Big Data, Artificial Intelligence, Privacy, and Personal Data

By: Houston Putnam Lowry[1]

American Bar Association Section of International Law

Spring 2020 Virtual meeting-June 23, 2020

I. What is the problem?

You can't start intelligently without understanding the problem.

II. What is "big data"?

One definition is "extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions." Sometimes the analytical results surprise the data subjects.

It can be computationally difficult to obtain meaningful information from data. Store enough data and you are bound to get a spurious result (even if you set the probability to the 99.9% level, there is so much data to be analyzed you are bound to find a correlation for every thousand data categories analyzed).

While big data may not have a data subject's name, it can contain enough data to eliminate all but one data subject (meaning the data subject is identifiable as a practical matter even though the name is not available).

It is surprising how little data is needed to draw a conclusion with a 95% statistical confidence level.

Cambridge Analytical claimed to have 5,000 data points on every American voter.[2] ProPublica claims Facebook has

---

[1] Houston Putnam Lowry is a member of Polivy, Lowry & Clayton, LLC and is admitted to the Connecticut, District of Columbia and New York bars. His email is PTL@HPLowry.com

[2] https://medium.com/better-marketing/the-great-hack-reveals-facebook-ads-arent-just-selling-leggings-ea50b2191bf dated August 8, 2019.

52,000 unique attributes to classify each user.[3] Just describing the categories of data becomes difficult.

a. The amount of erroneous data stored increases as:

i. The price of storage goes down (Moore's law suggests the cost of storing data drops 50% every 18 months).

ii. The cost of correcting data exceeds the price of collecting data.

III. Is the problem social media? I think not, but it is certainly part of the problem.

a. The latest issue seems to be Facebook.
i. How does Facebook make money?
1. They are an advertising company that provides very targeting advertising.

ii. Facebook makes on average about $29.25 per user per year based upon 2019 ***revenue*** (not profit). This has increased over time:

Year	Amount
2011	$5.00
2012	$5.32
2013	$6.81
2014	$9.45
2015	$11.96
2016	$15.98
2017	$20.21
2018	$24.96
2019	$29.25

iii. This means Facebook hypothetically would not use your information for marketing purposes if you paid them roughly $30.00/year. In short, you

---

[3] https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them dated December 27, 2016.

don’t value your privacy because you wouldn’t pay $30.00/year for it.

b. What kinds of questions can be asked:

i. Do social media users feel they “control and own the information and content” which they post on their social media accounts? Almost certainly yes.

ii. Do the terms and conditions of the privacy policy of popular social media platforms (e.g., Facebook, LinkedIn, Google, Instagram, Twitter, etc.) actually provide so?

iii. Should the “privacy policies” of social media platforms be regulated?

iv. What legislative changes and policies do you expect to be effective in preventing the abuses which have been highlighted in the 2018 Senate hearings?

v. What legislative changes and policies do you expect will NOT be effective in preventing the abuses which have been highlighted in the 2018 Senate hearings?

vi. Will you disclose publically right now to our assembled audience here the source, recipient, and content of your last ten text messages or emails? Probably not…

vii. If some users wish to pay for using a social platform, rather than having the platform have access to their data in exchange for “free service”, is that a viable business model?

viii. Do you agree with Sen. John Kennedy’s statement that “Your user agreement sucks” in referring to Facebook’s user agreement, and if so what do you suggest be done.

ix. Should user content be expressly owned by the originator, and only licensed in a limited manner to the social media platform?

x. Should competition law and unfair trade practice law be used to regulate the privacy practices of social media platforms?

xi. Should targeted advertisements be banned, *Ban Targeted Advertising* by: David Dayen, The New Republic, April 10, 2018.

c. Why do you use social media anyway?

i. Is using social media worth the cost of your privacy?

ii. I was distressed when Facebook identified me in a picture with my new wife (and I have never been on Facebook and never tagged in a Facebook picture to my knowledge). How did it know?

d. What social media do Americans use as of September 2019?

	Millions of users[4]
Facebook	169.76
Instagram	121.23
Facebook messenger	106.4
Twitter	81.47
Pinterest	66.88
Reddit	47.87
Snapchat	45.98

e. What percentage of Americans use social media as of February 7, 2019?

Date[5]	18-29	30-49	50-64	65+
2/7/2019	90.00%	82.00%	69.00%	40.00%

[4] Pew Research Center, Social media update September 2019 https://www.statista.com/statistics/248074/most-popular-us-social-networking-apps-ranked-by-audience/

[5] Pew Research Center, Social media fact sheet 2/5/2018 http://www.pewinternet.org/fact-sheet/social-media/

1/10/2018	88.00%	78.00%	64.00%	37.00%
11/6/2016	89.00%	80.00%	64.00%	34.00%
7/12/2015	90.00%	77.00%	51.00%	35.00%
1/26/2014	84.00%	77.00%	52.00%	27.00%

f. If you use your Facebook account (or your Google account) to login to another website, that allows the two web sites to aggregate information about you. All of a sudden, potentially two separate people are confirmed to be one. The data is arguably doubled, but the value of the data likely increases exponentially.

IV. Is the problem more pernicious than traditional social media? As I was preparing for the on-line presentation of this program on my new wife's computer, it sent her a text message saying I was using her laptop (really?).

Consider your cell phone. You have it with you 24 hours a day and 7 days a week. *The Aisles Have Eyes*, by: Joseph Turow, Yale University Press, 2017.

The problem is businesses want to sell more and to have their advertising dollar work better. While economic efficiency is a laudable business goal, but should it happen at the expense of your privacy?

a. Do you know what information is (or can be) collected about you by your cell phone?

i. Location.

1. If you visit a location often enough, the demographics of the location will allow an observer to figure out if you live there or work there.

2. An observer can figure out who your social contacts are?

3. Consider how accurate the location information must be for your cell phone to give you GPS directions.

4. Your location information is automatically imbedded into each cell phone photo you take.

5. Aggregated cell phone statistics were used during the pandemic to determine the effectiveness of “lock down” orders.

ii. Speed.

b. Has your spouse ever called you to pick up an item on the way home because your spouse knows you are close to that particular store? Is that creepy or what?

c. Your phone can tie your billing zip code to your location so an advertiser will know your demographic’s disposable income as you walk in their door? Is that creepy?

i. My experience with the CVS app on my iPhone:

1. It sent me a text message coupon as I went into a store. How did it know I was entering the store?

2. The CVS app could run in the background of my iPhone even though I had not turned it on. I turned off that feature.

3. Some retailers even use low powered WiFi to track customers in the store (which would disclose which sales displays were working). The accuracy is within 10 feet.

4. Some retailers even use low powered Bluetooth to track customers in the store (which would disclose which sales displays were working). The accuracy is within 10 feet. Bluetooth Low Energy (BLE) uses less power and costs less.

5. Verizon asked if they could release data about me to advertisers. I said no (even though it was a business cell phone used by one of the other lawyers in the office). That might have created an interesting data

set because Verizon thought it was tracking me and it was tracking a different person.

AT&T never asked me the same question. Does that mean AT&T doesn't sell my data or they just don't get my permission to sell my data?

d. If you use a price checking app, that gives the app owner the chance to sell your information quickly to the manufacturer for use in a targeted advertisement (don't buy it at THAT price-we'll sell it for less and ship it to your house for free!). Amazon had an app that did that (but has discontinued it).

e. Do you let Siri listen to you? Where does that information go and what happens to it? Your phone does not have sufficient computational power to analyze speech, so it must use cloud processing.

f. You can then combine this information with your profile on a frequent user program (such as frequent flyer miles, CVS value points, the hardware store and the supermarket, etc). They have YEARS of data on you.

   i. Do you think they use this data to market to you?

   ii. Why not?

   iii. This is all possible because of the Universal Price Code (UPC).

   iv. Walmart's computer system is second only to the Pentagon in storage capacity.

   v. Walmart has the largest corporate satellite system in the world.

   vi. Target sent "targeted" advertisements to a young girl because their marketing analysis showed she was likely to be pregnant. Her father objected because he didn't know she was pregnant (an embarrassing situation!).

V. What law should govern privacy expectations? There are a number of possibilities:

a. Location where to data is collected. Does this make sense? This is controlled by the data collector and not the data subject.

b. Nationality of the data collector. This has nothing to do with the data subject, who may not even know the nationality of the data collector.

c. Location where the data is stored. Does this make sense? Did anyone plan on this? Where is your gmail account stored or managed? You probably don't know…and you probably do not care. The data subject has no control over this.

i. Did you know you have given gmail permission to "read" your email to better target advertisements to you? Does that have any attorney client implications for lawyers?

d. Nationality/habitual residency of the data subject.

Which one do you think makes sense? *See Transborder Data Flow: Public and Private International Law Aspects*," 6 Houston Journal of International Law 159 (1984) (attached).

VI. Uniform Law Commissioners[6] project: Collection and Use of Personally Identifiable Data Act.[7] (a copy of the current

---

[6] The Uniform Law Commission provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law. The organization comprises more than 300 lawyers, judges, and law professors, appointed by the states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, to research, draft and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical. Since its inception in 1892, the group has promulgated more than 200 acts, among them such bulwarks of state statutory law as the Uniform Commercial Code, the Uniform Probate Code, and the Uniform Partnership Act. http://www.uniformlaws.org/

draft is attached) There are a number of issues being considered:

a. Scope of the act: excludes small businesses[8] and activities already subject to data privacy regulation (such as HIPPA).

b. Data which does not identify a person (such as GPS tracking on an automobile or an IP address, which likely identifies a household).

c. Publicly available data (is this just government data or data from widely distributed media?)

d. Business to business data.

e. Contractual vs. Rights-Based Models. Should an "opt-in" or an "opt-out" model be used?

f. How should the rights be enforced (public office enforcement, private right of action, class action, private attorney general, etc.)

g. The jurisdictional "hook" is the commercial activities of a person who:[9]

i. Conducts business in the state.
ii. Provides services targeted to the state.

VII. American Law Institute (ALI) project on data economy studies, identifies, and collates the existing and potential legal rules applicable to transnational transactions in data as an asset and as a tradeable item

---

[7] https://www.uniformlaws.org/committees/community-home?CommunityKey=9aadc6d7-0020-4df2-821d-19aa34084532

[8] Must have custody of more personal data on more than 50,000 individuals or derive more that 50% of its gross annual revenue from personal data. Collection and Use Of Personally Identifiable Data Act §3(a)(1) and (2).

[9] Collection and Use Of Personally Identifiable Data Act §3(a).

and assess the “fit” of those rules with these transactions.[10]

a. This project commenced in early 2018.

b. This is a joint project with the European Law Institute.

c. The ALI reporter is Professor Neil B. Cohen of the Brooklyn Law School.

d. The project just completed tentative draft #1 in June 2020.

e. The choice of law issues will be discussed in Principle 38, which hasn’t been written yet.

[10] https://www.ali.org/projects/show/data-economy/

TRANSBORDER DATA FLOW ARTICLE

TRANSBORDER DATA FLOW: PUBLIC AND PRIVATE INTERNATIONAL LAW ASPECTS

Houston Putnam Lowry *

Regrettably, the very title of this field is misleading. Taken literally, transborder data flow means the international flow of information. The term does not connote any limitations of the method by which the information may be transmitted. These could range from courier and smoke signal to electron and laser. However, it is not simply the transmission, in and of itself, which concerns everyone. To reflect this problem much of the international community has adopted a new label for this field: Informatics.

Much has been written on this topic in recent years, but little has been said. Perhaps this is because no one really understands either the scope of the field or its content. It is very difficult to regulate in a vacuum, which is what most legal minds have been forced to do. American lawyers and businessmen do not like change because it creates confusion and uncertainty. To create order out of chaos is more the job of the philosopher or programmer. Such a mind must balance the basic forces of conflict, often unstated but nevertheless manifesting themselves through distracting symptoms and fads. The problems of computer networks are difficult enough to solve within a unified law district.[1] These difficulties increase exponentially when they arise in the international arena or in a context involving multiple law districts.[2]

The reader may nod sagely and comment about the political problems inherent in dealing in the international arena. That is not the source of the problem, although it certainly is a contributing factor.[3] Distance does not exist to a computer network; it is a meaningless con-

* J.D. *cum laude*, Gonzaga University School of Law; LLB in International Law, The University of Cambridge; Former Charles A. Dana Fellow in International & Comparative Law; Certificate in Private International Law, Hague Academy of International Law; Former Visiting Scholar, Yale Law School; Member of the Connecticut Bar and of the Honorable Society of Gray's Inn.

1. A unified law district is a single geographical, but not necessarily a single political, area where only one law applies. An example of a unified law district is England and Wales. All laws which are in force in England are *ipso facto* equally in force in Wales.

2. Federated states may be composed of multiple law districts, like the United States of America. Others may be multiple law districts for purposes of substantive law, but unified law districts for purposes of their conflict of laws rules, like the Federal Republic of Germany.

3. Professors McDougal and Reisman might reprimand me for forgetting that law and

cept. To every user, the whole computer is effectively in the same room as the user is. When distance is a meaningless concept, every problem becomes a border problem.[4] As every scholar knows, border problems are very difficult to contend with, which explains why there are so many jurisdictional principles.[5] While science fiction can create many more complex problems for the legal scholar,[6] the legal community has its hands full trying to handle this one.

A computer system, any computer system, can be broken down into four fundamental functions:

(1) Telecommunications;
(2) Memory;
(3) Manipulation of information; and
(4) Remote movement.

Each of these elements exists outside of computer systems and has been dealt with by the legal community for years. Computers add a quantitative rather than a qualitative dimension to each element. The combination of these elements with a computer's speed may create a synergistic effect. If that is so, putting the entire bundle of elements together may be sufficient to produce a qualitative change. First, however, each element should be examined carefully.

Telecommunications is the simplest element. It is a connection between two or more points which allows a flow of information. There is at least one virtually universal telecommunications system readily available to everyone, the telephone system. Within each state, there is a second and more limited telecommunications system, the power lines.[7] Now there is a rapidly growing telecommunications system which will hopefully become universal in the near future and allow at least one-way (if

politics are merely two sides of the same coin. While I have not forgotten that dearly learned lesson, it is still easier to concentrate on one side of the coin at a time, rather than two.

4. A border problem is one of those hypothetical problems which haunt first year law students, *i.e.*, person *A* in country *1* shoots across the border into country *2*, killing person *B*. What law governs? If the hypothetical was carefully drafted, it is possible that *A*'s action would have been a crime in either country *1* or *2* but was not simply because the crime occurred across the border so that its elements did not occur in the pertinent states. Of course, it is equally possible that two crimes could have been committed, but such a hypothetical would have no intellectual interest.

5. *I.e.,* (1) Territoriality, including objective or extended territoriality;
(2) Active personality (nationality of the actor);
(3) Protective or Security (national defense, counterfeiting, etc.);
(4) Universal (piracy, genocide, etc.);
(5) International (as distinguished by Ian Brownlie from Universal); and
(6) Passive personality (nationality of the victim).

6. Consider the legal problems created by Extra Sensory Perception (ESP) or even time travel, due to the meaninglessness of time and distance in these fields.

7. This is the means by which "wireless" intercoms and the like work.

not two-way) communications, television, and video text.[8]

From a practical standpoint, information is only useful to the extent that it is distributed. As a general rule, information known to no one or to only one person is not very useful.[9] Information is a commodity and telecommunications is the most efficient method of distributing that commodity.

Information is a very unusual commodity. It can be sold but cannot be consumed. Its value can alter dramatically from one moment to another. The value of information lies in its scarcity, which the very act of distribution starts to destroy. Distribution of information in effect creates more information, unlike almost any other commodity. The useful life of information is short and will get shorter as telecommunications become more efficient.

Some authors have broken down data communications into various parts:

(1) Electronic mail;
(2) Facsimile equipment;
(3) Electronic information and documentation services; and
(4) Electronic Funds Transfer (EFT) systems.[10]

This scheme is interesting but flawed. Certainly this list is not complete and is useful only for illustrative purposes. While these categories do exist, this breakdown does not contribute to an understanding of the subject. An electronic blip of a facsimile transmission is no different in quality from an electronic blip of electronic mail or even a voice telephone. What is important, in terms of regulating the content of communications, is the fact that the signal was sent, not the relative efficiency of the sending device.

The international community recognized this when the International Telecommunications Union (ITU) was named. The ITU regulates radio, television, telephone, and so on. The common thread is telecommunications. It would be foolish to regulate the functions of microwaves, lasers, and old-fashioned copper wire in different manners, at least in terms of function. Obviously, each is different from an administrative viewpoint: microwaves can cook people, lasers can blind people, and copper wire can conduct enough electricity to electrocute people. None

8. Consider scandal, for example, although that also depends on how one defines "useful."

9. *E.g.*, United Kingdom's Ceefax and Oracle.

10. Working Party on Information, Computer and Communications Policy, Directorate for Science, Technology and Industry, OECD, Symposium on Transborder Data Flows and Protection of Privacy (Sept. 20-23, 1977) (Vienna Symposium) (DSTI/ICCP/77.4).

of this should affect the regulations imposed on each medium simply because it may be used for a telecommunications purpose.

Second, is the element of memory. Every computer network has at least some memory, and most have a substantial amount of memory. Memory is, in and of itself, inherently frightening. Most people are ashamed of something they have done in the past, and would rather not be reminded of it. Even though the physical event may be imaginary or grossly exaggerated, the threatening feeling is very real.

Memory can be used as an instrument of social control, in the same way that language may become an instrument of social control. In more barbarous times, memory deprivation was used for that purpose. Books, a form of memory, have been destroyed for centuries because their contents were heretical, against public policy, or threatened the security of the king or the state. Oral communications, another more fragile manifestation of memory, were disrupted by blinding or cutting the tongue. A witness' credibility is dramatically reduced when he can no longer see. A man who has had his tongue cut out will have a difficult time passing along an oral tradition to his children, especially in an illiterate society. Of course, the grossest manipulation of all involves the murder of a man and his family before any information can be passed along.

Often, the accuracy of the information was not in dispute. Information that was true or mostly true was more dangerous than information which was demonstrably false. At common law, the greater the truth, the greater was the libel. Not only was truth no defense, but truth was an aggravating circumstance.

With the advent of modern technology, the manipulation of memory takes on more subtle methods. An unfortunate person can be hypnotised, pumped full of psychoactive drugs, given electro-convulsive shock "therapy," or subjected to psychosurgery. As more and more information is gleaned through the media, control of the media is merely remote control of the general population's memory. Careful control of the input into any "memory device," be it a person or a computer, ultimately regulates memory. Sometimes this memory can be recovered by calculation or deduction, but only in a limited number of cases. Most information is remembered, not calculated. As the total store of information increases, this proposition becomes increasingly more accurate.

An interesting thing happens as the cost of memory goes down. The value of the information remembered decreases also. Eventually, the marginal cost of the information will equal the marginal cost of the memory required to preserve the additional information. As information costs drop, it becomes more likely that incorrect, incomplete, or other valueless information will be retained. Verification and correction work

in a similar fashion. A low marginal cost for having incorrect data coupled with a moderate or high marginal cost for updating the information means the data will not be updated. It is simply economically unfeasible. This is why incorrect data so often gets recorded into records and is so difficult to get out.

Third, is the element of manipulation. Within a computer's hardware, this is represented by the central processing unit (CPU) or arithmetic logic unit (ALU). This is the ability to take information and process it in a uniform manner. It can be as complex as monitoring the health of orbiting astronauts or as simple as adding two plus two. This is the element which separates analysis from regurgitation. Data is taken and treated in some fashion to yield further data which was not obvious from the original data.

Fourth and last is the element of remote movement. At present, this is the element which is closest to science fiction. It has received no attention at all in the current debate about transborder data flow. Of course, that does not mean remote movement will not obtain importance in the relatively near future. Perhaps remote movement will enable "robots" to perform tasks which would be impossible for humans to do, ranging from maintenance of the core in a nuclear reactor to deep sea bed mining and salvage. Physicians are currently working on computer-controlled artificial replacement limbs and direct muscle stimulation to help paralyzed patients walk and move. Already robots are used in car manufacturing plants. There is nothing to stop them from being reprogrammed remotely or even from being centrally controlled from a remote, possibly foreign, site.

By now, the reader should be able to see the potential synergy in each of these fundamental function building blocks. Telecommunications plus memory could possibly create the largest "library" ever conceived, available to everyone everywhere. Telecommunications plus manipulation could create anything from an overgrown calculator to an idiot-savant Delphi oracle. Telecommunications plus remote movement could create remotely controlled robots, with all of their attendant good and bad multiple uses. Perhaps it would revolutionize the travel industry, particularly to hazardous areas. Putting all four elements together creates a very powerful force; something which communicates easily, forgets nothing without being told to forget it, and is capable of performing manipulations no ordinary person could perform in a lifetime.

No one can be certain of the effect of such a system. Without a doubt, it would have a fundamental effect on our world community as did paper, reading, and writing. To this day, no one knows the full effect paper had on society. The changes have been so radical that life would

seem to be impossible without paper. Computer networks will have a similar impact, not unlike the effect of the industrial revolution. Certainly there will be bad or traumatic effects from having this change, but they will probably be outweighed by the good or beneficial effects. In the beginning, the negative effects will be more evident than after a period of adjustment.

It is important to remember what is at stake, in terms of economics, when transborder data flows are discussed. The potential value of information processing is simply staggering. One-half of the United States' gross national product is taken up by the so-called "information economy."[11] Airlines rely on the SITA reservation network. Banks rely on SWIFT and EUREX to conduct their business in the multi-arena financial markets with some semblance of coordination. Hotels rely on reservation systems ranging from Holidex to UTELL. Major computer service vendors have created multinational networks, such as GEIS, Tymshare, CISI, and FIDES. Usually these commercial organizations have absolutely no idea for what purpose their computer network is being used or what information is being stored in their network. Surprisingly, there is no clear significant connection between data processing and employment.[12]

Some of the side effects are foreseeable. Doubtless some special interest groups will want to use computer networks for their own benefit and to the detriment of the world community. This manipulation may be direct, secondary, or tertiary. It will be justified on many counts, ranging from privacy to protection of infant domestic industries.[13] A wide assortment of national barriers can be and are erected, for whatever reason, against multinational computer networks.[14]

Historically, nations have not liked the idea of allowing a free flow of information across their borders. At one time it was very cumbersome to send transnational telegrams in Europe. The telegram was sent to the

11. Hamburg, *Transborder Data Flow*, 184 N.Y.L.J. 1 (1980).

12. INTERGOVERNMENTAL BUREAU FOR INFORMATICS, THE ECONOMIC DIMENSIONS OF TRANSBORDER DATA FLOWS, TDF 101 (May 1981).

13. *See generally* Gotlieb, Dalfen & Katz, *The Transborder Transfer of Information by Communications and Computer Systems*, 68 AM. J. INT'L L. 227 (1974) [hereinafter cited as Gotlieb].

14. Examples of such barriers are: (1) taxes; (2) interception of things contrary to public order, morals, or standards of good behavior; (3) requirement of a percentage to be produced domestically; (4) outright ban (based upon cultural preservation, national sovereignty, etc.); (5) data protection laws (privacy); (6) imposition of inconsistent or narrowly interpreted technical standards; and, (7) monitoring requirements. *See generally International Data Flow, 1981: Hearings Before a Subcomm. on Government Operations of the House Comm. on Government Operations*, 96th Cong., 2d Sess. (1980) [hereinafter cited as *Hearings*]; Eger, *Emerging Restrictions on Transborder Data Flows: Privacy Protection or Non-Tariff Trade Barriers*, 10 LAW & POL'Y IN INT'L BUS. 1055 (1978).

border, where it was transcribed. A courier carried the telegram physically across the border. Once on the other side, the telegram was re-sent on to the next border outpost or to its destination if it was within the borders of that nation.[15] While this cumbersome system has thankfully faded into obscurity, the reflex it symbolizes has not dwindled appreciably.

An analysis must be made of the nature of a computer network. Is the access to a computer network limited, or is it essentially unlimited? An example of an unlimited system is speech, where access is not limited by any inherent natural or technological limitations. An example of a limited system is broadcast radio or television where the electromagnetic spectrum has room for only a finite number of channels. Different policies govern the two types of systems because of the difference in the availability of access. An unlimited system is characterized by freedom of access, while a limited system is characterized by controlled access.[16] There is no technological reason to limit access to a hypothetical computer network, which suggests that access to a hypothetical computer network should not be controlled by governments.

This was not the approach taken by the General Assembly of the United Nations in December 1978.[17] A resolution entitled "A New World Information Order" was passed by the General Assembly, calling for:

(1) Free circulation, and wider and better balanced dissemination of information;
(2) Change LDC's (Lesser Developed Countries) from dependence to interdependence and cooperation; and
(3) Equal dialogue between differing societies.

This resolution has the same political overtones as those of the "New Economic Order" resolution which in and of itself is neither good nor bad. Perhaps it is idealistic because it is self-contradictory. Often the cry for "balance" is contrary to the free circulation of information because it is a cry for censorship. Such a cry is potentially justifiable when dealing with a limited access medium. It has no applicability when dealing with unlimited access media, except as a sword for censorship. Since computer networks are an unlimited access medium, the "balance" concept is not applicable. A computer network does not centrally create informa-

15. Gotlieb, *supra* note 13, at 228.

16. A limited system may be balanced in terms of access, *e.g.*, users may be restricted to five minutes; or it may be balanced as a content, *e.g.*, through presentation of differing viewpoints.

17. *See generally Hearings*, *supra* note 14, at 547 (statement of Ambassador Vohn Rein Larda, Director, International Communications Agency); Colby, *Intelligence in the 1980s*, 1 INFORMATION SOC'Y 53 (1981).

tion. Rather, information is gathered and disseminated decentrally, which is the very phenomenon which makes a computer system so hard to control.

After all of this, it is important to examine the actual applications of computer network transborder data flow. Since the common users of these systems are large multinational companies, particular attention should be paid to their current uses and needs. One example is Motorola Inc., which stores:

(1) Inventory information;
(2) Sales data;
(3) Incoming orders (internal and external);
(4) Payroll;
(5) Cost accounting standards;
(6) Independent timesharing applications with shared files;
(7) Product test parameters;
(8) Part characterization data;
(9) Invoices;
(10) Accounts receivable information; and
(11) Production schedules.[18]

Another example is Levi Strauss, which stores:

(1) Manufacturing schedules;
(2) Intercompany prices;
(3) Inventory status;
(4) Shipping instructions;
(5) Financial information of all types; and
(6) Operating information from production and distribution activities.[19]

A final example is Chase Manhatten Bank[20], which stores and uses information on high net worth individuals in connection with its cash management service, and its international private banking department.

As the reader can see, very little of this information is about individuals. Most transborder data flows are by organizations and about their operations.[21] Privacy plays a very minor part of the import and export of this type of information. Certainly some data, such as payroll or personnel files, should be protected. But often privacy is just a convenient club with which to beat to death the freedom to exchange information.

18. *Hearings, supra* note 14, at 630 (statement of W.D. Connor, Vice President and Chairman of Corporate Multinational Operations, Motorola). *See also* Turn, *Privacy Protection and Security in Transborder Data Processing Systems*, 16 STAN. J. INT'L L. 67 (1980).

19. *Hearings, supra* note 14, at 693 (statement of Walter Haas, Chairman, Levi Strauss).

20. *Hearings, supra* note 14, at 740 (statement of Kay Riddle, Vice President, Chase Manhattan).

21. Novotny, *Transborder Data Flows and International Law: A Framework for Policy-Oriented Inquiry*, 16 STAN. J. INT'L L. 141, 165 (1980).

It also follows that national security claims are equally exaggerated.[22] Member states of the International Telecommunications Convention have a great deal of control over the import and export of information into and out of their countries. A state may stop private telegrams and intercept any private telecommunications which threatens its security.[23] A state may require disclosure of cryptographic keys.[24] There is no reason to give nations even greater power, since this should be sufficient. Nor should "national security" be interpreted so broadly as to swallow up the major premise that information should be freely exchanged.

Regulation of an actual transborder data transmission can be effectively accomplished under existing public international law, particularly the ITU. Regulation regarding privacy need not be done at an international level. It can be done effectively on a national level, particularly since the much feared "data havens" have failed to materialize.[25]

Several states have data protection laws.[26] Of course, the scope of these laws does vary. Some recognize the privacy rights of only natural persons,[27] while others accord privacy rights to corporations and other legal persons as well as to natural persons.[28] Some of these laws apply

22. *Id.* at 166.

23. International Telecommunications Convention, Oct. 25, 1973, art. XIX, 28 U.S.T. 2497, T.I.A.S. No. 8572.

24. *Id.* at art. XXII.

25. INTERGOVERNMENTAL BUREAU OF INFORMATICS, FIRST MEETING OF THE INTERNATIONAL WORKING GROUP ON DATA PROTECTION AND INTERNATIONAL LAW, May 25-26, 1981, TDF 104 (July 1981) (Summary Records) [hereinafter FIRST MEETING].

26. Federal Act of 18th October, 1978 on the Protection of Personal Data (Data Protection Act), Bundesgesetzblatt No. 565/1968 (Austria); Canadian Human Rights Act, ch. 33, [1976-1977] Can. Stat. 887 (1977) (Canada); Public Authorities Registers Act, No. 294, § 21(3) [1978] (Denmark); Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Data Processing, Files and Freedom Act), § 24, [1978] J.O. 227 (France); Federal Data Protection Act, [1977] BGBl I 201 (Federal Republic of Germany); Act 63 of Systematic Recording of Personal Data, [1981]; Protection of Privacy Law, [1981] L. 5741-1981 (Israel); Law Governing the Use of Name-Linked Data in Data Processing, Doc. Parl. No. 2131 [1979] (Luxembourg); Act of 9th June, 1978 Relating to Personal Data Registers (Norway); Data Act of 11th May, 1973, *as amended* on January 19, 1977 (Sweden); Privacy Act of 1974, 5 U.S.C. § 552a (1976 & Supp. V 1981); Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (September 1980), *reprinted in* TRANSNAT'L DATA REPORT, October 1980, at 17; Organization for Economic Cooperation and Development, Recommendation for the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80)58 (Oct. 1, 1980) [hereinafter cited as Guidelines]. *See also* OFFICE OF TELECOMMUNICATIONS, U.S. DEPT. OF COMMERCE, SELECTED FOREIGN NATIONAL DATA PROTECTION LAWS AND BILLS (C. Wilk ed. 1978); Bull, *Regulation of Transborder Data Flow under the German Data Protection Act*, 4 TRANSNAT'L DATA REPORT 13 (1981).

27. Act of 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Data Processing, Files and Freedom Act), art. 26, [1978] J.O. 227 (France).

28. *E.g.*, Act of 63 on Systematic Recording of Personal Data, art. 1 (Iceland); Act of 9th June, 1978 Relating to Personal Data Registers (Norway).

only to state maintained records,[29] to privately maintained records,[30] or to both publicly and privately maintained records.[31] However there are certain principles which are common to virtually all privacy legislation.[32]

To start, there is a social justification principle. Information should be collected only for those uses which are socially acceptable. For instance, it may be acceptable to collect data on traffic ticket scofflaws but it would not be acceptable to compile a data register of all Jews. Of course, what is socially justifiable varies from society to society, so this is an elusive limitation.

Next, there is a collection limitation principle. Only the minimum necessary data should be collected to perform the task at hand. The data should be collected by fair and lawful means.[33] If appropriate, the data subject should either consent to or know about the collection. Reasons for this limitation should be self-evident. It is very difficult to violate the privacy of personal records which do not exist.

The validity of any data must be assured, mandating a data quality principle. Any data should be accurate, complete, and up to date. Very often the usefulness of data is significantly impaired because the data is not accurate. Incorrect and incomplete data is frequently worse than no information at all. A complete lack of information acts as a cautionary flag. Undetected errors cause problems because information is always assumed to be correct.

There is usually a use limitation principle, sometimes called a purpose restriction. This requires the data subject to be informed of the reason for the data collection at the time it is collected. Data collected for one purpose can only be used for that purpose or another compatible purpose. Of course, the data subject could subsequently authorize another use, or the law may specify another use based upon public policy, *i.e.*, collecting taxes. After the reason for the data has expired, the data should be destroyed.

Laws also embody a security principle. Reasonable precautions should be taken to prevent unauthorized access, destruction, use, modification, or disclosure of data. Even the finest data becomes useless if it is tampered with or destroyed between the time it is collected and the time it is used.

At the heart of the privacy issue is the disclosure limitation princi-

29. 5 U.S.C. § 552a (1976 & Supp. V 1981).
30. Federal Data Protection Act § 4, [1977] BGB1 I 201 (Federal Republic of Germany).
31. Protection of Privacy Law § 23, [1981] (Israel).
32. Kirby, *Transborder Data Flows and the "Basic Rules" of Data Privacy*, 16 STAN. J. INT'L L. 27 (1980). *See also* Guidelines, *supra* note 25.
33. This gives rise to the possibility that a means may be lawful but unfair; an issue not unlike the unjust law problem which haunts jurisiprudential scholars.

ple. Privacy requires disclosure to balance the need to use the information against the individual's desire to prevent disclosure. Information can be disclosed with consent, by authority of law, and by a publicly known usage of common and routine practice. This allows practices such as the publishing of a telephone directory. Certain information is so common, such as names and addresses, that the regular practice is to disclose them. In effect, the data subject impliedly consents to such disclosures. This may be explained under some type of social contract theory.

To avoid a "Catch-22" situation, most laws embody an openness principle. It should be easy to discover, perhaps as a matter of public record, the existence and nature of personal data, its main purpose, and the identity of its custodian. If this information were not available, it would be very difficult for the data subject to verify the accuracy of such data. Accuracy is positively correlated to knowledge that the data exists. Very often secret records are misleading, incomplete, and inaccurate.

Another corollary is the time limitation principle. Data which has fulfilled its usefulness should be destroyed. This is simple and economic, and yet it is a rare procedure in today's business world. Record keepers are trained to keep data, not to dispose of it. Keeping data which can no longer be used for its original purpose invites a violation of the use limitation principle.

It is very important to have an accountability principle. There must be someone who takes responsibility for the data under the law. In large organizations, responsibility is frequently passed on and ultimately avoided altogether. No one wishes to be accountable, even though all covet the power which goes hand in hand with that accountability. Hence, all laws require that a data controller be designated as a prerequisite for compliance with the law.

Finally, there is the individual participation principle. This can be broken down into a bundle of rights that every person, however "person" is defined under the relevant law, holds and can enforce against the data controller. First, an individual has a right to know he is included in the data register. Second, any data in the register must be conveyed to the subject within a reasonable time, free of cost or at a reasonable charge, in a reasonable manner, and in a form that is readily intelligible to the subject. Third, a subject must be given reasons why a data controller will not comply with these disclosure requirements, and an opportunity to challenge that determination. Finally, the subject may challenge the validity, correctness, or completeness of the data about him. If the challenge is successful, the data shall be erased, rectified, completed, or amended as necessary.

Aside from the issue of privacy, the issue of copyright has been given a great deal of attention as it applies to computers. Thus far, no one has been successful in getting the concept of a computer network inside the umbrella of copyright. Simply put, this is because copyright is meaningless within the computer environment.[34] Copyright best fits technologies which produce multiple identical copies at a central location, such as books, newspapers, or records. With such technologies, it is relatively easy to locate the source, in terms of both content and means of production, and to prove the number of copies made. Computers do not fit into that mold. Often copies are not identical but merely substantially similar. Most likely the copier will introduce changes during the copying process itself. When this happens, it is easy to lose sight of the original within a very short number of generations. It is also very easy to make copies of computer data; no special equipment is needed, just the computer itself. Perhaps computers are better suited to ASCAP type pooled royalty arrangements. Certainly this is the argument put forward by authors concerned about video tape piracy. Similar arguments will be heard shortly about the pirating of video games.

But the questions of privacy and copyright actually have very little to do with the overall impact of computer networks. Each is but a small area of the entire field, albeit a very visible area. The bulk of the law of computer networks will be formulated at the national level. It will be up to private international law to harmonize the divergent municipal laws, assuming that UNIDROIT is not successful in the near future. Public international law will have very little, if anything, to do with this process. Of course, it would be absolutely marvelous if the Hague Conference on Private International Law would put out a convention regulating this area. Regrettably, such advances do not appear to be forthcoming in the near future.

There has been only one attempt to regulate transborder data flow principles within a conflict of laws setting.[35] It leaned very heavily towards application of the law of the state of origin, namely, the state of collection. While the superficial attraction of this choice is strong, it is about as desirable as the *lex loci delicti* rule in torts, *i.e.*, in some cases it will produce absurd results. Conflict of law norms should be analyzed according to the pertinent fundamental function of the computer network in question.

The most obvious example of this is the remote movement function. The preferred standard is to judge the movement by the laws of the state

34 Pool & Solomon, *Intellectual Property and Transborder Data Flows*, 16 STAN. J. INT'L L. 113 (1980).

35. FIRST MEETING, *supra* note 25, at 44.

in which the movement occurred, rather than by the laws of the state in which the impulse originated. An obvious example of this is driving. An Englishman remotely controlling an automobile in France should be required to meet the requirements of French motor vehicle laws, such as driving on the right hand side of the road. The liability should not be shifted or avoided just because the Englishman is in St. Albans or London, while his car is being driven in Jussy-Champagne or Paris.

Physical security and safety standards of the computer network should be governed by the law of the situs of the equipment. While this means different parts of the network will be subject to different standards, it does not create any problems. *Depecage* is a well known and tolerated principle in private international law. This concept stands for the proposition that the physical security and safety standards for any part of the network are fixed, since a network does not physically move around, and each user, no matter where he is located, is subject to the same requirements and offered the same protection regarding any particular part of the network. This alternative also satisfies any *ordre public* interests a state may have in preventing unsafe conditions within its territory, such as electrocution, explosion, fire, and so forth.

The next topic for consideration is the actual import and export of information, the telecommunications function. As with any other form of communication, a state may interrupt or suspend it for reasons of national security. While there is no way to ensure a uniform interpretation of national security, this is not likely to present a practical problem. Countries have, by and large, restrictively interpreted national security under Article 19 of the International Telecommunications Convention and they are very likely to continue to do so. A side effect of this would allow states to require users or networks to divulge any cryptographic keys to the national PTT (Post, Telegram, and Telephone, a nationally owned and operated monopoly) or its equivalent. While this appears to be a radical idea, it is in keeping with current public international law principles regarding telecommunications.

Many people are, and will continue to be, interested in privacy or data security. Doubtless much of this interest is in good faith, but a certain minority would use it as a non-tariff weapon to compete in the data processing field. The Intergovernmental Bureau of Informatics (IBI) has suggested by implication that the law of the state where the data is stored should determine the applicable privacy law. This proposition would only provide a short-term solution. As networks get larger, data will be stored in more than one place. On many computers, it is possible for part of a file to be stored on one device, while another part of the same file is stored on an entirely physically separate device. With the advent of

computer systems which simultaneously "back themselves up," such as the Tandem Non-Stop Computer, the same data will be stored in two different places at the same time to prevent possible loss or damage.

A naive or casual user will never even notice this. An expert may notice it, but may not care. The computer does not care—most often it will store the data in the first available place, *regardless of where that place is*. This bears no relationship to how much free storage space is available in that place, unless it is completely full. Therefore the IBI's suggestion would lead to different parts, or possibly even the same part (in a "back up" type system), of a person's file being protected by different laws entirely on the basis of chance. Since random choice of law essentially destroys predictability, no rational legislator would knowingly make such a choice. As storage devices are refreshed or updated, a purely technical and internal computer function which usually cannot be performed by a user, the applicable law governing one piece of data would probably change, essentially randomly.

Therefore, a more predictable and rational connecting factor should be chosen. Nationality of the data subject is an obvious first choice. People often expect to be governed by the law of their nationality. This connecting factor presents several problems. In Europe, people often retain one nationality while residing in another country. The European Communities encourage and facilitate this. Further, companies often do not store the nationality of their data subjects. When a person changes his nationality, he does not normally notify his bank, credit bureau, or insurance company. There is also the problem of stateless people. What law would govern when a data subject has either no nationality or dual nationality?

Similar problems exist in choosing domicile as a connecting factor. Very few people know the location of their actual domicile. It may even be a place the data subject has never been to, such as the domicile of origin of one's parents, as in the case of a military man born to a military couple. There is no rational connection between the domicile of origin and a data subject, like there is between a data subject and a domicile of choice.

The simplest solution to the problem may be to choose the law of the data subject's habitual residence. Habitual residence is not the same thing as nationality or domicile.[36] It is different because it follows the actual physical location of the data subject more closely. A data subject will usually notify his bank or insurance company of his new address.

36. *See* Hague Conference on Private International Law, XXV Convention on the Law Applicable to Matrimonial Property Regimes.

Most data registers already store this information as a matter of course. A mailing address will usually be the same as, and almost certainly in the same law district as, the data subject's habitual residence. Therefore, while multiple laws may apply to the bank as a whole, only one law would apply to each data subject within the data bank, regardless of where the data comes from or where it is physically stored.

This connecting factor will work equally well in cases of electronic theft or conversion, as opposed to physical theft, *i.e.*, one authorized user copying another authorized user's file illicitly. Electronic theft of computer network time would be controlled by the law of the principal place of business of the network. It is a rebuttable presumption that a corporation's principal place of business is the place of its nationality, its place of incorporation. While one law district will enforce the civil laws of another district, no law district will enforce the penal laws of another law district.

Difficulties also spring forth when considering transactional data. Transactional data is generated from an event, such as an American Express charge card purchase in Istanbul. A certain superficial attraction attaches to the idea of using the law of the place of the transaction.[37] That would not work well in all circumstances. It would be the correct law to apply to determine if there was a valid contract or a valid negotiable instrument. Public laws considered part of the *loit d'application immediate*[38] would be applied using the principle of *lex fori*. On the other hand, the purchaser's habitual residence would dictate the consumer protection laws.[39]

This discussion shows that there is no final answer on this issue. Like traditional choice of law, the questions of what law to apply should rely on characterization, at least to some extent. The applicable law should be determined from the context of the question: for what purpose is the applicable law being sought? The connecting factor can be, and probably should be, different for negotiable instrument considerations, consumer sales considerations, or privacy considerations. Since this is the normal state of affairs in private international law, this uncertainty should not cause any more than the traditional problems.

Of course, there will be courts and legal scholars who will try to insist on *lex fori*, for a variety of reasons such as familiarity, national

37. *See* Inter-American Specialized Conference on Private International Law (CIDIP-I, II, and III).

38. Convention of the Law Applicable to Contractual Obligations, opened for signature June 19, 1980, art. 7, 23 O.J. EUR. COMM. (No. L. 266) 1 (1980) [hereinafter cited as Convention], *reprinted in* Delaume, *The European Convention on the Law Applicable to Contractual Obligations: Why a Convention?*, 22 VA. J. INT'L L. 124, 124-54, at app. 1 (1981).

39. Convention, *supra* note 38, at art. 5.

sovereignty, and public policy. Such a stance is cowardly from an intellectual standpoint and counterproductive in the long run. Where and when multinational computer networks exist, and several do exist connecting over 20 countries,[40] choice of the applicable law will turn into a race to the courthouse. Every country where the network can be accessed will claim jurisdiction, creating a massive concurrent jurisdiction problem with each forum trying to apply its own law. The stakes are high enough to make it financially advantageous for 20 countries to get embroiled in such a tar-baby, urged on by the parties. Such an outcome would do more than a simple disservice to the legal profession and the pursuit of justice.

40. *E.g.*, Mark III Network of General Electric Information Services Company, Telenet, Tymnet of Tymshare Inc., and Euronet (slightly less than 20 countries at present).

Uniform Law Commissioners Collection And Use Of Personally Identifiable Data Act (draft)

D R A F T

FOR DISCUSSION ONLY

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

February 21–22, 2020 Drafting Committee Meeting

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the drafting committee. They do not necessarily reflect the views of the Conference and its commissioners and the drafting committee and its members and reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

January 7, 2020

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

The committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this act consists of the following individuals:

HARVEY S. PERLMAN	Nebraska, *Chair*
JAMES BOPP JR.	Indiana
STEPHEN Y. CHOW	Massachusetts
PARRELL D. GROSSMAN	North Dakota
JAMES C. McKAY JR.	District of Columbia
LARRY METZ	Florida
JAMES E. O'CONNOR	Nebraska
ROBERT J. TENNESSEN	Minnesota
KERRY TIPPPER	Colorado
ANTHONY C. WISNIEWSKI	Maryland
CANDACE M. ZIERDT	Florida
DAVID V. ZVENYACH	Wisconsin
CARL H. LISMAN	Vermont, *President*
WILLIAM H. HENNING	Alabama, *Division Chair*

OTHER PARTICIPANTS

WILLIAM McGEVERAN	Minnesota, *Reporter*
MICHAEL AISENBERG	Virginia, *American Bar Association Advisor*
STEVEN L. WILLBORN	Nebraska, *Style Liaison*
TIM SCHNABEL	Illinois, *Executive Director*

Copies of this act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

TABLE OF CONTENTS

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

SECTION 1. SHORT TITLE. This [act] may be cited as the Collection and Use of Personally Identifiable Data Act.

SECTION 2. DEFINITIONS. In this [act]

(1) "Data controller" or "controller" means a data custodian who, alone or jointly with others, decides upon the purposes, means, and extent of processing to be conducted in relation to personal data that has been in its possession or control.

(2) "Data custodian" or "custodian" means a person in possession or control of personal data or deidentified data. Controllers and processors are data custodians.

(3) "Data processor" or "processor" means a data custodian who processes personal data on behalf of a data controller and under that data controller's direction.

(4) "Data subject" means the individual, device, or household to whom personal data refers.

(5) "Deidentified" means that the capacity of information to identify, describe, or be associated with any particular individual, device, or household has been eliminated, provided the custodian of the information makes no attempt to reidentify the information and implements all of the following:

(A) Technical safeguards that reasonably prevent reidentification of the individual, device, or household to whom the information may pertain.

(B) Business processes that specifically prohibit reidentification of the information; and

(C) Business processes that reasonably prevent inadvertent release of deidentified data.

(6) “Device” means any physical object that connects to the internet or to another device.

(7) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(8) “Person” means an individual, estate, business or nonprofit entity, or other legal entity. The term does not include a public corporation, government or governmental subdivision, agency, or instrumentality.

(9) “Personal data” means information that identifies or describes a particular individual, household, or device, and information that can be associated with a particular individual, household, or device by using a reasonable amount of effort. Personal data need not have been collected directly from a data subject. Probabilistic inferences about an individual, household, or device, including inferences derived from profiling, are included in the definition of personal data. Deidentified data and publicly available data are not personal data.

(10) “Processing” means any operation performed on personal data, whether or not by automated means, including use, storage, disclosure, analysis, and modification.

(11) “Profiling” means any form of automated processing of personal data to evaluate, analyze, or predict a data subject’s economic status, health, demographic characteristics (including race, gender, or sexual orientation), personal preferences, interests, character, reliability, behavior, social or political views, physical location, or movements. Profiling does not include evaluation, analysis, or prediction based solely on a data subject’s current activity, including search queries, if no personal data is retained for future use after the completion of the activity. Probabilistic inferences derived from profiling are personal data.

(12) “Publicly available data” means information that has been made available from federal, state, or local government records in accordance with law, provided the information is

being used in a manner consistent with any conditions on its use imposed by law.

(13) "Sensitive data" means

(A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, activities or preferences related to gender or sexuality, or citizenship or immigration status;

(B) biometric and genetic data; and

(C) personal data about a data subject who is known to be under [13] years of age.

(14) "Sign" means, with present intent to authenticate or adopt a record:

(A) to execute or adopt a tangible symbol; or

(B) to attach to or logically associate with the record an electronic symbol, sound, or process.

(15) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. [The term includes a federally recognized Indian tribe.]

(16) "Targeted advertising" means advertising displayed to a data subject on the basis of profiling.

(17) "Transfer" means to convey personal data into the possession or control of another custodian.

SECTION 3. SCOPE.

(a) This [law] applies to the commercial activities of a person who conducts business [in the State of X] or produces products or provides services targeted to [the State of X], provided that the person:

(1) is the custodian of personal data concerning more than [50,000] individuals,

devices, or households in one year,

(2) earns more than [50] percent of its gross annual revenue directly from its activities as a controller or processor of personal data, or

(3) is a data processor acting on behalf of a data controller whose activities satisfy the requirements of this section.

(b) This [act] does not apply to personal health information as defined under the Health Information Portability and Accountability Act [CITE] [and regulations] when the custodian of that data is regulated by that statute.

(c) This [act] does not apply to the activities of a consumer reporting agency as defined under [FCRA] in connection with activities regulated by that statute.

(d) This [act] does not apply to state or local government entities.

Reporter's Note: Other exclusions from scope?

SECTION 4. DUTIES ACCORDING TO ROLE. A data custodian shall be responsible for the duties in Sections 5-9. A data controller shall be responsible for the additional duties in Sections 10-11 and for the satisfaction of data subject rights in Sections 12-17.

(a) Processing by the processor shall be governed by a written contract between the controller and processor that is binding on both parties and that sets out the nature and purpose of the processing, the type of personal data subject to the processing (including the identification of any sensitive data), the duration of the processing, and the obligations and rights of both parties.

(b) A data processor shall adhere to the instructions of the data controller and shall assist the controller in fulfilling its duties under this [act].

(c) A data processor shall not process personal data for any purpose that was not included in the notice provided to data subjects by the data controller as required by this [act].

(d) A data processor shall make available to the data controller all information necessary to demonstrate the processor's compliance with the requirements of this [act] and with the requirements of the contract between the controller and processor. The contract shall give the controller a reasonable right to audit the conduct of the processor in relation to the processing.

(e) A data processor may only transfer personal data to another processor or to any other person with the express written consent of the controller. Any such transfer must be governed by a written contract that imposes all the same obligations on the recipient of the personal data that are imposed on the processor in the contract between the controller and the processor, regardless of whether the recipient is otherwise subject to this [act].

(f) A data controller may indemnify a data processor for liability of the data processor under this [act].

SECTION 5. DESIGNATION OF DATA PRIVACY OFFICER. A data custodian shall designate an individual employee or contractor to serve as the custodian's data privacy officer.

(a) A data privacy officer shall have qualifications appropriate for the supervision of the custodian's responsibilities under this [act]. Minimum qualifications shall depend on the scale, complexity, and risks of the data processing activities undertaken by the custodian.

(b) A data privacy officer shall be responsible for the data privacy assessments required by this [act] and shall sign each data privacy assessment personally.

(c) A data privacy officer may perform other duties for the custodian or for other persons, provided the data privacy officer spends a reasonably sufficient amount of time directing a custodian's duties under [this law]. If a data privacy officer is not an employee of the custodian, the custodian and the data privacy officer must execute a written agreement that clearly specifies

the data privacy officer's duties. An individual may serve as a data privacy officer for more than one data custodian.

(d) A data privacy officer may assign or delegate other persons to complete tasks under supervision, but the data privacy officer must retain authority over the completion of those tasks.

SECTION 6. DATA PRIVACY ASSESSMENT. A custodian must conduct, to the extent not previously conducted, a written data privacy assessment of each data processing activity undertaken by the custodian, in order to evaluate all material risks, harms, and benefits of processing.

(a) A data privacy assessment shall be completed about each data processing activity every two years. It shall be updated any time a change in processing activities may materially increase privacy risks to data subjects.

(b) A data privacy assessment shall evaluate

(1) the type of personal data being processed;

(2) the presence of any sensitive data among the personal data being processed;

(3) the scale of the processing activities;

(4) the context in which personal data is collected and processed;

(5) the seriousness of privacy risks imposed on data subjects as a result of the processing;

(6) the likelihood of privacy risks causing harm to data subjects as a result of the processing;

(7) the benefits that may flow directly or indirectly to the custodian, data subjects, the public, or others as a result of the processing;

(8) the resources reasonably available to the data custodian for addressing privacy

risks, taking account of the revenue generated by the processing; and

(9) the measures the custodian has undertaken to mitigate any privacy risks.

(c) Privacy risks evaluated in a data privacy assessment shall encompass risks of all potential harms to data subjects, including

(1) accidental disclosure, theft, or other breaches of security causing personal data to be revealed to persons without authorization;

(2) identity theft;

(3) harassment;

(4) unwanted profiling;

(5) stigmatization or reputational harm;

(6) emotional harm including anxiety, embarrassment, fear, and other demonstrable mental harms; and

(7) other foreseeable outcomes that would be highly offensive to the reasonable person.

(d) A data processor may adopt data privacy assessments completed by a data controller concerning the same personal data, provided the assessment satisfies all requirements of this section.

(e) A data custodian must retain a written copy of all data privacy assessments for ten years after their completion. Upon request of the [Attorney General] in connection with [an investigation], a data custodian must provide copies of all current and former data privacy assessments.

(f) Whether or not a data custodian has provided data privacy assessments to the Attroney General, a data privacy assessment is confidential business information [and is not subject to

public records requests or subject to compulsory civil discovery in any court].

Legislative Note: *The state should include appropriate language in subsection 6(f) exempting data privacy assessments from open records requests and compulsory civil discovery requests to the maximum extent possible under state law.*

SECTION 7. CUSTODIAN'S DUTY OF LOYALTY. A data custodian shall not

(a) process or use personal data when processing or use exposes a data subject to reasonably foreseeable and material risks and harms that are not outweighed by benefits to the data subject or the public, or

(b) engage in processing practices that are unfair, deceptive, or abusive.

SECTION 8. CUSTODIAN'S DUTY OF DATA SECURITY. A data custodian shall adopt, implement, and maintain reasonable data security measures to protect the confidentiality and integrity of personal data in the custodian's possession or control. Reasonable data security measures shall include administrative, technical, and physical safeguards as appropriate. Data security measures shall be evaluated as part of the data privacy assessment required under this [act]. An evaluation of the reasonableness of data security measures shall take into consideration the magnitude and likelihood of security risks and potential resulting harms, the resources available to the custodian, and industry practices among other custodians who are similarly situated. Reasonable security practices may be derived from best practices promulgated by professional organizations, government entities, or other specialized sources.

SECTION 9. CUSTODIAN'S DUTY OF DATA MINIMIZATION. A data custodian shall not collect, process, or retain more personal data than necessary to achieve the purposes of processing. When a data controller transfers personal data to a data processor, the controller shall transfer and the processor shall accept only as much personal data as is necessary to complete the processor's processing activities. At the completion of processing, a processor

shall destroy all personal data or return it to the controller, pursuant to the agreement between the controller and processor required under section 4.

SECTION 10. CONTROLLER'S DUTY OF TRANSPARENCY.

(a) A data controller shall provide data subjects with a reasonably accessible, clear, and meaningful privacy notice which discloses

(1) the categories of personal data collected or processed by or on behalf of the controller;

(2) the purposes for processing of personal data, either by the controller or on the controller's behalf;

(3) the categories of personal data that the controller provides to processors or to any other persons;

(4) the categories of processors or other persons who receive personal data from the controller;

(5) the nature and purpose of any profiling of data subjects conducted using the personal data; and

(6) the means by which a data subject may exercise rights provided by this [act].

(b) The notice under this section shall clearly and conspicuously designate at least two methods for a data subject to contact the data controller in order to exercise rights under this [act]. At least one of these methods shall be a toll-free telephone number. If the controller maintains an internet web site, at least one of these methods shall be contact through the web site.

(c) If the data controller processes personal data for targeted advertising, or provides personal data to any processor or other person to process for targeted advertising, the notice

under this section shall clearly and conspicuously disclose such processing and shall provide an automated internet-based mechanism for the data subject to exercise the right to opt out of targeted advertising under this [act].

(d) The notice under this section shall be reasonably available at the time personal data is collected from a data subject.

SECTION 11. CONTROLLER'S DUTY OF PURPOSE LIMITATION. A controller shall not process personal data, or permit processors or other persons to process personal data, for purposes that are not specified in the notice to data subjects required by this [act].

SECTION 12. DATA SUBJECT RIGHTS GENERALLY.

(a) A data subject may exercise rights under sections 13-16 by notifying the controller by any reasonable means of the data subject's intent to exercise one or more of these rights. Parents of a [minor child] may exercise these rights on behalf of the [minor child]. If personal data pertains to a household or device, a person who belongs to the household or owns the device may identify the household or device and exercise the rights specified under this [act] in relation to personal data about that household or device.

(b) A data controller shall comply with requests without undue delay. If the data controller has not complied with the request within 45 days of receiving it, the data controller shall notify the data subject who made the request and shall provide an explanation of the actions being taken to comply with the request.

(c) A data controller shall make reasonable efforts to ensure that its responses to requests by data subjects to exercise rights under this [act] include personal data in the possession or control of data processors acting on the controller's behalf. The data controller shall make

reasonable efforts to notify processors acting on its behalf when a data subject exercises these rights, and shall instruct the processor to comply in the same fashion as the controller.

(d) A data controller shall establish procedures for determining responses to data subjects' assertions of rights under sections 13-16. The data privacy officer for a data controller shall approve such procedures. An explanation of the procedures in clear language shall be reasonably accessible to all data subjects. The procedures shall include an opportunity to appeal an initial determination by the data controller. Appeals of an initial determination shall be reviewed under the supervision of the data privacy officer. If a data subject is dissatisfied with the final disposition of an appeal, the data processor shall inform the data subject of the procedure to [file a complaint] with the [Attorney General].

SECTION 13. RIGHTS OF ACCESS AND PORTABILITY.

(a) A data subject has the right to receive confirmation from a data controller indicating whether the data controller controls or possesses any personal data that the controller knows pertains to the data subject.

(b) A data subject has the right to receive a copy of personal data covered by subsection (a). Once per year, the data controller must provide this copy free of charge. The data controller may charge a reasonable fee based on actual administrative costs to comply with additional requests for copies under this subsection. If requests are manifestly unreasonable or excessive, in particular because of their repetitive character, the data controller may refuse to act on requests from that data subject for one year. The data controller bears the burden of demonstrating that a request is manifestly unreasonable or excessive.

(c) If a data controller collected personal data directly from the data subject, the data controller shall provide the copy in subsection (b) to the data subject in a format that, to the

extent technically feasible, is portable and enables the data subject to transmit the personal data to another data controller conveniently and, where applicable, by automated means.

SECTION 14. RIGHTS RELATED TO TARGETED ADVERTISING AND PROFILING.

(a) A data subject has the right to restrict a data controller from processing or transferring personal data pertaining to the data subject (an "opt out") for purposes of

(1) targeted advertising;

(2) profiling in furtherance of decisions that produce legal effects or similarly significant effects concerning the data subject.

(b) If a controller processes or transfers sensitive data for the purposes listed in subsection (a), the controller must receive affirmative consent (an "opt in") from the data subject before undertaking such processing or transfer.

SECTION 15. RIGHT OF CORRECTION. A data subject has the right to require a controller to correct inaccuracies in personal data pertaining to the data subject.

SECTION 16. RIGHT OF DELETION. A data subject has the right to require a controller to delete personal data pertaining to the data subject.

SECTION 17. NONDISCRIMINATION. A data controller shall not discriminate against any data subject for exercising rights under this [act], including by denying goods and services, charging different rates, or providing a different level of quality, except that a data controller may provide benefits to data subjects that are closely related to the purpose of processing and that require access to personal data.

SECTION 18. WAIVERS PROHIBITED. Any provision of a contract or agreement that purports to waive or limit rights or duties imposed by this [act] is contrary to public policy

and shall be void and unenforceable, except that a controller may indemnify a processor for liability under this [act].

SECTION 19. REGULATORY ENFORCEMENT. The provisions of this [act] shall be enforced by [the Attorney General].

Legislative Note: *The state should include appropriate language cross-referencing the particular powers of the Attorney General that will be applied to enforcement of this statute and the applicable penalties.*

SECTION 20. PRIVATE RIGHT OF ACTION.

(a) A data subject may bring a civil suit against a data custodian for violations of sections 7, 8, 11, 13, 14, 15, 16, or 17. A private party may not bring suit in state or federal court alleging violation of any other part of this [act].

(b) Damages available to a person in a suit under this section shall be actual damages or damages of [$100], whichever is greater.

(c) Evidence about the development or results of a data privacy assessment is not subject to compulsory discovery in a civil suit brought under this [act], and shall be treated by the court in the same manner as a confidential offer of settlement, unless a data custodian voluntarily introduces evidence related to a data privacy assessment. If a data custodian voluntarily introduces evidence related to a data privacy assessment, admissibility and discoverability of evidence related to that data privacy assessment shall be handled in accordance with the court's ordinary rules of evidence.

SECTION 21. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

SECTION 22. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND

NATIONAL COMMERCE ACT. This [act] modifies, limits, and supersedes the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001, et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

SECTION 23. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.

Legislative Note: *Include this section only if this state lacks a general severability statute or a decision by the highest court of this state stating a general rule of severability.*

SECTION 24. EFFECTIVE DATE. This [act] takes effect [180 days] after the date of enactment.