (2006); Census Confidentiality Statute, 13 U.S.C. § 9 (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2006), 16 C.F.R. § 312 (2009); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006); Video Privacy Protection Act, 18 U.S.C. § 2710 (2006); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2006); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2006); Tax Reform Act, 26 U.S.C. §§ 6103, 6108 (2006); Health Insurance Portability and Accountability Act, 29 U.S.C. §§ 1181-1183 (2006), 42 U.S.C. § 1320a-7c (2006), 45 C.F.R. §§ 160-164 (2009); Health Research Data Statute, 42 U.S.C. § 242m (2006); Criminal Justice Information Systems Act, 42 U.S.C. § 3789g (2006).

[11] *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).

[12] *See, e.g.*, Health Insurance Portability and Accountability Act, 29 U.S.C. §§ 1181-1183 (2006), 42 U.S.C. § 1320a-7c, 45 C.F.R. §§ 160-164 (2009).

[13] *See, e.g.*, Administrative Procedures Act, 5 U.S.C. §§ 551-559 (2006); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2006); Criminal Justice Information Systems Act, 42 U.S.C. § 3789g (2006).

[14] *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3402-3403 (2006).

[15] *Id.* § 3401(2).

[16] *Id.* § 3413(a).

identified or identifiable with a particular individual.

2. Census Confidentiality Statute

The Census Confidentiality Statute ("CCS") prohibits certain governmental entities from "mak[ing] any publication whereby the data furnished by any particular . . . individual . . . can be identified."[17] Similar to the RFPA, the CCS: (a) does not expressly recite each of the data elements that the Census Bureau collects; but (b) generally prohibits publication of personally-identifiable information.

Similar to the RFPA's shortcoming, the CCS also does not indicate which data elements, either alone or in combination, are personally-identifiable data elements.

3. Fair Credit Reporting Act

The Fair Credit Reporting Act ("FCRA") allows disclosure of consumer reports only for statutorily-permissible purposes.[18] The FCRA defines consumer reports to include "any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living . . . ."[19] By including "character, general reputation, personal character, or mode of living," the FCRA broadly prohibits disclosure of personally-identifiable information. And it is this broad application that makes compliance difficult. For example, the general texts of "creditworthy" or "not creditworthy" are not individually identifiable; rather, they are only individually identifiable when combined with an element that identifies the individual. However, as broadly classified here, the terms are prohibited from use in perfectly compliant statistical reporting or other analysis using only that text.

Similar to the CCS and RFPA, the FCRA also suffers from a lack of definition on which data elements, if any, can identify an individual.

4. Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act of 1998 ("COPPA") proscribes collection of personal information of a child.[20] Noticeably different about the COPPA (as compared to the previously-examined statutes) are: (a) COPPA regulates the collection of data (rather than merely regulating the dissemination of data); and (b) COPPA expressly defines data

[17] Census Confidentiality Statute, 13 U.S.C. § 9(a)(2) (2006).
[18] Fair Credit Reporting Act, 15 U.S.C. §§ 1681b, 1681e(a) (2006).
[19] *Id.* § 1681a(d)(1).
[20] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502(a)(1)-(b) (2006).

elements that it considers to be personal information.[21]

The individual data elements that are expressly recited include: first name; last name; home address; other physical address; street name; name of a city; name of a town; email address; telephone number; and Social Security number.[22] By its own terms, the list is not limiting, insofar as the COPPA also prohibits collection of "any other identifier that the Commission determines permits the physical or online contacting of a specific individual . . . ."[23] Moreover, the COPPA also proscribes the collection of information that combines with one or more of the expressly-recited data elements.[24]

5. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") prescribes the conditions under which financial institutions can disclose "nonpublic personal information."[25] Similar to the other privacy statutes implicating personally identifiable information,[26] the GLBA provides a relatively amorphous (and somewhat unhelpful) definition of nonpublic personal information; namely, by defining personally identifiable financial information[27] axiomatically as information that "does not include publicly available information."[28] As such, the GLBA provides no guidance with reference to individual data elements.

6. Electronic Communications Privacy Act

Under the Electronic Communications Privacy Act ("ECPA"), an email or network service provider is prohibited from "knowingly divulg[ing] a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity."[29]

Unfortunately, while the ECPA includes a definitions section,[30]

---

[21] *Id.* § 6501(8)(A)-(G) ("The term 'personal information' means individually identifiable information about an individual collected online, including — (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.").

[22] *Id.* § 6501(8)(A)-(E).

[23] *Id.* § 6501(8)(F).

[24] *Id.* § 6501(8)(G).

[25] Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(a) (2006) ("[A] financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information . . . .").

[26] *Id.* §§ 1681a(d)(1), 6501(8)(A)-(G), 6502(a)(1).

[27] *Id.* § 6809(4)(A).

[28] *Id.* § 6809(4)(B).

[29] Electronic Communications Privacy Act, 18 U.S.C. § 2702(a)(3) (2006).

[30] *Id.* § 2711.

which cross-references the definitions section of the Federal Wiretap Act,[31] neither of these statutory sections provides any definition of the term record. As such, the ECPA is devoid of any definition that explains what data elements, if any, are safe-guarded.

7. Video Privacy Protection Act

Both the Video Privacy Protection Act ("VPPA") and the ECPA can be seen as a sub-category of the Stored Wire and Electronic Communications and Transactional Records Access provisions in Title 18.[32] Yet, we address the VPPA as a separate item because the VPPA appears to define "personally-identifiable information" in a manner that makes little sense with reference to the remainder of the ECPA. Specifically, the VPPA defines personally-identifiable information as "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider . . . ."[33] As one can readily see, the VPPA provides little guidance on what data elements fall within the category of "personally-identifiable information."

8. Driver's Privacy Protection Act

The Driver's Privacy Protection Act ("DPPA") prohibits disclosure of both personal information and highly restricted personal information, except for statutorily-enumerated permissible uses.[34] In doing so, the DPPA is one of the few statutes that both: (a) identifies data elements; and (b) categorizes the identified data elements into distinct categories.

The broad category of personal information is defined as information that identifies an individual, such as an individual's: (a) photograph; (b) Social Security number; (c) driver identification number; (d) name; (e) address (but not the 5-digit zip code); (f) telephone number; and (g) medical or disability information.[35] The DPPA identifies permissible uses for an individual's personal information.

Within the category of personal information are those the DPPA considers to be highly restricted personal information, such as an individual's: (a) photograph or image; (b) Social Security number; and (c) medical or disability information.[36] The permissible uses for this highly restricted personal information are a much smaller subset than the uses permitted for non-highly restricted but personal information.

---

[31] *Id.* § 2510.
[32] *See* Video Privacy Protection Act, 18 U.S.C. §§ 2701-2712 (2006).
[33] *Id.* § 2710(a)(3).
[34] Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2006).
[35] *Id.* § 2725(3).
[36] *Id.* § 2725(4).

Data elements that are specifically excluded from personal information include: (a) information on vehicular accidents; (b) driving violations; and (c) driver's status.[37] For these categories, it appears there are no restrictions on disclosure or use.

The DPPA expressly recites data elements that fall within three specific categories, namely: (a) highly restricted personal information; (b) personal information that is not highly restricted; and (c) information that is not subject to disclosure restrictions. In doing so, the DPPA provides much more than the amorphous descriptions found in many other statutes.

9. Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act ("FERPA") prohibits publication of directory information of a minor student, unless the parents of the minor student have been afforded the opportunity to object to the publication of the directory information.[38] In other words, the FERPA provides an opt-out mechanism for directory information. This directory information under FERPA includes a student's: (a) name; (b) address; (c) telephone listing; (d) date of birth; (e) place of birth; (f) major field of study; (g) participation in officially recognized activities and sports; (h) weight and height of members of athletic teams; (i) dates of attendance; (j) degrees and awards received; and (k) most recent previous educational agency or institution attended by the student.[39]

In the companion section on the protection of pupil's rights,[40] the statute prohibits compelling a student to divulge: (1) political affiliations or beliefs of the student or the student's parent; (2) mental or psychological problems of the student or the student's family; (3) sex behavior or attitudes; (4) illegal, anti-social, self-incriminating, or demeaning behavior; (5) critical appraisals of other individuals with whom respondents have close family relationships; (6) legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; (7) religious practices, affiliations, or beliefs of the student or the student's parent; or (8) income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).[41] It should, however, be noted a student may voluntarily provide this information.

Also, "[a]ctivities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or

---

[37] *Id.* § 2725(3).
[38] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(5)(B) (2006).
[39] *Id.* § 1232g(a)(5)(A).
[40] *Id.* § 1232h.
[41] *Id.* § 1232h(b).

for selling that information" require notification (i.e., an opportunity to opt-out).[42] Under this section, personal information is defined as individually-identifiable information, including: "(i) a student or parent's first and last name; (ii) a home or other physical address (including street name and the name of the city or town); (iii) a telephone number; or (iv) a Social Security identification number."[43] With the exception of one data element (email address), these elements are identical to those found in the COPPA. Also, these elements have substantial overlap with the highly restricted personal information found in the DPPA.

One should appreciate the treatment of these data elements under FERPA (i.e., opt-out mechanism for disclosure) is markedly different than the treatment of similar data elements under DPPA (i.e., verifiable consent needed for disclosure, or "opt-in").

10. Tax Reform Act

The Tax Reform Act ("TRA") requires all return information to be confidential, except as authorized by the TRA.[44] Under the definitions section of the TRA, return information is defined as, among other things: (a) "a taxpayer's identity"; (b) "the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments"; (c) "whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing"; or (d) "any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense . . . ."[45] The TRA further defines taxpayer identity as the taxpayer's name, address, taxpayer identifying number, or any combination thereof.[46]

Excluded from a taxpayer's return information is "data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer."[47] Additionally, the TRA prohibits disclosure of statistics from any collected information that "shall in any manner permit the statistics . . . to be associated with, or otherwise identify, directly or indirectly, a particular taxpayer."[48]

---

[42] *Id.* § 1232h(c)(2)(C)(i).
[43] *Id.* § 1232h(c)(6)(E).
[44] Tax Reform Act, 26 U.S.C. § 6103(a) (2006).
[45] *Id.* § 6103(b)(2)(A).
[46] *Id.* § 6103(b)(6).
[47] *Id.* § 6103(b)(2).
[48] *Id.* § 6108(c).

In short, the TRA permits the collection of a taxpayer's information and the statistical analysis of the collected information. However, the TRA prohibits disclosures that can associate a particular data element with a particular taxpayer, unless that disclosure is expressly permitted by the TRA.

The data elements the TRA shares with other statutes include name, address, and Social Security number (referenced more broadly in the TRA as taxpayer identifying number). But, because the TRA is directed to a particular governmental sector (i.e., tax), the TRA recites numerous data elements that are not germane to other sectors.

11. Health Insurance Portability and Accountability Act

One of the more publicized statutes, the Health Insurance Portability and Accountability Act ("HIPAA"), requires covered entities to "protect[] the confidentiality of the information and the privacy of individuals receiving health care services and items."[49] In the administrative rules promulgated under the HIPAA, covered entities are required to maintain safeguards against unauthorized disclosure of protected health information, which is defined as individually identifiable health information.[50] In an axiomatic statement, the regulations exclude from individually identifiable health information any "information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual . . . ."[51]

Relevant to this paper, the HIPAA recites an extensive list of data elements (referred to in the HIPAA as "identifiers"), which the regulations require to be removed for certain types of disclosures.[52] The list in 45

---

[49] Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320a-7c(a)(3)(B)(ii) (2006).
[50] 45 C.F.R. § 160.103 (2009).
[51] *Id.* § 164.514(a).
[52] *Id.* § 164.514(b)(2)(i), which recites:

> A covered entity may determine that health information is not individually identifiable health information only if . . . [t]he following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
>
> (A) Names;
>
> (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
>
> *(1)* The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
>
> *(2)* The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
>
> (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,

C.F.R. § 164.514(b)(2)(i) is duplicated, almost in its entirety, in another section of the regulation, where limited data sets that fall outside of the realm of protected health information are defined.[53]

Hence, with reference to the healthcare sector, the HIPAA both: (a) expressly recites a plethora of data elements (called "direct identifiers" in the HIPAA); and (b) provides specific guidelines on how those data elements are to be treated within the healthcare sector.

12. Health Research Data Statute

The Health Research Data Statute ("HRDS") restricts the use of

---

discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section . . . .

[53] *Id.* § 164.514(e)(2), which defines a limited data set as follows:

A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
(i) Names;
(ii) Postal address information, other than town or city, State, and zip code;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses;
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resource Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints; and
(xvi) Full face photographic images and any comparable images.

information "if an establishment or person supplying the information or described in it is identifiable . . . ."[54] Other than proscribing the use of information in such general terms, the HRDS provides no guidance on what data elements, if any, are considered to be "identifiable" information.

13. Criminal Justice Information Systems Act

The Criminal Justice Information Systems Act ("CJISA") restricts the use of several categories of information, including research or statistical information,[55] criminal history information,[56] and criminal intelligence information.[57] Of these three categories, the CJISA only defines criminal history information.[58] The specific data elements included in the CJISA's criminal history information are "records of arrests, the nature and disposition of criminal charges, sentencing, confinement, rehabilitation, and release . . . ."[59]

14. Administrative Procedures Act

The Administrative Procedures Act ("APA") provides detailed procedures on maintaining and disclosing an individual's record.[60] As defined by the APA, an individual's record means

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph . . . .[61]

While not directly applicable to this paper, it is worthwhile to note that, for some of the disclosures mandated under the APA, the decision on whether or not to remove identifying details from the record are optional and not mandatory.[62]

---

[54] Health Research Data Statute, 42 U.S.C. § 242m(d) (2006).
[55] Criminal Justice Information Systems Act, 42 U.S.C. § 3789g(a) (2006).
[56] *Id.* § 3789g(b).
[57] *Id.* § 3789g(c).
[58] *Id.* § 3791(a)(9) ("'[C]riminal history information' includes records and related data, contained in an automated or manual criminal justice informational system, compiled by law enforcement agencies for the purpose of identifying criminal offenders and alleged offenders and maintaining as to such persons records of arrests, the nature and disposition of criminal charges, sentencing, confinement, rehabilitation, and release . . . .").
[59] *Id.*
[60] Administrative Procedures Act, 5 U.S.C. § 552a (2006).
[61] *Id.* § 552a(a)(4).
[62] *See, e.g.*, *id.* § 552(a)(2) ("To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details . . . .") (emphasis added).

B. Data Elements from Selected U.S. State Laws

The complication from this sector-by-sector treatment of data elements in the federal statutes is compounded by the fact individual states also promulgate statutes to address personally identifiable information.[63] Thus, in addition to variability in the treatment of private information from business-sector to business-sector, there exists variability in the treatment of private information from state to state.

Since many of the data elements from the federal laws overlap with the data elements in state laws, we intentionally focus only on those statutes that recite data elements that are absent from the federal statutes.[64] Additionally, because California appears to have the most extensive privacy laws,[65] we limit our review to California,[66] with the presumption other

---

[63] By way of example, the state laws that touch on privacy include: bank records statutes; cable television statutes; common law remedies for invasion of privacy; public disclosure of privacy facts, defamation, and breach of duty of confidentiality; computer crime statutes; credit reporting statutes; criminal justice information statutes; employment records statutes; fair information practices statutes; genetic information statutes; insurance records statutes; media shield statutes; medical records statutes; polygraph test statutes; privilege statutes (e.g., attorney-client privilege, patient-doctor privilege, priest-penitent privilege, etc.); school records statutes; stored wire communications statutes; tax return statutes; telephone/facsimile solicitation; uniform commercial code; video privacy statutes; and wiretap statutes.

[64] We note that a vast number of California statutes recite overlapping data elements, as those recited in corresponding federal statutes. For example, various portions of California's Penal Code restrict use of Social Security numbers, bank account numbers, etc. Since the goal is to identify unique data elements, we omit any duplicative items in our analysis of California law.

[65] *See* CAL. BUS. & PROF. CODE §§ 17529, 17538.41, 17590-17594 (West 2008) (computer and phone anti-spam); CAL. BUS. & PROF. CODE §§ 22575-22579 (West 2008), CAL. GOV'T CODE §§ 6254.21, 11015.5 (West 2008) (online privacy); CAL. BUS. & PROF. CODE §§ 22947-22947.6 (West 2008) (computer virus); CAL. BUS. & PROF. CODE §§ 22948-22948.3 (West 2008) (anti-"phishing"); CAL. CIV. CODE § 1708.8 (West 2009) (invasion of privacy); CAL. CIV. CODE §§ 1725, 1747.05, 1747.06, 1747.08, 1747.09 (West 2009) (credit cards); CAL. CIV. CODE §§ 1748.10-1748.12 (West 2009) (information used for marketing); CAL. CIV. CODE §§ 1749.60-1749.66 (West 2009) (personal information by supermarket clubs); CAL. CIV. CODE §§ 1785.1-1785.36, 1786-1786.60 (West 2009) (consumer credit reporting); CAL. CIV. CODE §§ 1788-1788.33 (West 2009) (fair debt collection practices); CAL. CIV. CODE §§ 1798-1798.29 (West 2009) (state data collection and disclosure); CAL. CIV. CODE § 1798.24 (West 2009), CAL. WELF. & INST. CODE § 10850 (West Supp. 2010) (personal information for research); CAL. CIV. CODE §§ 1798.29, 1798.82, 1798.84 (West 2009) (security breach notice); CAL. CIV. CODE §§ 1798.79-1798.795 (West 2009) (RFID interception); CAL. CIV. CODE §§ 1798.80-1798.81, 1798.81.5, 1798.83-1798.84 (West 2009) (personal information in business records); CAL. CIV. CODE § 1798.90.1 (West 2009) ("swiping" of driver's license information); CAL. CIV. CODE § 1798.91 (West 2009) (medical information for marketing purposes); CAL. CIV. CODE § 1799.1b (West 2009) (address change information); CAL. CIV. CODE § 1936 (West Supp. 2010) (rental car onboard electronic surveillance); CAL. CIV. CODE § 52.7 (West Supp. 2010) (implant devices); CAL. CIV. CODE §§ 56-56.37 (West 2007 & Supp. 2010) (medical records); CAL. CIV. PROC. CODE § 674 (West 2009), CAL. FAM. CODE § 2024.5 (West 2004), CAL. REV. & TAX. CODE § 2191.3 (West Supp. 2010), CAL. CIV. CODE §§ 1798.85-1798.89, 1785.11.1, 1785.11.6 (West 2009), CAL. COM. CODE § 9526.5 (West Supp. 2010), CAL. EDUC. CODE § 66018.55 (West Supp. 2010), CAL. GOV'T CODE §§ 27300-27307 (West 2008), CAL. LAB. CODE § 226 (West 2010) (Social Security Number); CAL. EDUC. CODE §§ 89090-89090.5, 92630 (West Supp. 2010) (alumni information); CAL. ELEC. CODE §§ 2166.7, 2194, 8023, 8105, 8202, 8204 (West Supp. 2010), CAL. GOV'T CODE § 6254.24 (West 2008) (voter privacy); CAL. FIN. CODE §§ 4050-4060 (West Supp. 2010) (financial privacy); CAL. FIN. CODE § 4100 (West Supp. 2010) (bank account number reuse); CAL. GOV'T CODE § 11019.9 (West 2005) (state privacy policy); CAL. GOV'T CODE §§ 6218-6218.05 (West 2008) (information of reproductive health care providers); CAL. GOV'T CODE §§ 6250-6268 (West 2008) (public records act); CAL. GOV'T CODE §§ 6254, 6267, 6276.28 (West 2008) (registration and circulation records for libraries); CAL. HEALTH & SAFETY CODE §§ 102230-102232, 103525-103528 (West 2006) (birth and death records); CAL. HEALTH & SAFETY

jurisdictions will recite similar (if not identical) data elements for their corresponding statutes. With that said, we now turn to these California statutes to identify any data elements that are not expressly recited in the federal statutes.[67]

California's vehicle code section restricts the use of vehicle data recorders,[68] which track the following data elements related to an individual's vehicle: (a) speed; (b) direction; (c) locations visited; (d) steering performance; (e) brake performance; (f) seatbelt use; and (g) accident information.[69]

California also requires protection of confidential personal information for crime victims,[70] which California's Penal Code defines as including: (a) place of employment; (b) employee identification number; (c) mother's maiden name; (d) demand deposit account number; (e) savings account number; (f) checking account number; and (g) credit card number.[71]

The California Penal Code recites additional data elements with reference to bank account access cards, which include: (a) computer password; (b) access code; (c) debit card number; (d) bank account number;

CODE §§ 120975-121020 (West 2006) (AIDS testing); CAL. HEALTH & SAFETY CODE §§ 1280.15, 123110-123149.5 (West 2006 & West Supp. 2010) (patient records); CAL. INS. CODE §§ 791-791.28 (West 2005) (insurance information); CAL. PENAL CODE §§ 293, 964 (West 2008 & West Supp. 2010), CAL. CIV. CODE § 1798.79.8 (West 2009), CAL. GOV'T CODE § 6254 (West 2008) (personal information of victims); CAL. PENAL CODE §§ 4017.1, 5071 (West Supp. 2010), CAL. WELF. & INST. CODE § 219.5 (West 2008) (inmate jobs that give access to personal information); CAL. PENAL CODE § 502 (West Supp. 2010) (computer crimes); CAL. PENAL CODE § 502.6 (West Supp. 2010) (credit card "skimming"); CAL. PENAL CODE §§ 629.50-629.98, 630-638 (West 1999 & West Supp. 2010) (electronic eavesdropping by government); CAL. PUB. UTIL. CODE § 2891.1 (West Supp. 2010) (cell phone directories); CAL. PUB. UTIL. CODE §§ 2891-2894.10 (West Supp. 2010), CAL. PENAL CODE § 638 (West 1999) (prohibits utilities from disclosing telephone calling patterns); CAL. VEH. CODE §§ 11713.3, 11713.25 (West Supp. 2010) (personal information in automobile dealers' computers); CAL. VEH. CODE §§ 1808-1821 (West 2000) (personal information from Department of Motor Vehicles); CAL. VEH. CODE §§ 40303, 40305, 40305.5, 40500, 40504 (West Supp. 2010), CAL. PENAL CODE §§ 182, 186.2, 529.7, 530.5-530.8, 786, 853.5-853.6 (West Supp. 2010), CAL. CIV. CODE §§ 1748.95, 1788.2, 1788.18, 1798.92-1798.97 (West 2009), CAL. FIN. CODE §§ 4002 and 22470 (West Supp. 2010) (identity theft); CAL. VEH. CODE § 9951 (West Supp. 2010) (vehicle data recorder); CAL. WELF. & INST. CODE § 5328 (West Supp. 2010) (psychiatric records).

[66] Indeed, California's State Constitution expressly recites "privacy" as an "inalienable right." CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."). To advance the State's constitutional guarantee of privacy, California established a State Office of Privacy Protection. CAL. GOV'T CODE § 11549.5(a) (West Supp. 2010) ("The purpose of the Office . . . is to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect [consumer] privacy . . . to ensure the trust of the residents of this state.").

[67] For all practical purposes, any company that operates nationwide or that has an Internet presence will be required to adhere to the most restrictive privacy laws. Thus, while California's privacy laws are theoretically limited to California's territorial boundaries, in practice California effectively dictates the privacy law for all other states within the Union. For this reason, a review of California law is, in effect, a review of the privacy law for all fifty states.

[68] CAL. VEH. CODE § 9951(c) (West Supp. 2010).

[69] *Id.* § 9951(b).

[70] CAL. PENAL CODE § 964(a) (West 2008).

[71] *Id.* § 964(b).

and (e) numbering or coding which is employed in the issuance of access cards.[72] With reference to electronic eavesdropping by cable and television operators, California's Penal Code adds the following data elements: (a) television viewing habits; (b) shopping choices; and (c) energy uses.[73]

To this already-growing list of data elements, California's consumer credit reporting laws add: (a) past delinquencies; (b) late payment history; (c) irregular payment history; (d) insolvency; and (e) any form of default information.[74] Furthermore, the California Business and Professions Code add purchase history and websites visited to the list of data elements.[75]

Insofar as data elements from other California statutes appear to be duplicative of the data elements already recited, those statutes are not discussed here.

III. SYNTHESIS OF CONCEPTS COMMON TO PRIVACY LAWS

Having identified many data elements present in both federal and state statutes, we now provide some general observations on how state and federal entities address these data elements.

Broadly, these privacy statutes fall into one of four distinct structures, based on how the statutes are written. We discuss each of these structures in turn.

A. Structure-1: Two Classes with No Specific Recitation of Data Elements

The first structure (referred to herein as "Structure-1") includes statutes that define two classes of data (protected and unprotected), but do not provide useful guidance on how to determine which data element falls within which class. One example of this type of statute is the Right to Financial Privacy Act ("RFPA"), which protects financial records but does not expressly define each of the data elements that are a part of an individual's financial records.[76]

Structure-1 statutes may be sufficient for easily-classifiable data elements. For example, even without specific guidance, one can readily decide a bank account number is a protected financial record, while a county of residence is not a protected financial record.

However, because Structure-1 statutes provide little guidance on which data elements fall squarely within the protected class, they become problematic for data elements that are not so easily classifiable. For

---

[72] *Id.* § 484j (West 1999).
[73] *Id.* § 637.5(a)(2) (West Supp. 2010).
[74] CAL. CIV. CODE § 1785.26(a)(2) (West 2009).
[75] CAL. BUS. & PROF. CODE § 22947.1(k)(5)(D), (G) (West 2008).
[76] *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (2006).

example, it is unclear whether an individual's income, standing alone, would be a protected class data element or an unprotected class data element. Due to this deficiency, we avoid the Structure-1 format in our proposed omnibus privacy statute.

B. Structure-2: Three Classes with No Specific Recitation of Data Elements

The second structure (referred to herein as "Structure-2") includes statutes that define three classes of data (highly-protected, somewhat protected, and unprotected), but do not provide useful guidance on how to determine which data element falls within which class. One example of this type of statute is the Criminal Justice Information Systems Act ("CJISA"). As noted above, the CJISA recites several categories of information, including research or statistical information,[77] criminal history information,[78] and criminal intelligence information.[79] However, the CJISA provides little guidance on which data elements fall within the research or statistical information or criminal intelligence information.

Structure-2 statutes suffer from the same deficiency as Structure-1 statutes, and for this reason we also avoid the Structure-2 format in our proposed omnibus privacy statute.

C. Structure-3: Two Classes and a Specific Recitation of Data Elements

The third structure (referred to herein as "Structure-3") includes statutes that define two classes of data (protected and unprotected), and also recite examples of specifically protected data elements. Catetory-3 statutes include the Children's Online Privacy Protection Act of 1998 ("COPPA") and the Health Insurance Portability and Accountability Act ("HIPAA").

As noted above, COPPA: (a) defines a protected class of data, which it designates as personal information; and (b) expressly identifies data elements it considers to be personal information, which includes (but is not limited to) first name, last name, home address, other physical address, street name, name of a city, name of a town, email address, telephone number, and Social Security number.[80]

HIPAA also: (a) defines a protected class of data, which it designates as protected health information; and (b) expressly identifies data elements (referred to in the HIPAA as identifiers) it considers to be protected health information,[81] which includes (but is not limited to) names, street addresses, cities, counties, precincts, zip codes, birth date, admission

[77] Criminal Justice Information Systems Act, 42 U.S.C. § 3789g(a) (2006).
[78] *Id.* § 3789g(b).
[79] *Id.* § 3789g(c).
[80] Child Online Privacy Protection Act of 1998, 15 U.S.C. § 6501(8)(A)-(E) (2006).
[81] 45 C.F.R. § 164.514(b)(2)(i) (2009).

date, discharge date, date of death, telephone numbers, fax numbers, email addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, license plate numbers, device identifiers and serial numbers, web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers, and biometric identifiers (e.g., finger prints and voice prints, and full face photographic (and any comparable) images).[82]

This binary nature of Structure-3 statutes provides a simple classification of data elements. Also, insofar as Structure-3 statutes provide a specific recitation of protected data elements, they remove much of the ambiguity present in both Structure-1 and Structure-2 statutes.

One deficiency in a Structure-3 statute is its binary classification is very coarse. Thus, a Structure-3 statute inherently forces any mid-level sensitive information into a higher level of classification than necessary. While this may not be problematic for the private sector, this becomes somewhat problematic for the government sector because it removes much of the government's transparency to its own citizens by prohibiting disclosure of more information than is necessary.[83]

D. Structure-4: Three Classes and a Specific Recitation of Data Elements

The last structure (referred to herein as "Structure-4") includes statutes that define three classes of data (highly-protected, somewhat-protected, and unprotected) and also recites examples of specifically-protected data elements for each of these data classes. Structure-4 statutes include the Driver's Privacy Protection Act ("DPPA").

The DPPA: (a) identifies data elements; and (b) categorizes the identified data elements into one of three distinct categories. The broad category of personal information is defined as information that identifies an individual, such as an individual's: (a) "photograph"; (b) "social security number"; (c) "driver identification number"; (d) "name"; (e) "address (but not the 5-digit zip code)"; (f) "telephone number"; and (g) "medical or disability information . . . ."[84] Within the category of personal information are those data elements the DPPA considers to be highly restricted personal information, such as an individual's: (a) "photograph or image"; (b) "Social Security number"; and (c) "medical or disability information . . . ."[85] The DPPA also recites data elements specifically excluded from personal

[82] *Id.*

[83] The issue of whether the federal government or the state governments should collect personally identifiable information on its own citizens is beyond the scope of this paper. We proceed with our analysis with the presumption that personally identifiable data is collected, with the only question being how it should be treated (both during collection and archiving).

[84] Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2725(3) (2006).

[85] *Id.* § 2725(4).

information, such as: (a) information on vehicular accidents; (b) driving violations; and (c) driver's status.[86] In short, the DPPA expressly recites specific data elements that fall within three specific categories, namely: (a) highly restricted personal information; (b) personal information that is not highly restricted; and (c) information that is not subject to disclosure restrictions.

The ternary structure employed by the DPPA provides a finer classification than the coarser binary-classification of Structure-3 statutes. As such, Structure-4 statutes address the deficiency of Structure-3 statutes while also remedying the ambiguity of the Structure-1 and Structure-2 statutes.

E. Miscellaneous Issues

Before proceeding to our model omnibus privacy statute, we address some peripherally-related issues. First, it seems intuitive that if a ternary classification is better than a binary classification, then a finer data class resolution (i.e., four data classes, five data classes, one hundred data classes, etc.) would be even better. However, we note our goal is to achieve uniformity in the treatment of data across many sectors, and increasing the data class resolution contravenes uniformity. For this reason, we truncate the number of data classes to three.[87]

Next, since the purpose of collecting information will be different between sectors, we purposely craft the omnibus statute to allow for different sector-by-sector uses, so long as the classifications of (and consequently the protections afforded to) the data elements are uniform across all sectors. In other words, the proposed statute dictates a uniform classification and protection of data elements, but does not dictate the purposes for which the categorized data elements are used within any particular sector. By narrowly focusing on only classification and protection, the proposed statute allows vast freedom within each sector to use the collected data for that sector's particular purpose, as long as the required protections are met.

Lastly, we note others may disagree with our classification of each data element (as proposed below). Thus, we fully recognize reasonable minds can disagree on which data elements deserve more protection and which data elements deserve less protection. With this in mind, we err by being overly protective for data elements that (arguably) fall into multiple data classes.

---

[86] *Id.* § 2725(3).

[87] We fully admit that our selection of three classes (rather than four or more classes) is somewhat arbitrary. However, we did not go beyond three data classes because none of the currently-reviewed statutes went beyond three data classes.

It is also important to reestablish this analysis is element driven. Therefore, when considering an element's risk classification (e.g., high-risk, medium-risk, or low-risk), the element is considered in isolation and not in combination with other elements. This combination can directly impact whether the element remains individually identifiable and thus whether the associated risk may change.[88] It is for this reason an entity's policies on information collection and use clearly define how each element or category of elements will be used to ensure accountability for elevated risk associated with these elements as a result of combination.

With that said, we now propose our model omnibus privacy statute.

IV. PROPOSED FEDERAL OMNIBUS PRIVACY STATUTE

(a) Short Title

(1) This chapter shall be known as the "Federal Omnibus Privacy Act."

(b) Congressional Findings

(1) The Congress finds that different entities in various sectors (business and government) collect information from individuals;

(2) The Congress further finds that substantially similar information is collected from individuals, even though the information may be collected for different purposes;

(3) The Congress further finds that sometimes the treatment of collected information varies from sector to sector;

(4) It is the purpose of this chapter to provide uniformity in the collection and treatment of information across these various sectors.

(c) Definitions

(1) "**agent**" means employee, officer, director, or any other entity that acts on behalf of, or receives direction from, an organization, whether that entity be internal to the organization or external to the organization.

---

[88] While not consulted for purposes of this article, essential to the discussion of the categorization of elements is the statistical analysis of such data elements and their likelihood of combination across publicly available and private data sets in the digital age. *See, e.g.,* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATISTICAL POLICY WORKING PAPER 22 (SECOND VERSION, 2005): REPORT ON STATISTICAL DISCLOSURE LIMITATION METHODOLOGY (2005).

(2) "**aggregate**" means to combine data elements in any manner.

(3) "**collect**" means to request, accumulate, gather, or otherwise obtain. Collection precedes either "use" or "sharing."

(4) "**data element**" means information that is, standing alone, distinct. An original and a copy of any data element shall be treated in the same manner. Every data element falls within one of the following mutually-exclusive classes: (i) high-risk data element; (ii) mid-risk data element; and (iii) low-risk data element.

(5) "**high-risk data element**" means a data element that, standing alone, has the ability to: (i) identify an individual; and/or (ii) expose an individual to either economic or non-economic harm as a result of unauthorized disclosure. Examples of high-risk data elements include:

(A) access code (e.g., passwords, personal identification number (PIN), etc.);

(B) account number (e.g., bank account, checking account, credit card account, debit account, demand deposit account, savings account, etc.);

(C) address (home address, other physical address, street name, street number, zip code);

(D) biometric identifier (e.g., fingerprint, voiceprint, DNA, etc.);

(E) device identifier (e.g., device serial number, Media Access Control (MAC) address, Internet Protocol (IP) address, Universal Resource Locator (URL), etc.);

(F) email address;

(G) employment (e.g., current employer, employment history, previous employer, etc.);

(H) fax number;

(I) financial transactions (e.g., deposits, withdrawals, fund transfers, etc.);

(J) images (e.g., photograph);

(K) medical information (e.g., health plan beneficiary number, medical history, mental problems, psychological problems, health problems, disability information, etc.);

(L) name (e.g., first name, last name, mother's maiden name, etc.);

(M) privileged information (e.g., attorney-client, priest-penitent, doctor-patient, psychiatrist-patient, etc.);

(N) telephone number;

(O) unique identifying characteristic, code, or number (e.g., driver's license number, employee identification number, Social Security number, taxpayer identification number, medical record number, or any other identifying characteristic, identification code, identification number, or identification symbol that is assigned to an individual); and

(P) vehicle identifiers (e.g., vehicle serial number, license plate number, etc.).

(6) "**de-identification**" means to render information not individually identifiable.

(7) "**encrypt**" means to transform information using a cipher to make the information only readable to those possessing a deciphering key.

(8) "**essential business purpose**" means a purpose directly related to the reason that an individual provided a data element.

(9) "**low-risk data element**" means a data element that is behavioral or attributable to a population as much as it is attributable to any individual. No high-risk or medium-risk data elements are contained within the set of low-risk data elements. Examples of low-risk data elements include:

(A) activities (e.g., sports, clubs, events, etc.);

(B) awards;

(C) behavioral characteristics[89] (e.g., anti-social behavior, demeaning behavior, illegal behavior, self-incriminating behavior, etc.);

(D) default (financial);

(E) driver's status;

(F) education (e.g., degrees, academic institutions, major field of study, etc.);

(G) eye color;

(H) hair color;

(I) height;

(J) vehicle performance information (e.g., brake performance, direction of travel, seatbelt use, vehicle speed, vehicle steering performance, etc.); and

(K) weight.

(10) "**mid-risk data element**" means a data element that, when combined with at least one other data element, has the ability to: (i) identify an individual; and/or (ii) expose an individual to economic or non-economic harm. Examples of mid-risk data elements include, but are not limited to:

(A) city or town (e.g., city of residence, city of employment, city of birth, etc.);

(B) criminal history (e.g., accident information, confinement, disposition of criminal charges, driving violations, nature of criminal charges, penalties, record of arrests, rehabilitation information, release, sentencing, etc.);

(C) consumer characteristics[90] (e.g., consumer credit capacity, consumer credit standing, consumer credit worthiness, consumer's general reputation, consumer's mode of

[89] Characteristics can often be presumed to be individually identifiable. This is not always the case. Whether or not someone is creditworthy is not, by itself, individually identifiable. However, when combined with another element such as age, gender and 5-digit zip code, the characteristic may take on individually identifiable properties.

[90] *See id.* and accompanying text.

living, consumer's personal characteristics, credit and debt payment amounts, credit and debt payment history, insolvencies, interest payments, past delinquencies, purchase or payment receipts, etc.);

(D) county (e.g., county of residence, county of employment, county of birth, etc.);

(E) dates (e.g., date of birth, date of death, dates of attendance, date of admittance, date of discharge, etc.);

(F) political information (e.g., political affiliations, political beliefs, voting history, voting precinct, etc.);

(G) religious information (e.g., religious affiliations, religious beliefs, religious practices, etc.);

(H) sex (e.g., sexual orientation, attitudes, behavior, etc.);

(I) tax information (e.g., assets, exemptions, forfeitures, income, tax credits, tax deductions, tax deficiencies, tax liabilities, tax overassessments, tax payments, taxes withheld, tax penalties, fines, net worth, past delinquencies, tax payment history, tax receipts, etc.); and

(J) vehicle locations visited.

(11) "**organization**" means any business or governmental entity, including but not limited to a corporation, a partnership, a limited liability company, a governmental agency, a sole proprietorship, and any other entity that collects and uses the subject data elements as it transacts business.

(12) "**retain**" means to keep, store, or otherwise maintain in any manner as to permit use.

(13) "**security permission**" means authorization granted to access information.

(14) "**share**" means to transmit, distribute, disseminate, convey, transfer or otherwise disclose in any manner to an entity that is external to an organization.

Sharing follows collection.

(15) "**use**" means to access, copy, retrieve, combine, disclose, truncate, alter, or otherwise process in any manner solely within an organization. Any use of data elements external to the organization shall be considered to be sharing of the data elements. Use follows collection.

(d) High-Risk Data Elements

(1) **General Requirements**: Any organization that collects, uses, and/or shares high-risk data elements must have clearly-established and published policies and procedures[91] for collecting, using, and/or sharing the high-risk data elements by the organization and any of its agents. These policies and procedures must clearly explain the organization's essential business purposes for collecting, using, and/or sharing the high-risk data elements.

(2) **Requirements for Collecting High-Risk Data Elements**: Any organization that collects high-risk data elements from any individual:

(A) Must identify the high-risk data elements that are being collected;

(B) Must provide clear notice to the individual that the individual is sharing high-risk data elements with the organization;

(C) Must clearly explain the organization's essential business purposes for collecting the individual's high-risk data elements;

(D) Must affirmatively obtain verifiable consent from the individual to collect the high-risk data elements; and

(E) Must provide a copy of, or access to, the organization's policies and procedures to the individual.

[91] Policies and procedures can be both internal and external to a company. Thus, the use of the terms here specifies those a customer should expect to see published. The use of the terms in this context is not meant to suggest a company should disclose all of its data processing policies and procedures, but rather those that a customer must understand prior to consenting to the use of his/her personally identifiable information.

(3) **Requirements for Using High-Risk Data Elements**:

(A) **Essential Business Purposes and Restricted Actors**: An organization may freely use an individual's high-risk data elements without informing the individual or obtaining consent from the individual only if both of the following two (2) conditions are met:

(i) **Limited Access**: Only agents that are internal to an organization and who have predefined job titles or predefined security permissions establishing a "need to know"[92] may use the individual's high-risk data elements; and

(ii) **Limited Purpose**: An organization may use the individual's high-risk data elements only for the organization's essential business purposes, which have been clearly conveyed to the individual prior to the organization's use of the high-risk data elements.

(B) **Restricted Actors and Other Business Uses**: An organization may use an individual's high-risk data elements for a use other than an essential business purpose, provided, however, that the organization:

(i) Must limit use of the high-risk data elements to only the organization's agents that are internal to the organization and who have predefined job titles or predefined security permissions;

(ii) Must provide clear notice to the individual that the individual's high-risk data elements are being used for a purpose other than an essential

[92] "Need to know" is a generally accepted tenant of privacy compliance supporting a "minimum use" policy. Personally identifiable information should be minimally used only to the extent necessary to accomplish the business purpose for which it was collected. This includes minimizing access to this information to only those in an organization who are essential to executing that business purpose.

business purpose, to include providing a detailed explanation to the individual of the purposes for which the individual's high-risk data elements are being used;

(iii) Must identify the individual's high-risk data elements that are being used for those purposes;

(iv) Must obtain verifiable consent from the individual to use the high-risk data elements for those purposes; and

(v) Must de-identify the high-risk data elements prior to those uses.

(C) **Limitations on Data Retention**: An organization shall not retain high-risk data elements, except for:

(i) **Retention Period**: a period of time that is necessary to accomplish the business purpose for which the high-risk data elements were collected or is required by law; and

(ii) **Encrypted Retention**: in an encrypted form at the most secure encryption level that is commercially reasonable for the organization's industry.

(4) **Requirements for Sharing High-Risk Data Elements**: For an organization to share an individual's high-risk data elements, the organization:

(A) Must determine that sharing the high-risk data elements is reasonably necessary to advance an essential business purpose of the organization and that there is no reasonable alternative to accomplishing the organization's essential business purpose without sharing the individual's high-risk data elements;

(B) Must ensure that the entity with which the organization will share the high-risk data elements has clearly-established and

published policies and procedures that are not less protective of the high-risk data elements than the organization's policies and procedures;

(C) Must provide clear notice to the individual that the individual's high-risk data elements will be shared;

(D) Must identify the entity with which the organization will share the individual's high-risk data elements;

(E) Must provide a detailed explanation to the individual on why it is necessary to share the individual's high-risk data elements;

(F) Must identify the individual's high-risk data elements that are being shared;

(G) Must affirmatively obtain verifiable consent from the individual to share the high-risk data elements;

(H) Must, if possible, de-identify the high-risk data elements prior to sharing the high-risk data elements; and

(I) Must encrypt the high-risk data elements at the most secure encryption level that is commercially reasonable for the organization's industry prior to sharing the high-risk data elements.

(e) Mid-Risk Data Elements

(1) **General Requirements**: Any organization that collects, uses, and/or shares any mid-risk data elements must have clearly-established and published policies and procedures for collecting, using, and/or sharing the mid-risk data elements by the organization and/or any of its agents. These policies and procedures must clearly explain the organization's essential business purposes for collecting, using, and/or sharing the mid-risk data elements.[93]

[93] We support using existing models for information collection, such as the Fair Information Practice Principles, to govern these procedural requirements. *See* FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES (June 25, 2007), http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

(2) **Requirements for Collecting Mid-Risk Data Elements**: Any organization that collects mid-risk data elements from any individual:

(A) Must identify the mid-risk data elements that are being collected;

(B) Must provide clear notice to the individual that the individual is sharing mid-risk data elements with the organization;

(C) Must affirmatively obtain verifiable consent from the individual to collect the mid-risk data elements; and

(D) Must provide a copy of, or access to, the organization's data collection policies and procedures to the individual.

(3) **Requirements for Using Mid-Risk Data Elements**:

(A) **Essential Business Purpose**: An organization may use mid-risk data elements for the organization's essential business purpose without informing the individual or obtaining consent from the individual;

(B) **Aggregation and Research**: An organization may freely use mid-risk data elements for aggregation or research without informing the individual or obtaining consent from the individual, provided, however, that the organization must de-identify the mid-risk data elements prior to aggregation or research.

(C) **All Uses Other than for Essential Business Purposes**: For any use of an individual's mid-risk data elements other than an essential business purpose the organization:

(i) Must provide clear notice to the individual that the individual's mid-risk data elements are being used for a purpose other than an essential business purpose;

(ii) Must provide a detailed explanation to the individual of the purposes for

which the individual's mid-risk data elements are being used;

(iii) Must identify the individual's mid-risk data elements that are being used for those purposes; and

(iv) Must affirmatively obtain verifiable consent from the individual to use the mid-risk data elements for those purposes.

(4) **Requirements for Sharing Mid-Risk Data Elements**: An organization may share an individual's mid-risk data elements, provided, however, that:

(A) The organization must de-identify the mid-risk data elements prior to sharing the mid-risk data elements; or

(B) The organization:

(i) Must provide clear notice to the individual that the individual's mid-risk data elements will be shared;

(ii) Must identify the entity with which the organization will share the individual's mid-risk data elements;

(iii) Must identify the individual's mid-risk data elements that are being shared; and

(iv) Must affirmatively obtain verifiable consent from the individual to share the mid-risk data elements.

(f) Low-Risk Data Elements

(1) **General Requirements**: Any organization that collects, uses, and/or shares only low-risk data elements may do so without restriction.

(g) Collecting, Using, and/or Sharing Multiple Categories of Data Elements

(1) **General Requirements**: In the event that an organization collects data elements of different classifications (e.g., high-risk data elements, mid-risk data elements, and low-risk data elements), the

organization shall ensure that each data element is collected, used, and/or shared in accordance with its respective requirements as set forth in the Federal Omnibus Privacy Act.

(2) **Template for Collection of Data Elements**: An organization that collects data elements of different classifications (e.g., high-risk data elements, mid-risk data elements, and low-risk data elements) shall be in compliance with the collection procedures set forth in the Federal Omnibus Privacy Act if the data elements are collected using a form that is substantially identical to the form set forth in Appendix A.

V. CONCLUDING REMARKS

In this paper, we propose a model omnibus privacy statute. In doing so, we attempt to unify the treatment of data across differing sectors without unduly hampering an organization's operations. Our approach allows each sector, and indeed each organization within a sector, to define for itself what would constitute an essential business purpose. Thus, the statute provides great latitude for organizations, as long as they comply with the uniform requirements for how data elements are collected, retained, and shared.

In proposing our model omnibus privacy statute, we adopt a ternary structure that permits segregation of data elements into three distinct classifications, namely, high-risk data elements, mid-risk data elements, and low-risk data elements. As with all structures, the ternary structure has its advantages and disadvantages. Thus, we freely admit this ternary structure has its limitations. However, in our humble opinion, we believe it provides a reasonable balance between a coarse binary structure and an overly complicated four-plus-tiered structure.

Lastly, we harvested from currently existing statutes every data element we could find and assigned each data element to a particular data classification. We did so in an effort to provide clearer guidance on how each data element should be treated, irrespective of whether it is in the financial sector, the healthcare sector, the government sector, or whatnot. By expressly reciting every conceivable data element and categorizing it, we maximize the uniformity in data treatment across multiple sectors.

Lastly, as noted at the outset, our purpose was not to advocate for (or against) a federal omnibus privacy statute. Rather, presuming Congress chooses to press forward with an omnibus privacy statute, our goal was to provide one way in which such a statute could (and in our humble opinion should) be penned.

APPENDIX A: TEMPLATE FOR COLLECTION OF PERSONALLY-IDENTIFIABLE INFORMATION.

CUSTOMER PERSONAL INFORMATION

HIGH-RISK DATA ELEMENTS				
Signature			Date *Year Month Date*	
Last Name	First Name		Middle Initial	
Social Security Number - -	Driver's License Number *State Number*			
Email Address	Telephone Number ( ) -		Fax Number ( ) -	
Home Street Address	City	County of Residence	State	Zip Code
Mailing Address (if different)	City	County of Residence	State	Zip Code

MID-RISK DATA ELEMENTS		
Birthday *Year Month Date*	Place of Birth	Country of Citizenship
Political Affiliation	Religious Affiliation	Gender M F

LOW-RISK DATA ELEMENTS				
Height *Feet - Inches*	Weight *Pounds*	Education *High School*	*Year of Graduation*	
Activities		*College*	*Year of Graduation*	*Major*
		Graduate Degrees	*Year of Graduation*	*Major*
		Professional Degrees	*Year of Graduation*	*Major*
Awards				

[*COMPANY NAME*] REQUIRED INFORMATION

HIGH-RISK DATA ELEMENTS	Internal Account Number	Passcode / PIN

MID-RISK DATA ELEMENTS	Account General Information	
Criminal History		Consumer Characteristics

(a) High-Risk Data Elements

(1) **General Requirements**: Any organization that collects, uses, and/or shares high-risk data elements must have clearly-established and published policies and procedures for collecting, using, and/or sharing the high-risk data elements by the organization and any of its agents. These policies and procedures must clearly explain the organization's essential business purposes for collecting, using, and/or sharing the high-risk data elements.

(2) **Requirements for Collecting High-Risk Data Elements**: Any organization that collects high-risk data elements from any individual:

- (A) Must identify the high-risk data elements that are being collected;
- (B) Must provide clear notice to the individual that the individual is sharing high-risk data elements with the organization;
- (C) Must clearly explain the organization's essential business purposes for collecting the individual's high-risk data elements;
- (D) Must affirmatively obtain verifiable consent from the individual to collect the high-risk data elements; and
- (E) Must provide a copy of, or access to, the organization's policies and procedures to the individual.

(3) **Requirements for Using High-Risk Data Elements**:

- (A) **Essential Business Purposes and Restricted Actors**: An organization may freely use an individual's high-risk data elements without informing the individual or obtaining consent from the individual only if the following two (2) conditions are both met:
  - (i) **Limited Access**: Only agents that are internal to an organization and who have predefined job titles or predefined security permissions establishing a "need to know" may use the individual's high-risk data elements; and
  - (ii) **Limited Purpose**: An organization may use the individual's high-risk data elements only for the organization's essential business purposes, which have been clearly conveyed to the individual prior to the organization's use of the high-risk data elements.
- (B) **Restricted Actors and Other Business Uses**: An organization may use an individual's high-risk data elements for a use other than an essential business purpose, provided, however, that the organization:
  - (i) Must limit use of the high-risk data elements to only the organization's agents that are internal to the organization and who have predefined job titles or predefined security permissions;
  - (ii) Must provide clear notice to the individual that the individual's high-risk data elements are being used for a purpose other than an essential business purpose, to include providing a detailed explanation to the individual of the purposes for which the individual's high-risk data elements are being used;
  - (iii) Must identify the individual's high-risk data elements that are being used for those purposes;
  - (iv) Must obtain verifiable consent from the individual to use the high-risk data elements for those purposes; and
  - (v) Must de-identify the high-risk data elements prior to those uses.
- (C) **Limitations on Data Retention**: An organization shall not retain high-risk data elements, except for:
  - (i) **Retention Period**: a period of time that is necessary to accomplish the business purpose for which the high-risk data elements were collected or is required by law; and
  - (ii) **Encrypted Retention**: in an encrypted form at the most secure encryption level that is commercially reasonable for the organization's industry.

(4) **Requirements for Sharing High-Risk Data Elements**: For an organization to share an individual's high-risk data elements, the organization:

- (A) Must determine that sharing the high-risk data elements is reasonably necessary to advance an essential business purpose of the organization, and that there is no reasonable alternative to accomplishing the organization's essential business purpose without sharing the individual's high-risk data elements;
- (B) Must ensure that the entity with which the organization will share the high-risk data elements has clearly-established and published policies and procedures that are not less protective of the high-risk data elements than the organization's policies and procedures;
- (C) Must provide clear notice to the individual that the individual's high-risk data elements will be shared;
- (D) Must identify the entity with which the organization will share the individual's high-risk data elements;
- (E) Must provide a detailed explanation to the individual on why it is necessary to share the individual's high-risk data elements;
- (F) Must identify the individual's high-risk data elements that are being shared;
- (G) Must affirmatively obtain verifiable consent from the individual to share the high-risk data elements;
- (H) Must, if possible, de-identify the high-risk data elements prior to sharing the high-risk data elements; and
- (I) Must encrypt the high-risk data elements at the most secure encryption level that is commercially reasonable for the organization's industry prior to sharing the high-risk data elements.

(b) Mid-Risk Data Elements

(1) **General Requirements**: Any organization that collects, uses, and/or shares any mid-risk data elements must have clearly-established and published policies and procedures for collecting, using, and/or sharing the mid-risk data elements by the organization and/or any of its agents. These policies and procedures must clearly explain the organization's essential business purposes for collecting, using, and/or sharing the mid-risk data elements.

(2) **Requirements for Collecting Mid-Risk Data Elements**: Any organization that collects mid-risk data elements from any individual:

- (A) Must identify the mid-risk data elements that are being collected;
- (B) Must provide clear notice to the individual that the individual is sharing mid-risk data elements with the organization;
- (C) Must affirmatively obtain verifiable consent from the individual to collect the mid-risk data elements; and
- (D) Must provide a copy of, or access to, the organization's data collection policies and procedures to the individual.

(3) **Requirements for Using Mid-Risk Data Elements**:

- (A) **Essential Business Purpose**: An organization may use mid-risk data elements for the organization's essential business purpose without informing the individual or obtaining consent from the individual;
- (B) **Aggregation and Research**: An organization may freely use mid-risk data elements for aggregation or research without informing the individual or obtaining consent from the individual, provided, however, that the organization must de-identify the mid-risk data elements prior to aggregation or research.
- (C) **All Uses Other than for Essential Business Purposes**: For any use of an individual's mid-risk data elements other than an essential business purpose the organization:
  - (i) Must provide clear notice to the individual that the individual's mid-risk data elements are being used for a purpose other than an essential business purpose;
  - (ii) Must provide a detailed explanation to the individual of the purposes for which the individual's mid-risk data elements are being used;
  - (iii) Must identify the individual's mid-risk data elements that are being used for those purposes; and
  - (iv) Must affirmatively obtain verifiable consent from the individual to use the mid-risk data elements for those purposes.

(4) **Requirements for Sharing Mid-Risk Data Elements**: An organization may share an individual's mid-risk data elements, provided, however, that:

- (A) The organization must de-identify the mid-risk data elements prior to sharing the mid-risk data elements; or
- (B) The organization:
  - (i) Must provide clear notice to the individual that the individual's mid-risk data elements will be shared;
  - (ii) Must identify the entity with which the organization will share the individual's mid-risk data elements;
  - (iii) Must identify the individual's mid-risk data elements that are being shared; and
  - (iv) Must affirmatively obtain verifiable consent from the individual to share the mid-risk data elements.

(c) Low-Risk Data Elements

(1) **General Requirements**: Any organization that collects, uses, and/or shares only low-risk data elements may do so without restriction.

(d) Collecting, Using, and/or Sharing Multiple Categories of Data Elements

(1) **General Requirements**: In the event that an organization collects data elements of different classifications (e.g., high-risk data elements, mid-risk data elements, and low-risk data elements), the organization shall ensure that each data elements is collected, used, and/or shared in accordance with its respective requirements as set forth in the Federal Omnibus Privacy Act.

(e) Documentation

(1) The following documents may be required for the collection, use, or sharing of the information in the above-recited categories. Please ensure that the appropriate documents are completed or shared at the time of information collection. These documents can be found in [COMPANY LOCATION]:

- (A) Customer Consent Form;
- (B) Company Policies and Procedures, to include notice of privacy practices; and
- (C) Other company contracts or disclosures.