Pergamon

Government Information Quarterly 19 (2002) 317–336

Government Information Quarterly

The structures of centralized governmental privacy protection: approaches, models, and analysis

Paul T. Jaeger*, Charles R. McClure, Bruce T. Fraser

Information Use Management and Policy Institute, School of Information Studies, Florida State University, Tallahassee, FL 32306, USA

Abstract

This article asserts that the United States federal government should adopt a centralized governmental structure for the privacy protection of personal information and data. There are a number of significant reasons, ranging from facilitation of the international dealings of United States corporations to the interactions of the United States government with other governments, for creating a centralized privacy protection structure for the United States federal government. This article examines the rise of centralized governmental privacy protection structures, identifies reasons for adopting such structures, and analyzes a selection of the structures used by various nations and states at present. From this analysis, the article presents a number of models of centralized governmental privacy protection structures. These models then form the basis of a discussion of what type of structural models of privacy protection would be most appropriate for the U.S. federal government.

1. Introduction: a structural approach to privacy protection

There are certain elements that can be identified as essential to any centralized governmental attempt to protect privacy in the contemporary world. These essential elements of privacy protection include the types of privacy protections offered, the way these privacy protections are enforced, and the centralized government structure created to implement and oversee the privacy protections.[1] Each of these elements merits careful examination. This article provides a discussion of the various roles of the structural element in centralized governmental privacy protection, the reasons for having a centralized privacy protection

* Corresponding author.
E-mail address: ptj0956@garnet.acns.fsu.edu (P.T. Jaeger).

0740-624X/02/$ – see front matter
PII: S0740-624X(02)00111-9

structure, the effects of such structures, and issues that governments that lack such a structure should consider.

The term *structure* describes the relationships of components or units of an organization among other components or units in that organization.[2] Privacy protection as a centralized structure within a government can only occur by action of the government. Such centralized governmental structures for privacy are designed as a method to promote and preserve privacy protections within the society. Due in significant part to the negative effect of technology on the ability to keep information private, many governments have adopted centralized structures to protect privacy, though the United States has not.

It is the assertion of this article that the United States federal government needs to adopt some form of centralized government privacy protection structure. The article will detail multiple reasons for this need and offer numerous models of centralized privacy protection structures for consideration and adoption. There are many ways in which to adopt a centralized government privacy protection structure in the United States and the assessment here will highlight those models that would likely conform to the framework of the U.S. federal government.

2. Privacy protection and the United States federal government

The United States has thus far avoided creating a centralized privacy protection structure, relying on privacy protection to emanate from three disparate and uncoordinated sources: specific laws, the policies of individual government agencies, and the rulings of the judiciary. This combination of factors does not, however, create a functional structural approach to privacy protection. Unlike many other nations, the privacy laws of the United States federal government are not omnibus laws and the federal government does not have a centralized privacy protection structure or agency. The current approach of the United States government is a sectoral one, where the privacy laws are narrow in focus, unconnected to a greater privacy protection system, and are uncoordinated with each other. The ultimate results of this approach are the lack of an identifiable, unified federal government concept of or approach to issues of privacy protection and the lack of an identifiable centralized structure for privacy protection.

2.1. The role of federal law in privacy protection

The United States has passed one major federal law to address privacy concerns, as well as numerous other laws with a limited scope of privacy protection. The *Privacy Act of 1974* established privacy protection standards for collection, use, and management of personal information by federal government agencies.[3] However, these standards do not apply to certain parts of the federal government, to state or local government agencies, or to private organizations. Furthermore, the protections of the act can be overridden by the agencies it does apply to when an agency believes the privacy concern is outweighed by other legitimate factors. Ultimately, the *Privacy Act of 1974*, as it is written, does not contemplate a centralized privacy protection structure.

All of the other federal laws regarding privacy are limited in scope. Laws like the *Telephone Consumer Protection Act of 1991*,[4] the *Driver's Privacy Protection Act of 1994*,[5] and the *Video Privacy Protection Act of 1988*[6] apply to a single narrow area of privacy protection. Each law protects personal information in a particular context, such as the content of video rental records. Even viewed as a whole, these laws do not provide a unified approach or structure through which privacy can be protected. In fact, these laws, for the most part, do not even address the structure through which the laws will be implemented or enforced. Each law provides a limited amount of privacy protection in an isolated area.

The lack of an omnibus privacy protection law and a centralized privacy protection structure has caused difficulties for the U.S. when dealing with some nations and organizations that do have centralized privacy protection structures. For example, the U.S. laws do not comply with the privacy protections required by the European Union (EU) for transactions involving transfers of personal data. The Article 29 Data Protection Working Party of the EU, the EU commission in charge of evaluating non-EU data and privacy protection laws, determined U.S. laws "cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."[7]

This disjunction between U.S. law and EU law led to the negotiated set of Safe Harbor principles for transactions involving the transfers of personal information between organizations in the U.S. and the EU.[8] As a result of this special Safe Harbor agreement between the United States and the EU, the United States has not needed to conform to the requirements of the Directive. Seven principles underlie the Safe Harbor framework for data transfers from EU Member States to the United States: notice, choice, onward transfer, security, data integrity, access, and enforcement.[9]

These Safe Harbor principles are intended to fulfill the requirements governing data exports for U.S. organizations that receive personal information from organizations within the EU. Compliance with the Safe Harbor principles is voluntary and can be accomplished by compliance with the principles and public declaration of compliance. However, the Safe Harbor principles may ultimately be inadequate to meet the data protection standards of the EU and other nations. Even after the Safe Harbor principles had been agreed upon, the Article 29 Data Protection Working Party still confirmed "general concerns" about the effectiveness of the Safe Harbor arrangement.[10] These lingering doubts about the usefulness of the Safe Harbor principles, and about U.S. privacy protection in general, emphasize the need for the adoption of a centralized privacy protection structure by the United States federal government.

2.2. The role of federal agencies in privacy protection

Within the organization of the U.S. federal government, there is no agency charged with coordination of privacy protection. As the federal privacy laws are limited in scope and unconnected to one another, there has been no manner to establish a centralized privacy protection agency. Some federal agencies have privacy protection responsibilities, but few have taken initiatives to protect personal information in a general sense. Certain federal agencies, such as the Department of Defense and the Internal Revenue Service, have

established their own privacy offices, but these are limited to the activities of the one particular agency.

The Privacy Act of 1974 gave the Office of Management and Budget (OMB) responsibility for federal privacy protection activities without giving the OMB the authority or power necessary to implement or enforce privacy protection policies at the individual agencies. As a result, each agency, to a certain extent, is left to its own devices to implement and comply with federal laws regarding privacy protection. In line with its responsibilities under the *Privacy Act of 1974*, the OMB undertakes privacy policy-making as part of its general management activities. Some of the more narrow privacy protection laws, however, are under the jurisdiction of other agencies.

After the OMB, the Federal Trade Commission (FTC) is perhaps the most active in attempting to protect the privacy of the general population by overseeing privacy concerns in certain types of commercial transactions. With the increase in Internet usage and electronic transactions, the FTC has become involved in addressing the electronic misuses of personal information. Since 1995, the FTC has maintained a Consumer Privacy Initiative meant to examine online consumer privacy and to promote consumer and business education about the use of personal information online.

Ultimately, there are a number of federal agencies with limited privacy protection duties or agendas, yet no agency to coordinate and manage federal privacy protection. The OMB provides guidance and regulations to government agencies regarding the *Privacy Act of 1974* and the FTC enforces some privacy laws in the commercial arena. Some other agencies have defined, limited roles for other privacy laws, depending on whether Congress passed privacy laws that relate to the activities of an agency. The current state of privacy protection in the agencies of the U.S. federal government does not resemble any sort of functional structure.

2.3. The role of the judiciary in privacy protection

The judicial branch of the federal government has traditionally been the most thoughtful and active guardian of privacy. In fact, the right of privacy first appeared in America as a legal concept in Judge Thomas Cooley's *Law of Torts.*[11] Cooley asserted rights that he labeled the right to one's person and the right to personal immunity, basically the right "to be let alone."[12] One year after the publication of Cooley's *Laws of Torts*, this idea began to be adopted by courts. The Michigan Supreme Court, in *DeMay v. Roberts*, granted tort relief for a battery action because the plaintiff "had a legal right to the privacy of her apartment at such a time, and the law secures to her this right by requiring others to observe it, and to abstain for its violation."[13]

In 1890, Samuel Warren and Louis Brandeis wrote the article that took this nascent legal right of privacy and gave it a clear definition, securing its place in the American legal landscape. Warren and Brandeis argued that established legal precedents had already created a right to privacy and a duty for the law "to protect the privacy of private life."[14] In 1905, Warren and Brandeis' argument was used by the Georgia Supreme Court to hold that an affirmative right to privacy existed in Georgia. The court wrote that privacy was "embraced with the right of personal liberty."[15] In the subsequent half century, the right of privacy was

so embraced by the judiciary that in 1960 William Prosser could declare without controversy that the overwhelming majority of courts protected an individual's right to privacy.[16]

The United States Supreme Court soon expanded the view of privacy taken by Prosser. Between 1965 and 1977, the Supreme Court firmly established the right to privacy of an individual as a Constitutional right through various parts of the Bill of Rights, the Constitution, and its amendments. This elaboration of the Constitutional right to privacy was so unexpected and unusual that it was labeled the "discovery of a Constitutional right to privacy."[17] This right was defined and refined in cases like *Griswold v. Connecticut, Loving v. Virginia, Eisenstadt v. Bard, Roe v. Wade, Whalen v. Roe,* and *Planned Parenthood v. Casey.*[18] The end result of these cases is the legal principle that the right to privacy, though never expressly stated in the Constitution, is embedded in numerous parts of the document, including the First, Third Fourth, Fifth, Ninth, and Fourteenth Amendments.

Because the judiciary has the most clearly articulated and most comprehensive conception of the right to privacy, it has often been the courts that have best provided privacy protections. There are, however, several serious problems with relying on the judiciary as the primary protection of privacy rights:

- The judiciary cannot mandate the content of privacy protections; it can only enforce those that have been established by law. If the legislature does not create a system for privacy protection, then the judiciary is very limited in the amount of privacy protection that can be offered.
- The judiciary can only become involved in a privacy protection issue once a law has been broken. It cannot protect rights in an affirmative or preventative sense.
- The judiciary is not a unified whole, decisions can vary between courts and districts.

As a result, the holdings of the judiciary can never constitute a centralized privacy protection structure.

3. The need for creating a centralized governmental structure for privacy protection

3.1. The concept of informational privacy

Early in the information age, Alan Westin described privacy as the right of individuals to determine "when, how, and to what extent information about them is communicated to others."[19] Another useful early definition explained privacy in terms of "limited accessibility," a concept that includes the elements of secrecy (information known about the individual), anonymity (attention paid to the individual), and solitude (physical access to the individual).[20] These descriptions of privacy illuminate the fact that the protection of private information has been a long running concern. While the older privacy concepts and concerns still have relevance, the concept of privacy has been altered irrevocably by technology. Certain people, for business, personal, or even illegal reasons, have always tried to collect and use (or abuse) personal data. For the individuals wishing to collect and use such personal

information, the technological advances have made these activities much faster, much easier, and much more ubiquitous.

The types of information that people wish to protect and the levels of protection they desire likely remain the same regardless of technology. However, technology has changed significantly the ways in which to collect personal information; the simplicity and speed of the collection of personal information; the volume of personal information collected; the sharing and exchanging of personal information; and the ease of use of personal information.[21] The data collection and sharing capabilities of computers have created tremendous new issues in the protection of personal information. Technology now can collect, process, use, and even sometimes abuse personal information around the clock with immense power and speed.[22] These technological changes encourage the development of centralized governmental structures for privacy protection.

Informational privacy is the "concern about limiting acquaintance with personal affairs" and is "the sense of privacy that is of concern most often in ordinary life."[23] In relation to technology, informational privacy is the concern for protection of personal information from unwanted collection or use by others, especially without the knowledge of the individual being studied. Personal information includes "those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation."[24] Informational privacy is the area in which technology has the greatest impact, making public information out of what the individual believes is private information. It is quite possible that in the near future, "informational technology will in all probability have penetrated every aspect of human activity."[25]

3.2. The impact of current technologies on informational privacy

Until recent decades, informational privacy was much easier to maintain. Even if information an individual wished to keep private was in the public records or recorded by a company, the information was not usually easy to find. It was certainly difficult to connect the information to many other sources of information about the individual. Medical records or a Social Security Number or financial information or information about shopping habits could be gathered, but only through a slow process involving contact with many specific places (either by visiting locations or by making telephone contact) to collect the desired information. Such efforts did not guarantee any results, either. It was by no means an effortless task to compile a profile about an individual based on personal information that was publicly and commercially available.

Much of the information privacy protection of the past was de facto protection based on the sheer difficulty of gathering information about an individual. This difficulty allowed the individual to maintain informational privacy in a practical sense even if they did not actually have perfect information privacy. Modern technology greatly altered the extent of protection of informational privacy.

"The same search engines and collections of information that provide the ideal tools for the searcher who dives into the World Wide Web in the hope of emerging with a fact in his

teeth work equally well whether the fact is historical or personal. Privacy through obscurity is not, or at least will not be, a practical option."[26]

Personal information is collected in the most routine activities, such as registering to vote, using a credit card, owning stock, having a baby, getting a pet vaccinated, paying an overdue fine for a library book, mailing in a warranty card, using an ATM, and subscribing to a magazine. These examples are a mere few among a staggering multitude of ways in which the collection of personal information transpires. The privatization of traditional government functions can create further problems for policies related to information.[27] In the era of the Internet, it is virtually impossible for an individual to manage to avoid ever having records kept about their activities. This personal information, depending on who collects it, is then used by the collector, sold to other data collectors for use, matched with data from other data collections, or even made part of the public record by government agencies. All of these activities are much simpler, faster, and more powerful as a result of the interconnectivity between databases and data collectors now possible due to the Internet.

The technology driving the Internet also provides additional ways to collect personal information, often without the knowledge of the data subject. The reasons for this inescapable collection of personal information are primarily economic. Unlike other kinds of privacy issues involving physical or emotional privacy, personal information can have a great financial value. Databases of personal information can be used to determine the viewing habits, shopping habits, and purchasing capacity of an individual, which can then be used to market specific products and services to the individual. The databases of personal information can be sold to other parties interested in marketing products and services, often being used to generate endless numbers of mailing lists. These databases of personal information can even go through the process of database matching where the personal information in multiple databases is brought together to create a profile of each individual in the databases that combines all the information about each individual in all of the databases. Such activities can provide financial gain to organizations that collect and use personal information. Personal information can even be used to alter the prices of items, from soda from vending machines to books from on-line stores, to match the needs and the spending habits of an individual.[28]

The financial benefits of collection of personal information are, of course, not new. However, the changes in technology make such data collection much easier. Technology facilitates the creation and expansion of databases of personal information, as well as the process of database matching incredibly efficient and simple. Web sites now collect huge amounts of personal information about visitors to the sites, information so personal that it can be accurately described as "finely grained personal data."[29] In light of these technological developments, governments may have "a vital role to play in crafting a supportive regulatory framework and 'filling the gaps' in private-sector action."[30]

3.3. The growth of centralized government privacy protection structures

Spurred by these technological changes, many nations implemented policies to address these concerns in order to address the activities of the government or of private entities, like corporations, or of both. Most centralized governmental structures for protecting privacy

were adopted between the late 1980s and the mid 1990s as information technology was becoming inextricably intertwined with many aspects of life. Further, the centralized government privacy protection structures that existed before the late 1980s have mostly been updated, and strengthened, by revisions of the implementing laws.

The most notable and influential is the privacy protection policy implemented by the European Union to govern the usage of personal information by government and private entities: the Data Protection Directive.[31] In fact, the emergence of privacy protection as a major international concern has been "driven by the Privacy Directive of 1995 adopted by the European Union."[32] The EU Data Directive intends to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[33] In brief, the EU Data Directive establishes minimum requirements for national privacy and data protection laws in member states. The Directive requires each member state to enact laws that govern the collection, recording, and use of any information relating to an identified or identifiable natural person. The Directive dictates that any personal information used must be accurate, up-to-date, relevant, and necessary for and limited to the intended purpose.

A complex organizational structure was created to enforce the Directive. In each EU member nation, at least one completely independent supervisory authority must oversee this data protection policy. Aside from being consulted on the creation of administrative measures and regulations regarding personal data, the regulatory agencies have powers to investigate data processing activities to ensure compliance with the protections of the Directive.

The Directive also created centralized governmental structures to protect privacy at the extranational level. In the EU itself, two institutions were established to oversee privacy protection throughout the EU. The Article 29 Working Party focuses on issues regarding the application of national measures to ensure uniformity of data protection within the EU and among the EU member nations. The Article 29 Working Party also monitors the levels of privacy protection in non-EU nations, evaluates any proposed changes to the Directive, and makes recommendations regarding privacy within the EU. The Article 31 Committee issues opinions relating to the levels of compliance with privacy protection policies by non-EU nations.

These policies and organizational structures have had a great deal of impact on non-EU member nations. A nation wishing to do business involving the use of personal information in the EU must satisfy the EU authorities that the protections of that nation are similar to EU protections. Since adoption of Directive-compliant policies provides a nation the opportunity to conduct business transactions without difficulty with EU nations, a great many non-EU nations, including the Czech Republic, Hungary, Iceland, Liechtenstein, Lithuania, Monaco, Norway, Poland, Russia, Slovakia, Slovenia, and Switzerland, have adopted privacy protection policies and organizational structures similar to those mandated by the Directive.[34]

4. Models of centralized governmental structures for privacy protection

The following models are all possible ways of establishing a centralized structure for privacy protection. Each is extrapolated from governmental privacy protection structures already in use by state governments, national governments, or extranational bodies. The

method used to develop these models included gathering data about various governmental privacy protection structures through a multimethod approach. This approach was based on the study's primary research questions: what are possible centralized organizational privacy structures that might be considered for implementation in the United States Government, and how are these models similar and different in terms of application.

A number of different structures were developed and evaluated through the following data collection activities:

- Analysis of relevant laws and policies at the Federal, national, and state levels;
- Interviews with government officials familiar with the structural issues related to privacy and data protection;
- Analysis of selected literature regarding organizational structures in government; and
- Expert review of the various proposed models.

This approach provided a basis by which the Information Institute staff could propose and describe a basic set of centralized structural models for privacy protection at the Federal level.

These models are not intended to be literal representations of the evaluated structures. Instead, the models are generalized concepts with specific and intended modifications designed to have general relevance rather than be tied too closely to the type of government from which the privacy structure was derived. As a result, the models are intentionally skeletal and abstract to enhance their usefulness in many governmental contexts. The primary focus of these models is their applicability and relevance in the context of the United States federal government. Finally, the order of presentation of the models of structural organization is alphabetical and is not intended to indicate any ranking or preference of the models.

4.1. The bureaucratic model

In a bureaucratic model, the privacy agency operates within the bureaucratic hierarchy of the government, functioning as a part of the executive branch. The bureaucratic privacy agency works with many different stakeholders in privacy issues. It makes recommendations to public and private organizations in the processing and use of data. The agency also provides advice, information, and referrals to members of the public regarding information privacy rights. Furthermore, the bureaucratic agency provides training services about privacy laws and duties to other state agencies.

An example of the bureaucratic approach, California's Office of Privacy Protection is a division of the Department of Consumer Affairs, a consumer protection agency.[35] The Office of Privacy Protection reports to the Department of Consumer Affairs that reports to the Secretary of State and Consumer Services, who, as a cabinet member, reports to the Governor. Through this position in the government hierarchy, the Office of Privacy Protection offers privacy policy opinions, assistance, and guidance to the agencies of the government and offers training to government offices and employees on privacy issues. Other than its internal government functions, the Office of Privacy Protection provides advice, information, and referrals about privacy issues to members of the public.

The primary consideration drawn from the bureaucratic model is how the placement of an agency within the government structure would affect the ability of the privacy agency to fulfill its mandate. If the United States federal government was to consider a bureaucratic model, the placement within the government structure must be weighed carefully, with respect to lines of authority and reporting, relationships with other agencies, enabling powers of the agency, and the separation of powers of the branches of government. The amount of power the agency would have and its ability to operate effectively could depend heavily on the bureaucratic placement of the agency within the federal government.

4.2. The federal-state model

The federal-state model has essential characteristics and functions at both the federal level and the state level. At the federal level, the privacy agency is independent of the rest of the government in its functions. The federal privacy agency works with both public and private organizations at the national level to ensure that privacy rights are protected. The federal privacy agency also encourages the development of nation-wide industry codes for privacy protection. The federal privacy agency works parallel to and in concert with the state privacy agencies to advance privacy policies. The state privacy agencies are responsible for similar activities at the state level, working with state and local public and private organizations.

The federal-state approach evolves from that used in Canada (as a federal-provincial approach) through the Office of the Privacy Commissioner of Canada.[36] As the privacy institutions of the provincial governments were created independently of one another, the privacy protection system in Canada operates in a decentralized manner, with the provincial agencies working parallel to Office of the Privacy Commissioner. The national agency addresses privacy issues at the national level, while each provincial agency addresses privacy issues in its individual province. The system in Canada allows for federal privacy protection without interfering with the privacy policies of the individual provinces. The flexibility of this framework, however, does not create a truly uniform set of privacy protections for each citizen.

The federal-state model offers several relevant characteristics for the United States. As many states already have established privacy laws or protection agencies, a federal-state model could be applied so that a centralized United States federal privacy agency could be functioning parallel to the state agencies. These parallel functions could involve separate efforts, such as is the system in Canada, or could be a coordinated effort between the federal agency and the state agencies. If the federal agency was more oriented toward coordination, such as an expanded and enhanced version of what the Office of Management and Budget does now, then the federal agency could take the lead on privacy matters or could work completely in concert with the state agencies.

4.3. The harmonizing model

The harmonizing model is based in the activities of a special supergovernmental organization to oversee privacy protection among member states of the organization. The legislative body of the organization creates legislation that places obligations on the member states.

This legislation serves to harmonize and standardize the legal privacy protections of the member states and guarantee that the laws of the member states are compatible. Within the organization, special committees are established to oversee these privacy protection activities by giving a voice to each member state in the policies without allowing any particular member to dominate the policies of the organization. This balance is maintained by the presence of a series of organizational safeguards within the organization. The most notable example of an organization employing the harmonizing approach is the European Union. The European Union Data Directive guides the privacy policies of the EU and also guides the privacy policies and protections of the member states.[37] The harmonizing model can function through an extranational organization, such as the EU, or through an organization overseeing parts of a single country.

The harmonizing model offers two distinct, though compatible, options for consideration. The first is a federal and state version of the harmonizing model. In such a case, a federal law could be passed that mandated each state establish a privacy protection agency to provide a certain level of privacy protection similar to the manner in which the EU has directed privacy protection in its member states. This harmonizing model would quickly bring uniformity to privacy rights throughout the states. The Congress could use its spending clause powers[38] or its powers to regulate commerce among the states[39] as the legal basis for the harmonization of state privacy laws. Such a model would have to be very carefully assessed, however. It could face legal challenges as violation of the Constitution if the harmonization were viewed by the state governments as an intrusion on the rights of the states as guaranteed in the 10th Amendment of the Constitution.[40]

A second version of the harmonizing model would be one that harmonized privacy protections in the United States with the protections provided in the EU. Such a model would harmonize the United States with the EU as well as with the large number of non-EU nations that have adopted the privacy standards of the EU. This model would take the United States beyond Safe Harbor principles and could even be the basis of providing privacy rights similar to those of the EU, as has been done by nations such as the Czech Republic and Poland. These two types of harmonizing approaches are not mutually exclusive and could efficiently work in conjunction.

4.4. The independent regulatory model

An independent regulatory privacy agency is appointed by the executive or the legislative branch of the government, but is independent in its operations. The independent regulatory privacy agency oversees all of the privacy-related activities of both public and private organizations that use personal information. It has an advising function to the legislature and the executive. It will consult and advise the government on administrative measures, regulations, and proposed and future legislation.

An example of an independent regulatory agency is the Data Protection Commission of Italy.[41] The Commission oversees compliance with laws and advises the government about the need for further legislation. It can conduct investigations, order technical assessments, issue orders based on the investigations, order changes to data use, or stop data operations entirely. It can also force payment of damages for improper processing of personal data and

can seek imprisonment and administrative remedies. The Commission can order public and private authorities to cooperate in an investigation. It informs the public of the legal rights of citizens regarding privacy.

The independent regulatory model is worthy of consideration if the specific goal of a federal privacy agency would be to address privacy-related matters in the public *and* private sectors. If implemented, this model has the potential to be a very active regulator of private information in the hands of both private businesses and public organizations. However, an independent regulatory agency could be hampered in its functions if too many exceptions are made to the regulatory powers of the agency.

4.5. The ombudsman model

The ombudsman privacy agency is a part of the executive branch. The privacy agency makes recommendations on privacy issues to the legislature. The privacy agency works primarily as an ombudsman between state agencies, private organizations, and members of the public. The ombudsman privacy agency gives opinions, assistance, and advice to all who make inquiries to the agency, regardless of the nature of the individual or organization making that inquiry. The ombudsman privacy agency hears claims regarding privacy issues by the members of the public and can issue orders to protect privacy rights.

New York's Committee on Open Government, which works on issues of privacy, open government, and freedom of information, offers an example of the ombudsman approach.[42] The Committee is an intermediary and a liaison between all parties in the state involved in privacy issues. It works with the government agencies, the members of the public and private organizations, offering advice and assistance to any party who seeks the assistance of the agency. It will investigate appeals by the members of the public involving privacy and data issues. Further reinforcing the ombudsman nature of the Committee, some of its members are appointed by the Governor, some of its members are appointed by the legislature, and other serve as part of their responsibilities within a government position.

The ombudsman model offers a number of issues for analysis and could be applied in two distinct ways. The ombudsman model has the potential to include all potential parties with interests in privacy issues. In the United States, an ombudsman privacy agency could work simultaneously with federal agencies, state governments, members of the public, and private sector organizations in addressing privacy-related issues. Such an agency could meet a number of privacy-related needs by hearing privacy-related claims, by offering opinions and advice, and by facilitating solutions. To do this effectively a substantial amount of trust and respect would first have to be built by the agency and its staff, which can only be earned over time and by gaining a thorough expertise that is recognized by all potential parties. Implementing this model alone, however effective it may otherwise be, will nevertheless be quite limited in its influence compared to an agency that has powers of investigation and enforcement.

A different, though not mutually exclusive, application of the ombudsman model would be an agency functioning as an ombudsman between the state privacy agencies. In such an ombudsman capacity, a federal privacy agency could work with the state privacy agencies to bring a greater sense of uniformity to privacy protections among the states. The federal

agency could ensure certain levels of privacy protection across the states by working to bring consensus among the states about privacy concerns. As with the harmonizing model, states' rights could become an issue.

4.6. The oversight model

The oversight model describes a privacy agency that is designed to oversee all government-related activities that effect privacy. The oversight privacy agency is appointed by the executive branch, but is independent in its functions. It advises the legislature on privacy issues that relate to proposed and future legislation. The oversight agency works as an ombudsman between the members of the public and government organizations on all issues related to privacy. Members of the public can file privacy-related complaints about government activities to the agency. The oversight agency can issue orders compelling government agencies to comply with privacy laws; these orders can be appealed to the judiciary.

The Freedom of Information Commission of Connecticut, although it's work involves more than privacy issues, is an example of the independent regulatory approach.[43] The members of the Commission are appointed by the Governor, but act as independent advisors for the state legislature. Along with advising the legislature on privacy issues, the Commission acts as on ombudsman between members of the public and state agencies on information issues. The Commission oversees the compliance of state agencies with privacy laws and policies, and can issue orders to an agency to compel compliance, though enforcement powers for these privacy orders is lacking.

The oversight model offers a broad array of considerations in the way in which it could be implemented. An oversight agency could be created at the federal level with oversight over the activities of federal agencies, of state governments, of private sector organizations, or of any combination of the aforementioned. However, the main lesson to be drawn from Connecticut's experiences with the oversight model is that, to operate effectively, an oversight agency needs to have enforcement powers. Its lack of such power regarding personal data protection has left that area subject to the uncertainties and inefficiencies of private causes of action. As a result, there is little agency oversight of personal data privacy in Connecticut. In contrast, the agency's well-defined, affirmative powers regarding freedom of information oversight has led to a set of practices statewide that are essentially consistent with the state's overall FOI policy.

4.7. The strong investigatory model

The strong investigatory privacy agency is appointed by the executive branch and also is administratively attached to the executive branch. The strong investigatory privacy agency oversees the privacy-related activities of government agencies. It hears complaints from members of the public and investigates the activities of government agencies. Government organizations can seek the advisory opinions of the privacy agency. The privacy agency issues advisory opinions to both state organizations and members of the public.

Hawaii's Office of Information Practices is a strong investigatory privacy agency that is part of the executive branch.[44] The Office reports to both the legislature and the Governor.

Members of the public file complaints about state agency activities with the Office, which can issue advisory opinions or take actions including compliance inquiries, investigations of possible violations, examinations of records, or recommendations of disciplinary action. This range of options for the Office allows it to make substantial investigations of compliance with privacy laws and policies. The Office also offers advisory opinions to state agencies that seek the assistance of the Office.

The strong investigatory model is worthy of consideration for the fact that it facilitates the involvement of and the interaction between many different parties involved in privacy-related issues, while also having the ability to enforce privacy protection. The strong investigatory model allows a privacy agency to work in an advisory role on privacy matters, but also to investigate and enforce privacy rights when violations occur. At the federal level, a strong investigatory privacy agency would have the potential to be very active and involved in the privacy-related issues involving the public and government agencies.

5. Issues for consideration regarding a centralized governmental structure for privacy protection

The most significant initial issue of centralized privacy protection structures involves whether the effort to design and implement a structure is worthwhile. A considerable number of governments have adopted centralized privacy protection structures, with the EU system being the most prominent and influential. Many of these governments are somewhat wary of dealings with states that lack such protections; the EU restrictions on economic activity with organizations located in nations lacking protections is a prime example. For a government and for the organizations located in that state, the lack of a centralized privacy protection structure can create the risk of a significant economic impact. Corporations based in states without centralized structures for privacy protections may be at risk of losing business transactions or entire markets as a result of the lack of protections.

In 2001, for example, the total value of business transactions requiring the transfer of personal data between the United States and the EU was approximately $125 billion.[45] If the lack of centralized privacy protection structure in the United States became an issue with the EU Data Directive, as it very well could, the amount of business threatened in both the United States and the EU could be staggering. For this reason alone, the adoption of a centralized privacy protection structure is worthy of consideration.

Beyond the immediate economic consequences, the lack of a centralized government structure for protecting privacy has the potential to lead to political and economic isolation. Much recent legal scholarship is relevant to considering the potential impacts of the United States lacking a coherent system of privacy protection when many of its major trading partners have one.[46] In this context, the primary concern is that the lack of a privacy protection system will eventually politically and economically isolate those states from those that do have them. This isolation could result from economic restrictions, such as can be found in the EU Data Directive, or from political concerns, such as lack of faith in a government that is not willing to provide equitable privacy protections. Since globalization and technology are continually increasing the interconnectivity of information across na-

tional boundaries, a nation may not really have the option of not taking action in the global information society.[47] Others may perceive a state that takes no action to implement a centralized privacy protection structure as self-isolating from the world economy.

Part of the potential problem with isolation results from how a state without a centralized privacy protection structure is perceived by states that do have one. The United States provides an interesting example of this point. The sectoral approach to privacy taken by the United States federal government has likely created some negative perceptions about the nation's commitment to privacy. Though the *Privacy Act of 1974* created the first real international standard for privacy rights, the United States has since not pursued federal privacy protection with the same vigor as many other nations. For example, it is most curious that the United Stated federal government has taken decisive action to protect video rental records,[48] but has not passed legislation regarding the drastically more important issue of health care records. This emphasis of legal protection on minor concerns could certainly cause other governments to question the United States government's commitment to privacy protection.

Though the practical realities of privacy protection structures cause significant economic issues for both private organizations and government organizations, the effects of centralized governmental privacy protection structures on multinational corporations can be more than economic. When some states have centralized privacy protection structures and others do not, all multinational corporations are left having to grapple with the differing levels of requirements, which can have a negative impact on the efficiency and effectiveness of the business. The lack of uniformity regarding privacy protection can delay business transactions and operations, even causing potential difficulties in everything from the recruiting of employees to the mundane exchange of business cards.[49] Mutlinational corporations located in every nation would benefit in numerous ways from a more coherent adoption of centralized privacy protection structures across states.

Despite these rather significant concerns about the lack of a centralized privacy protection structure, a state need not necessarily feel forced to create a centralized privacy protection structure. The same revolution in technology that has raised a great number of new concerns about information privacy may also, in the end, become the single best way to protect information privacy. Any new technological advance could be one that further erodes information privacy or it could be one that dramatically increases information privacy. At this early stage of the development of Internet technology, it is uncertain what will eventually become the technological standard and what level of privacy protection that standard will provide. Although an adequate level of protection of information privacy is hardly guaranteed by the ongoing technological revolution, it is important not to lose sight of the fact that the current technology is still developing at an incredible pace. Making laws to protect information privacy in terms of current technology might be unnecessary, as the technology may create stronger information privacy protections than legislation could.

Current technology could also be used to increase privacy protections in such a way as to reduce the need for centralized privacy protection. In the United States, the federal government could use certain agencies to actively and aggressively promote privacy self-protection by citizens, providing education, training, and access to privacy protection software. For

example, the FTC, as an agency likely to have an interest in such issues, could use its website to promote ways to protect against technology-based invasions of privacy. The FTC could also provide instruction on how to find and properly use security software and technology. This strategy might have a dampening effect on need for the creation of a centralized privacy protection structure. However, it is highly unlikely that such a program would make a great difference as it has sizeable unresolved flaws, as such a program would only be as effective as the software and training available on the website. More significantly, it would not be a centralized governmental attempt to protect privacy.

Ultimately, the options for the government without a centralized privacy protection structure are multiple and divergent. A government could choose to do nothing about the issue, to take limited action, or to do a great many things to attempt to address privacy concerns at the structural level. A government could decide not to take any action, hoping that the privacy protection issues will be solved through nongovernmental means, such as new technology providing a solution to privacy concerns, self-regulation by private and government organizations providing a solution to privacy concerns, or market-based forces dictating a solution to privacy concerns. In opting to take limited action, a government could introduce some legislation or regulations, without implementing a centralized government privacy protection structure, to guide private and government organizations into action over privacy concerns. Lastly, a government could choose to create a centralized privacy protection structure governing the activities of private organizations, government organizations, or both. In such a case, the issue would be what type of structural model the government would decide to implement.

A government choosing to implement a centralized privacy protection structure will have to seriously consider the structural model on which to base the privacy protection, as well as the legal placement of that structure. A centralized privacy protection structure can be based on laws establishing rules for those who are collecting and processing personal information, on laws establishing government interventions into activities involving personal information, or on laws creating incentives to properly collect and process personal information. The legal framework for the centralized government structure for privacy protection also will need to determine whether the structure will be applied in a sectoral manner, a multisectoral manner, or a comprehensive manner.

In establishing a centralized privacy protection structure, a government will have to consider whether they desire to address the issue of harmonization. As there are so many different kinds of centralized privacy protection structures, with so many different rules, the lack of harmonization between centralized privacy protection structures on the international level is considerable. Attempting to harmonize with other centralized privacy protection structures would serve to avoid potential conflicts with the privacy protections of other nations, would serve to facilitate international commerce in the state, and would help organizations based in the state conduct business internationally. However, attempting to harmonize with other states leads to the problem of which states to try to harmonize with. A state could choose to harmonize with a structure most compatible with its own government or could choose to harmonize with the most prevalent or influential international centralized privacy protection structure. Many states have already chosen the later route by adopting the influential EU model.

6. Applications and implications for the United States federal government

If the United States was to implement a centralized privacy protection structure, there are several models that would be most worth considering. In fact, there are very compelling reasons that make the use of the federal-state model and the harmonizing model essential in a centralized privacy protection structure for the United States federal government. Beyond those two essential models, the federal government would have several other options for the design of the centralized privacy protection structure.

The United States government was formed so that the federal government and the individual state governments have separate powers and duties. The federalist nature of the government will have a significant impact on the centralized privacy protection agency. As a result, the use of a federal-state model would be the first necessary component of a federal centralized privacy protection structure. In order to preserve states' rights, each individual state should be allowed their own privacy protection agency, whether that means keeping one that already exists or creating one. The federal privacy protection agency must function in a manner so that its efforts will parallel and enhance the efforts of the state agencies. The federal agency should also provide a certain quantity of privacy rights and protections without conflicting with the activities of the states.

Along with the federal-state model, the federal centralized privacy protection structure would also need to employ the harmonizing model as applied to the states. The federal centralized privacy protection structure would need to mandate some level of privacy protection by the states and coordinate activities between the state agencies beyond simply complimenting their efforts. This situation would necessitate applying the harmonizing model to the individual states. The harmonizing model would have to be used in such a manner that it directed the states to guarantee a certain basic amount of privacy protection at the state level, as well as a state structure to enforce that protection, without impinging on the Constitutionally guaranteed rights of the states.

Further, the use of the harmonizing model as applied to other nations, although not necessary, would be very important. Attempting to harmonize privacy protection policies with those of other nations can produce some very positive results, such as the facilitating of business activities between companies in different nations and avoiding conflicts with other nations regarding privacy issues. The United States could benefit from implementing the federal centralized privacy protection structure so that it harmonizes with the EU privacy protection structure in order to facilitate business transactions with the EU nations and all non-EU nations following the EU structure. Ultimately, harmonizing with the EU would help avoid potential problems that could cause "economic chaos for U.S.-based businesses by halting all personal data flow from the Member States."[50]

Beyond the necessary implementation of the federal-state model and both approaches of the harmonizing model, the United States federal government would have many other options for establishing the centralized privacy protection structure. Any other option would be to compliment and enhance the structure based on the federal-state and harmonizing models. The structure could also employ a traditional regulatory model or an ombudsman model or another model, depending on the goals of the federal centralized privacy protection structure, as well as the types of privacy protections offered and the means for enforcement

of those protections. The other models employed in the structure would depend greatly on the types of privacy protection offered by the government and how those privacy protections were enforced.

Structural organization is one of the primary components of a governmental privacy protection system. If the United States federal government is to offer centralized privacy protection at a level similar to what appears to be becoming the international standard, the structural organization for privacy protection must be appropriate to the federalist nature of federal government and recognize the existing privacy policy framework of the federal government. The current sectoral nature of privacy policy in the United States and the existing structure to implement that policy, however, impairs effective privacy protection for the country's citizens. Thought should be given to moving to a more centralized governmental structure for privacy protection.

Acknowledgments

Some initial ideas for this article arose from the authors' work on the study *Review and Analysis of Privacy Issues.*[51] The ideas presented here, however, were developed independently by the researchers of the Information Use Management and Policy Institute at Florida State University and were not part of the Grant Thornton final report.

Notes

1. Grant Thorton. (2002). *Review and analysis of privacy studies and issues: A report to the General Accounting Office.* Washington, D.C.: Grant Thorton.
2. Kast, F. E. & Rosenzweig, J. E. (1985). *Organization & management: A systems contingency approach*, 4th ed. New York: MacGraw Hill
3. *Privacy Act of 1974*, 5 U.S.C. §§ 552(a).
4. *Telephone Consumer Protection Act of 1991*, 47 U.S.C. § 227.
5. *Driver's Privacy Protection Act of 1994,* 18 U.S.C. § 2721.
6. *Video Privacy Protection Act of 1988*, 18 U.S.C. § 2710.
7. Article 29 Working Party. (2001). *Fourth Annual Report: On the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the community and in third countries, adopted on 17.5.2001.* 5019/01/EN WP 46, p. 15. Available at: ⟨*http://www.europa.eu.int*⟩.
8. Assey, J. A. & Eleftheriou, D. A. (2001). *The EU-U.S. Privacy Safe Harbor*, 9 Commlaw Conspectus 145; and George, B. C., Lynch, P., & Marsnik, S. F. (2001). *U. S. Multinational Employers: Navigating through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive.* 38 Am. Bus. L. J. 735.
9. Safe Harbor Principles issued by U.S. Department of Commerce. Available: ⟨*http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm*⟩.
10. Article 29 Working Party, note 7 above, p. 17.
11. Cooley, T. (1880). *Law of torts.* Chicago: Callaghan & Co.

12. Cooley, note 11 above, p. 29.
13. *DeMay v. Roberts,* 46 Mich. 160; 9 N.W. 146 (1881).
14. Warren, S. D. & Brandeis, L. D. (1890). *The Right to Privacy.* 4 Harv. L. Rev. 193, p. 215.
15. *Pavesich v. New England Life Insurance Company,* 122 Ga. 190 (1905).
16. Prosser, W. L. (1960) *Privacy,* 48 Cal. L. Rev. 383.
17. Turkington, R. C. and Allen, A. L. (1999). *Privacy: cases and materials.* West Group: St. Paul, Minnesota, p. 61.
18. *Griswold v. Connecticut,* 381 U.S. 479 (1965); *Loving v. Virginia,* 388 U.S. 1 (1967); *Eisenstadt v. Baird,* 405 U.S. 438 (1972); *Roe v. Wade,* 410 U.S. 113 (1973); *Whalen v. Roe,* 429 U.S. 589 (1977); *Planned Parenthood v. Casey,* 505 U.S. 833 (1992).
19. Westin, A. (1967). *Privacy and freedom.* New York: Atheneum, p. 7.
20. Gavison, R. (1980). *Privacy and the limits of the law,* 89 Yale L. J. 421, pp. 427–440.
21. Doty, P. (2001). Digital privacy: Toward a new politics and discursive practice. In M. E. Williams (Ed.) *Annual Review of Information Science and Technology.* Medford: NJ: Information Today, pp. 115–246; Frye, C. D. (2001). *Privacy-enhanced business: Adapting to the online environment.* London: Quorum Books; and Cody, J. P. (1999). *Protecting Privacy over the Internet: Has the Time come to abandon Self-Regulation?,* 48 Cath. U. L. Rev. 1183.
22. Frye, note 21 above; and Cody, note 21 above.
23. Turkington and Allen, note 17 above, p. 75.
24. Wacks, R. (1989). *Personal information: Privacy and the law.* Clarendon Press: Oxford, p. 26.
25. Michalski, W. (1999). *21st century technologies: A future promise.* Available: ⟨*http://www.oecdobserver.org/news/fullstory.php3?aid=48*⟩.
26. Friedman, D. (2000). Privacy and technology. In A. F. Paul, F. D. Miller, and J. Paul (Eds.) *The right to privacy* (pp. 186–212). New York: Cambridge University Press pp. 186–187.
27. Roberts, A. (2001). *Structural Pluralism and the Right to Information,* 51 U. Toronto L. J. 243.
28. Hays, C. L. (1999). Variable-price coke machines being tested, *N.Y. Times,* Oct. 28, 1999, at C1.
29. Schwartz, P. (2000). *Internet Privacy and the State,* 32 Conn. L. Rev. 815, p. 815.
30. Smith, B. L. (2001). *The Third Industrial Revolution: Policymaking for the Internet,* 3 Colum. Sci. & Tech. L. Rev. 1, p. 4.
31. European Union Data Protection Directive of 1995. *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data.* Official Journal L 281, 23/11/1995. Available: ⟨*http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html*⟩. EU privacy policy statements and other relevant EU documents on privacy and data protection are available at ⟨*http://europa.eu.int/comm/internal_market/en/dataprot/index.htm*⟩.
32. Litan, R. E. (2001). *Law and Policy in the Age of the Internet.* 50 Duke L. J. 1045, p. 1062.

33. European Union Data Protection Directive of 1995, note 31 above, article 1.
34. Frye, note 21 above; and Blackmer, S. (1998). *"The European Union Data Protection Directive" (paper presented at the Privacy & American Business Meeting on Model Data Protection Contracts and Laws, February 1998).* Available at: ⟨*http://privacyexchange.org/tbdi/EU_PDR/blackmerdirective.html*⟩ (March 21, 2002).
35. Office of Privacy Protection. (2002). Available: ⟨*http://www.privacyprotection.ca.gov*⟩.
36. Privacy Commissioner of Canada. (2002). Available: ⟨*http://www.privcom.gc.ca*⟩.
37. European Union Data Protection Directive of 1995, note 31 above.
38. U.S. Constitution, article 1, section 8.
39. U.S. Constitution, article 1, section 8(3).
40. U.S. Constitution, 10th Amendment.
41. Italian Data Protection Commission. (2002). Available: ⟨*http://astra.garanteprivacy.it/garante/HomePageNs*⟩.
42. Committee on Open Government. (2002). Available: ⟨*http://www.dos.state.ny.us/coog/coogwww.html*⟩.
43. Connecticut Freedom of Information Commission. (2002). Available: ⟨*http://www.state.ct.us/foi*⟩.
44. Office of Information Practices. (2002). Available: ⟨*http://www.state.hi.us/oip*⟩.
45. Lawson, S. (March 28, 2001). *Analyst: Multinationals lack uniform privacy law*. Available: ⟨*http://www.cnn.com/2001/TECH/industry/03/28/privacy.headches.idg/index.html*⟩.
46. For a range of examples, see Assey & Eleftheriou, note 8 above; Tan, D. R. (1999). *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the U.S. and the EU*, 21 Loy. L. A. Int'l & Comp. L. J. 661; Blanke, J. M. (2000). *Safe Harbor and the EU's Directive on Data Protection*, 11 Alb. L. J. Sci. & Tech. 57; Sunosky, J. T. (2000). *Privacy Online: A Primer on the EU's Directive and the United States' Safe Harbor Privacy Principles*, 9 Currents Int'l Trade L. J. 80; Cate, F. H. (1999). *The Changing Face of Privacy Protection in the EU and the U.S.*, 33 Ind. L. Rev. 174; Monahan, P. A. (1998). *Deconstructing Information Walls: The Impact of the EU Directive on the Protection on U.S. Business*, 29 L. & Pol'y Int'l Bus. 275; and Myers, J. M. (1997). *Creating Data Protection Legislation in the U.S.: An Examination of Current Legislation in the EU, Spain, and the U.S.*, 29 Case W. Res. J. Int'l L. 109.
47. Marsden, C. T. (2001). *Cyberlaw and International Political Economy: Towards Regulation of the Global Information Society*, 2001 Det. C. L. Rev. 355.
48. *Video Privacy Protection Act of 1988*, note 6 above.
49. Lawson, note 45 above.
50. George, Lynch, & Marsnik, note 8 above, p. 736.
51. Grant Thorton, note 1 above.