

# MANAGING GLOBAL DATA PRIVACY

## ■ Paul M. Schwartz

A Report from

*Research • Report • Improve*

the **PRIVACY**.org  
PROJECTS



## **Preface by Richard Purcell, Executive Director**

What is needed to advance privacy protections in the Information Age where the world may be flatter, but is also more complex? Globe-shrinking technologies that have enabled us to communicate, collaborate and share work are also mind-bogglingly complicated to explain.

Consumers want their purchase transactions to be fast, reliable and cheap. They also want commercial operators to treat personal data with respect and to protect it from harm. And if that means imposing government mandates, that's fine as long as the fast/reliable/cheap model is still in place. Is that possible?

As technologies shrink the world, enabling transactions to happen anywhere, anytime, by anyone on the planet quickly and accurately, how can we expect laws that are bounded by country borders to protect our personal information from being intercepted and exploited? Who touches the data? Who is accountable for its protection?

In this inaugural study, The Privacy Projects has asked these questions of Professor Paul M. Schwartz, the noted privacy law expert at UC Berkeley School of Law. Together, we assembled case studies of global data flows from six major multi-national companies in the United States and Canada. Our purpose in this exercise is to better understand how well the laws governing personal information protection address the explosion of world-wide data transfers enabled by advanced communications technologies.

These laws were developed in the mid-90's when companies managed centralized data bases and moved information from one point to another in ways similar to moving packages from one address to another. Do they remain relevant in a world of global communications, online processes, and outsourced business processes? Do legislators and data protection regulators have sufficient information to review the current laws and regulations to identify areas for improvement? Beyond the laws, are the data management procedures reliable for privacy and data protection?

The Privacy Projects was founded in 2009 to research and report on just these kinds of issues. In this report, we found that the world has changed in three dramatic ways. The scale of data transfers crossing national boundaries has massively increased. Each of the case studies reveals data volumes of huge sizes moving under company controls. The way these data flows are managed has also changed from predictable, observable events to dynamic, process-oriented procedures. And the management of these flows has also changed from a model of ad hoc oversight to one involving teams of professionals collaborating under an accountability model to provide value and manage compliance.

We conclude by identifying challenges to better laws and corporate safeguards based on our findings. Challenges breed opportunities; we welcome the dialogue for improvements in personal information management and protection.

**Managing Global Data Privacy:  
Cross-Border Information Flows in a  
Networked Environment**

**By Paul M. Schwartz  
UC Berkeley School of Law**



# Table of Contents

## I. Overview

## II. Executive Summary

## III. Critical Themes and Analysis

### A. A Change in Scale: Multipoint, Continuous Data Transfers with an Expanded Number of Participants

1. From the Past to the Present: Fiat-France, the Deutsche Bahn, and the Landscape Today
2. Examples from the Case Studies

### B. A Change in Processing: Dynamic Data Transfers and Networked Series of Processes

1. From the Past to the Present: Palmisano on the Contemporary Corporation, Coase on "Make or Buy," and the Rise of the Cloud
2. Examples from the Case Studies

### C. A Change in Management: The Professionalization of Corporate Data Protection and the Shift to a Process-Oriented Approach

1. From the Past to the Present: the Smith Study and the Rise of the Chief Privacy Officer
2. Examples from the Case Studies

### D. New Paths to High Levels of Data Protection?: The Call for Accountability and the Rise of Process-Oriented Corporate Safeguards

## Appendix A: Methodology

## Appendix B: Case Studies

1. Alpha Corporation
2. Beta Corporation
3. Gamma Corporation
4. Delta Corporation
5. Epsilon Corporation
6. Zeta Corporation

## Appendix C: An Illustrative Data Flow from the Zeta Hiring System

## About the Author

## About The Privacy Projects

## I. Overview

The Privacy Projects (TPP) is a non-profit organization dedicated to improving the practice of privacy by developing and promoting privacy standards and the trusted management of personal information in the networked environment. TPP focuses on privacy policies and practices, technology tools, education, and outreach programs through research, analysis, and dialogue.

This Report is TPP's inaugural study. It concentrates on the processes and controls implemented by six leading companies to protect personal data when transferring such information across national boundaries. The companies in the study are:

- a pharmaceutical company (Alpha Corporation);
- a marketing services company (Beta Corporation);
- a diversified financial services company (Gamma Corporation);
- a developer and provider of Internet-based software and online services (Delta Corporation);
- a provider of technology solutions and services for a range of customers, including consumers, the public sector, and businesses (Epsilon Corporation); and
- a globally integrated enterprise that helps public and private sector organizations through the use of business insight and advanced technology solutions (Zeta Corporation).

The study depicts the use by companies of international data transfers that take place in a multidirectional and a highly dynamic fashion. These new kinds of global data networks raise a series of challenges to and provide new kinds of opportunities for existing regulatory paradigms.

## II. Executive Summary

This Report examines the processes and controls implemented by six leading companies to protect personal data when transferring such information across national boundaries. It is built on a series of structured self-reported case studies. The companies in the study are:

- a pharmaceutical company (Alpha Corporation);
- a marketing services company (Beta Corporation);
- a diversified financial services company (Gamma Corporation);
- a developer and provider of Internet-based software and online services (Delta Corporation);
- a provider of technology solutions and services for a range of customers, including consumers, the public sector, and businesses (Epsilon Corporation); and
- a globally integrated enterprise that helps public and private sector organizations through the use of business insight and advanced technology solutions (Zeta Corporation).

These are all companies who have invested resources in data privacy and security issues, and who were also willing to talk about these practices by participating in this project. The potential of this Report is to open a valuable window into the professed practices of a set of companies who are actively seeking to develop responsible privacy and security practices.

The case studies demonstrate a dramatic set of changes from the past paradigm of international data transfers by private organizations. The changes fall into three groups. The first group of changes concerns the continuous, multipoint nature of modern international data flows. There has been massive growth in the complexity and volume of these transfers. Thus, the first transformation concerns a change in scale.

The second transformation concerns a change in the nature of information processing at companies. Data transmissions are no longer point-to-point transactions; they occur today as part of a networked series of processes made to deliver a business result.

The third change is one in management. There has been a professionalization of corporate data protection and a shift to a process-oriented management approach. These changes in international data transfers raise new challenges and opportunities for data protection law. In the 21<sup>st</sup> century, a necessary task for a data protection regulatory regime will be to find meaningful and effective ways to focus on privacy outputs rather than specifying each managerial input. This summary will now briefly

consider each of the three changes to the past model of international data transfers and conclude with analysis of the new challenges for data protection regulation.

**A Change in Scale.** The first change in the established past paradigm of data flow concerns the fashion in which data flows now occur through many points. The initial change is one of scale. In the recent past, companies generally worked with discrete, localized data sets and processes. In that model, an international data flow was an occasional event, an exception and not the rule, and data processing systems were generally nationally-based. Moreover, from a contemporary perspective, the past transfers were relatively static events, that is they did not occur continuously, and also involved a fairly limited number of participants in the processing.

**A Change in Processing.** The second group of changes from the classic paradigm of data processing concerns the new ability of international data transfers to be made dynamically as well as the increased ability of processes to be networked. In the past, companies typically finalized data transfers in advance and databases were centralized. In that past model, an international data flow occurred at a predictable moment and into a database controlled by a single entity. The process of transmission was straightforward. Today, in contrast, data transmissions occur as part of a networked series of processes made to deliver a business result.

New technologies and accompanying new business models now allow firms to approach their operations in innovative ways. Different functions and operations can be packaged as modular units that can be pulled apart and re-assembled. Today's technology for processing information permits flexibility for the firm that was previously unknown. The flexibility concerns decisions about how, when, and to what extent to structure relationships within a company's walls, and how, when, and to what extent to draw on outside parties and the market. In particular, data flows can be de-aggregated and de-coupled to allow companies to develop novel business approaches to operations and activities.

Firms also have greater flexibility than ever before in deciding on the shape and form of the work itself, that is, how they will distribute processes and services. As an example, transfers of personal data occur increasingly on demand. Modern information systems respond to data requests rapidly and in many instances in real time. Data flows are also more international than before because of the global nature of data networks. After all, the first "W" in WWW stands for "world" — there is now a data web that spans the earth. The latest manifestation of these developments in IT is the "cloud."

Cloud computing is the location of computing resources on the Internet in a fashion that makes them highly dynamic and scalable. The result of this distributed computing environment is to permit dramatic flexibility in processing decisions -- and on a global basis. For example, computing activities can be shifted from country-to-country depending on load capacity, time of day, and a variety of other concerns.

**A Change in Management.** In the recent past, modern corporations largely avoided privacy and security issues and devoted a low level of resources to them. Moreover, to the extent that such issues arose, companies had an ad hoc, reactive approach to handling personal information. Today, there has been a professionalization of corporate data protection, which, in turn, has been accompanied by a greater investment of business resources in this area. There has also been a shift to a new process-oriented management approach. Companies now seek to develop forward-looking systems for managing data flows and training personnel. Thus, the third transformation in this area concerns the management of privacy and security.

Many corporations have come today to view information privacy as important and worthy of ongoing attention. These organizations have increased investment in this area, and also sought to assign the development and management of privacy policy to specific employees, who, in turn, increasingly self-identify into categories such as Chief Privacy Officers, or Chief Security Officers. There is even a professional organization for privacy executives, the International Association of Privacy Professionals, which has over 6,000 members across fifty countries. Today, the investment in privacy and security in corporations has also increased. In sum, there is both a greater specialization of those who manage privacy and security, and a greater investment in it.

**New Paths to High Levels of Data Protection?** The final section of this Report's analytical section draws a connection between the case studies and a current policy discussion in data protection law that seeks to use organizational accountability as a touchstone.

Some of the most interesting recent voices in discussions about data protection law offer perspectives regarding the need for "modernization" of data protection law as well as for "accountability" as a central principle regarding international data transfers. There is an important connection to be made between the new interest in accountability and a corporate privacy culture focused on a process-oriented approach. The case studies in this report focus on safeguards being built-in to data processing management. Companies are now putting internal policies in place, centered on forward-looking rules of information management and training of personnel. Such policies are, at the least, a necessary precondition for an effective accountability regime that develops a high level of privacy protection.

The key to the merits of an accountability regime will be in the details of any regulation. Nonetheless, a challenge for a data protection law in the 21<sup>st</sup> Century will be to consider how to shift its safeguards and requirements to focus on organizational privacy outputs rather than managerial inputs. As an example, detailed registration requirements for data processing are unlikely to raise the level and quality of data protection. Rather, regulators might consider an approach that requires companies to develop effective privacy programs and policies and then monitors whether these

requirements are followed. A critical question for regulators, lawmakers, policymakers, and scholars is how to maintain information privacy law at a high level that responds in a meaningful fashion to the challenges and opportunities of global networked data flows.

### III. Critical Themes and Analysis

This Report contains anonymous case studies of the management of international data transfers at six leading companies. To inform the international regulatory and policy debate about data privacy and security, it provides detailed descriptions of these global data processing activities. The case studies of this Report demonstrate a dramatic set of changes from the past paradigm of international data transfers by private organizations. These changes fall into three groups.

The first group of changes concerns the continuous, multipoint nature of modern international data flows. There has been a massive growth in the complexity and volume of these transfers. This first transformation represents a change in scale.

The next section considers how companies now make these international transfers dynamically, and through an increasingly decentralized location of networked databases, services, and processes. This second transformation concerns a change in the nature of information processing at companies. For these companies, data transmissions are no longer point-to-point transactions; they occur today as part of a networked series of processes made to deliver a business result.

The third change is one of management. There has been a professionalization of corporate data protection and a shift to a process-oriented management approach.

The changes in the nature of data processing in the contemporary corporation and in the management of these processes raise new challenges to and opportunities for data protection law. The goal should be to develop strong and effective protections for privacy that reflect these changes in a meaningful fashion. The fourth and final section of this part of the Report analyzes the resulting challenges — ones shared by regulators, companies, policy advocates, and privacy scholars in developing a data protection law for the 21<sup>st</sup> century.

To understand this project's goals and some of its limitations, one must first, however, know something about its background and approach. This Report is built on a series of structured self-reported case studies. It focuses on the practices of companies who have invested resources in data privacy and security issues, and who were also willing to talk about these practices by participating in this project. Detailed information about the criteria for selecting companies and the methodology used for eliciting information follows in Appendix A.

Each of the three thematic sections identifying major changes in international data flows is followed by relevant extracts, in anonymous form, from the individual case studies. The reader may wish, however, to read all the thematic sections first, and only then turn to the complete case studies, which follow at the end of the Report in Appendix B. Whether the reader reads the extracts from each case study after each thematic section or the full case studies at the end of the report, she will be able to

learn much about practices and processes at the participating companies, from Alpha Corporation to Zeta Corporation.

This Report depicts companies that view themselves as "good apples" and wish their practices to inform the policy debate about international data transfers. It seeks neither to capture an empirical sample of all companies involved in international data transfers, nor to calculate the volume of data transfers globally. It also is not based on any independent audit of the participants' assertions. The potential of this project is to open a valuable window into the professed practices of a set of companies who are actively seeking to develop responsible privacy and security practices. As a final introductory matter, I wish to note that any opinions or conclusions in the analytic section or elsewhere are solely my own, and should not be attributed to the individual companies, or The Privacy Projects. We now turn to the first set of findings.

## **A. A Change in Scale: Multipoint, Continuous Data Transfers with an Expanded Number of Participants**

The first change in the established past paradigm of international data transfers concerns the fashion in which data flows now occur through many points. In the recent past, companies generally worked with discrete, localized data sets and processes. In that model, an international data flow was an occasional event, an exception and not the rule, and data processing systems were generally nationally-based. Moreover, from a contemporary perspective, the past transfers were relatively static events, that is they did not occur continuously, and also involved a fairly limited number of participants in the processing.

To trace these transformations, I wish first to discuss two past events, now an established part of the history of data protection law. The first concerns a data transfer of HR data in 1989 from Fiat-France to its parent corporation in Italy. The second one involves the Deutsche Bahn credit card, developed in 1995 in conjunction with Citibank. The resulting personal information of customers in Germany was to be processed in the United States. These historic examples show two data protection authorities acting in a suitably pro-active fashion to protect information privacy. The examples also demonstrate how much has changed in international data transfers in a relatively short time frame.

## 1. From the Past to the Present: Fiat-France, the Deutsche Bahn, and the Landscape Today

In 1989, Fiat-France sought to transmit HR information about its employees to its parent company, which was located in Turin, Italy.<sup>1</sup> This data transfer was to take place at a time when Italy had not yet enacted a national data protection statute. The CNIL intervened and issued a formal declaration that required Fiat-France and Fiat-Italy to sign a contract before the transfer could occur. In this contract, the entities were to pledge to provide "the protections for human rights and fundamental liberties" of the Council of Europe's privacy convention as well as of the national French data protection law.<sup>2</sup> Once the two Fiat entities signed the appropriate contract, and showed it to the CNIL, the French data protection agency gave them its formal approval, which was marked by a "receipt" (*récépisse*) that allowed the transfer.<sup>3</sup>

By the mid-1990's, international data flows were already more common an event and already more complicated. A leading example from that era involves a credit card that the Deutsche Bahn, the German railroad authority, offered in 1995 to its customers. The railroad wished to add a credit card function to its BahnCard, a membership card which allowed railway customers who paid a yearly membership fee to obtain discounts up to fifty percent on train tickets.<sup>4</sup> Building on the BahnCard, the Deutsche Bahn sought to create an affinity credit card in partnership with Citicorp Card Operations, an affiliate of Citibank. Resulting credit card information was to be processed in the United States.

The Berlin Data Protection Commissioner responded to this plan by requiring Citibank and the Deutsche Bahn to sign a contract agreeing to meet the requirements of German data protection law for all processing in the U.S. In particular, Citibank agreed to restrict any use of BahnCard customers for marketing purposes to certain strict limits and to refrain from marketing to customers who had chosen to have a BahnCard without the credit card option.<sup>5</sup> Moreover, customers with the credit card were given the right to receive access to their stored information, to have their data erased, and to obtain damages, should a legal harm occur, from both the Deutsche Bahn and Citibank. Finally, the contract gave the Berlin Commissioner for Data Protection the right to inspect Citibank's data processing operation in the U.S.<sup>6</sup>

---

<sup>1</sup> Commission nationale de l'informatique et des libertés, 10e rapport d'activité 32 (1989).

<sup>2</sup> Id. at 32-24.

<sup>3</sup> Id. at 32. For a discussion, see Paul M. Schwartz, European Data Protection Law and Restrictions on International Data Flows, 80 Iowa L. Rev. 471, 491-92 (1995).

<sup>4</sup> Berliner Beauftragter für Datenschutz und Informationsfreiheit, 25 Jahre Datenschutz, 5 Jahre Informationsfreiheit in Berlin 34-35 (2004).

<sup>5</sup> Id.

<sup>6</sup> Id.

These two events show data protection authorities acting to protect privacy when the respective laws did not contain detailed safeguards regarding international data flows. These incidents also reveal much about the extent to which the nature of international data flows has changed. As the case studies in this Report demonstrate, international data transfers today are not a finite event, as in the Fiat example, but take place on a continuous basis. Moreover, these data transfers no longer occur from one point to another, as in the Fiat and Deutsche Bahn-Citibank examples. In the first case, personal data were sent from branches of the same company in France to Italy. In the second example, the Berlin Data Protection Commissioner evaluated a data transfer that would go from two different companies, but again only from Point A, a Deutsche Bahn database in Germany, to Point B., a Citibank facility in the U.S. Today, data flows occur in a multi-directional fashion throughout the globe, and involve more companies and entities in the processing activities.

## 2. Examples from the Case Studies

**Alpha Corporation.** This case study depicts a data flow in a clinical trial system that is ongoing, and multi-directional. As the Alpha report states, data transfers "are rarely uni-directional." The report adds, "The data flow cannot be considered a discrete event, but is rather a continuous process." A number of interconnected systems will interact together to produce different data sets that are tailored to the specific user. For example, a Clinical Data Management System (CDMS) might collect data from clinical sites and also check that data against external sources for cross-verification.

This process allows a high volume of records to be transferred. Since 2000, the Global Clinical Data Management (GCDM) team has implemented over 350 Electronic Data Capture (EDC) systems for clinical trials. At this pace, more than eighty new data bases are added each year. In 2008, the clinical trials created more than five million data points. This last statistic suggests that in 2008 more than seventy-two data points were created every minute.

**Beta Corporation.** The case study provides a useful example of dynamic international databases in action. The resulting processes involve Beta, its client, and, in some cases, other outside vendors, in executing different data management practices as dynamic needs arise. From a legal perspective, Beta used a combination of Safe Harbor (for data from Europe) and contracts to transfer data on an international basis.<sup>7</sup>

As an illustration of this process-oriented, dynamic and international solution, Beta Corporation provides a rich description of its services in action for a typical marketing promotion. It states:

[A] marketer in Spain would use the criteria developed by the analytics vendor in India to select a list of customers from the global Customer Relationship Management (CRM) system in the U.S. which would be transferred to their call center in Mexico for execution of a telemarketing campaign to consumers in Spain. Results from the telemarketing effort from Mexico would then be fed back to the U.S. to update the information in the global CRM system.

To maintain the global marketing system, frequent batch updates are used. Even daily updates of information are possible. Thus, the services provided by Beta Corporation are highly dynamic, and can respond quickly to client needs.

---

<sup>7</sup> For more on the Safe Harbor process, see U.S. Department of Commerce, U.S.-EU Safe Harbor, at <http://www.export.gov/safeharbor/>.

**Gamma Corporation.** This case study demonstrates a company's cautious and incremental use of a third party vendor in India. Of all the case studies, Gamma Corporation made the most limited use of the potential of global data flows. In the 1990's, Gamma Corporation moved from a local branch model in its banking operations to a centralized domestic model. As part of this process, it changed from handling mortgage renewals at local branch offices to using central computers to store key information about mortgages. In its subsequent waves of automation, Gamma introduced online banking to allow clients to access information on their own and to contact support teams via a secure messaging system.

Beginning in 2007, Gamma Corporation then began to use "a global third party vendor processing model." At first, Gamma Corporation moved only its "midnight-shift team" to India. It then continued "to move some additional mortgage renewal processing offshore to India." The company sought to identify processes that did not add value in the company's relationship with the client. It wished to focus on "high touch" services, such as providing advice to clients, or creating an "advice-driven platform" for client services. As part of the goal, it was also interested in finding ways to make it easier for the front line staff to service its customers. The operation of mortgage renewal processing is not considered to be a core competency of the Gamma Corporation. By shifting it offshore, the company sought to "free up" resources to improve overall service to its customers. At the same time, Gamma personnel continue to have all direct contact with the bank's clients. As Gamma notes, "No tasks that work directly with our clients have been moved offshore."

**Delta Corporation.** The Delta case study reveals a system of data flows, whether oriented towards consumers and businesses, that are international. These flows are generally from the consumer's location, wherever in the world the customer is located, towards the U.S. At the same time, data locations of the Delta Corporation may be distributed to an even greater extent throughout the world in the future. Already, its organization-oriented services are hosted on a regional level, which means these customer's data are crossing national lines.

**Epsilon Corporation.** The Epsilon report shows how the data generated through product registration supports multiple businesses processes. Following a consumer's registration of her PC with Epsilon, a support agent is able to access the registration data should the consumer contact Epsilon, whether via online chat or phone. Depending on the location of the customer and the time of the day, the customer will be automatically directed to a specific global support center. Epsilon has international support centers in India, Costa Rico, and Bucharest. The product-based registration data flow is multi-directional. It moves from the consumer's PC to various Epsilon and vendor databases. Support agents are located at different international locations, and Epsilon assigns tasks to different locations using an algorithm, which incorporates several factors.

Note as well that third party vendors, acting on behalf of Epsilon, may participate in this data flow scenario. Epsilon places the third parties under contractual agreements, which require the third party to uphold Epsilon policies and use any personal data only to perform the contracted work.

**Zeta Corporation.** The Zeta Report examines its Global Recruiting Process (GRP) system. This data system permits interested individuals to apply for an employment position, independent of the country in which they are located or the country from which the opportunity originates. It allows “a world-wide view into available jobs at Zeta Corporation” that leads to unique benefits for the individual and Zeta Corporation. The GRP system allows Zeta and its wholly-owned subsidiaries to assist in identification and selection of candidates, both internal and external, for employment opportunities. It also assists in the employment process by allowing HR recruiters, hiring managers and other participating parties to manage employment offers and acceptances. This system is used as well for managing Zeta's equal opportunity requirements.

A third party vendor located in Zurich, Switzerland hosts the GRP system application. The Zeta report notes, “Cross border data flows occur dynamically as part of this system.” As the report also states, the GRP system leads to “data transfers on demand.”

These data transfers cannot necessarily all be predicted in advance of a job posting. A job can be posted from South Africa to the GRP system server in Zurich, and then accessed by Zeta employees in over 100 countries. Some of these employees will send their personal data to the system. In addition, outside recruiters from these or other countries might send in data. In Appendix C to this study, I have included a longer illustration from the Zeta Report of how data within the GRP system can flow dynamically and in an international fashion.

Within Zeta, second level application support and HR recruitment support are provided to applicants and hiring managers from Zeta's India office. System and application technical support for the GRP system are provided from Zeta service centers in Hungary and South Africa. The GRP system may also supply data to other Zeta data systems, which are located in various countries, and which support the recruitment process. These information systems concern areas such as government reporting requirements, compensation, and the ordering of IT equipment.

## **B. A Change in Processing: Dynamic Data Transfers and Networked Series of Processes**

The second group of changes from the classic paradigm of data processing concerns the new ability of international data transfers to be made dynamically as well as the increased ability of processes to be networked. In the past, companies typically finalized data transfers in advance and databases were centralized. In that past model, an international data flow occurred at a predictable moment and into a database controlled by a single entity. The process of transmission was straightforward. Today, in contrast, data transmissions occur as part of a networked series of processes made to deliver a business result.

To trace these developments, I wish first to discuss a picture of the contemporary corporation and its capabilities that Samuel J. Palmisano, the President of IBM, made in 2006. Building on Palmisano's description, one can see the range of choices that organizations make regarding data processing is part of a broader transformation of the corporate structure. I will then briefly discuss a seminal essay by Ronald Coase, an economist who was awarded the Nobel Prize in 1991. Coase's essay, dating from 1937, discussed how a corporation would decide the fundamental "make-or-buy" question. Should it make something for itself, that is, bring production within its corporate walls, seek partners, or purchase it in the marketplace? For Coase, the answer to this issue turns on transaction costs.

Drawing on Palmisano and Coase, we can see that networked transactions now permit new flexibility in pulling apart and re-assembling data processing operations and activities. Cloud computing forms the latest manifestation of the growth in networked services. Contemporary corporations have adapted their management and operations to take advantage of the business opportunities that new technology provides.

## 1. From the Past to the Present: Palmisano on the Contemporary Corporation, Coase on "Make or Buy," and the Rise of the Cloud

In the Fiat-France and Deutsche Bahn examples, data transfers occurred as a predetermined international flow. In those cases, the flow was between branches of the same company (from Fiat-France to Fiat-Italy), or between one company to a separate partner entity (from the Deutsche Bahn to Citibank). In an approach shared in both instances, the data flow occurred through a fixed transfer system. The data went from one established database to another. It was if the information went through a rigid pipeline, or a courier service delivered it from one point to another. A sole entity was in charge of the data at either end, and the transmission itself was uninteresting from a process perspective as long as sufficient data security was provided. The goal of transmission was simply to have the information arrive at the other end without outside interference or unauthorized access.

Our first touchstone in marking the change from this recent past is an essay in FOREIGN AFFAIRS by Samuel Palmisano. In *The Globally Integrated Enterprise*, Palmisano discusses the results of liberalization of trade and investment flows as well as the revolution in IT that began in the 1970's.<sup>8</sup> For our purposes, it is important, in particular, that the IT revolution "standardized technologies and business operations all over the world, interlinking and facilitating work both within and among companies."<sup>9</sup> The resulting combination of shared technologies and common business standards, which were "all built on top of a global IT and communications infrastructure, changed the sorts of globalization that companies found possible."<sup>10</sup>

International data flows reflect these new possibilities. As Palmisano notes in general, firms are now "actively managing different operations, expertise, and capabilities so as to open the enterprise up in multiple ways."<sup>11</sup> This result reflects, in turn, how technology has provided new answers to the "make-or-buy" question. At this juncture, it is helpful to consider an insight of Ronald J. Coase in his essay, *The Nature of the Firm*.<sup>12</sup> In 1937, Coase sought to shed light on a fundamental question of corporate organization. The question concerned when a firm will produce something for itself, and when it will procure from another. In a conclusion as valid today as over seven decades ago, Coase's answer to the "make-or-buy" question turned on the

---

<sup>8</sup> Samuel J. Palmisano, *The Globally Integrated Enterprise*, *Foreign Affairs* 127 (May/June 2006).

<sup>9</sup> *Id.* at 129.

<sup>10</sup> *Id.*

<sup>11</sup> *Id.* at 131.

<sup>12</sup> Ronald J. Coase, *The Nature of the Firm*, in *The Nature of the Firm: Origins, Evolution, and Development* 18 (Oliver E. Williamson & Sidney G. Winter, eds., 1993)(essay originally published 1937).

results of any company's efforts to economize on a variety of transaction costs.<sup>13</sup> If it is cheaper, on the whole, to buy, a firm will turn to the market or to partners. Otherwise, it will produce the entity or service itself.

New technologies and accompanying new business models now allow firms to approach "make-or-buy" in innovative ways. Different functions and operations can be packaged as modular units that can be pulled apart and re-assembled. Today's technology for processing information permits flexibility for the firm that was previously unknown. The flexibility concerns decisions about how, when, and to what extent to structure relationships within its walls, and how, when, and to what extent to draw on outside parties and the market.<sup>14</sup> In particular, data flows can be de-aggregated and de-coupled to allow companies to develop novel business approaches to operations and activities.

Firms also have greater flexibility than ever before in deciding on the shape and form of the work itself, that is, how they will distribute processes and services. As an example, transfers of personal data occur increasingly on demand. Modern information systems respond to data requests rapidly and in many instances in real time. Data flows are also more international than before because of the global nature of data networks. After all, the first "W" in WWW stands for "world" — there is now a data web that spans the earth.

The latest manifestation of these developments in IT is the "cloud." Cloud computing is the location of computing resources on the Internet in a fashion that makes them highly dynamic and scalable. Users no longer need to own technology, whether software or hardware, that is placed in the cloud. Rather, different parties in the cloud can contribute inputs, outputs, analytics, and execute other kinds of actions. The result of this distributed computing environment is to permit dramatic flexibility in processing decisions -- and on a global basis. For example, computing activities can be shifted from country-to-country depending on load capacity, time of day, and a variety of other concerns. The cloud has also touched more and more people. According to the Pew Internet & American Life Project, for example, already some

---

<sup>13</sup> Id. at 20-25.

<sup>14</sup> Interestingly enough, Coase thought that technology, or at least the technology of his day, would largely function to cause firms to grow and also to bring more activities within their walls. Here is a critical distinction with the role of technology in the 21<sup>st</sup> century. Coase wrote: "Changes like the telephone and the telegraph, which tend to reduce the cost of organizing spatially will tend to increase the size of the firm. All changes which improve managerial technique will tend to increase the size of the firm." Id. at 25. In addition to this point about firm growth, Coase also saw technology as bringing within a firm many transactions previously carried out externally for the firm by a number of organizations ("combination"), and also as organizing transactions previous carried out by the market and within a single firm ("integration").

69% of Americans "use webmail services, store data online, or use software programs such as word processing applications whose functionality is located on the web."<sup>15</sup>

---

<sup>15</sup> Pew/Internet, Pew Internet & American Life Project, Use of Cloud Computing Applications and Services (Sept. 2008).

## 2. Examples from the Case Studies

As an initial point, two companies have self-descriptions that reflect the new openness and flexibility of corporations regarding choices about integration of business processes. Thus, Epsilon Corporation describes itself as a provider of technology solutions and services for a range of customers, including consumers, the public sector, and businesses. As for Zeta Corporation, it views itself as a globally integrated enterprise that helps public and private sector organizations through the use of business insight and advanced technology solutions.

**Alpha Corporation.** The Alpha report demonstrates a system that permits a high volume of ongoing, multi-directional data flows that respond to system-based needs rather than geographical location. In other words, the flows follow system requirements concerning technology, operations, resources, and administration. As an example, the Alpha report states, “As data servers are located around the world, how data is transferred depends on the geographical region from which the data originates. For example, some Canadian systems might back up to a European-based server, even though the systems are geographically much closer to a United States server.” The physical proximity shared by different company sites in North America becomes less important, and data transfer choices can be made by system engineers to optimize various company processes.

Every Electronic Data Capture application at Alpha is developed to meet specific needs of an individual clinical trial. Nonetheless, the components of a Electronic Data Capture process are generally the same. The applications are generally web-based and can be used in a client-server network.

As an example of a data flow, a clinical trial site in Country A, which has in place a comprehensive data protection law, puts de-identified data regarding clinical trial subjects on its Electronic Data Capture (EDC) client. The information in Country A is then sent to a Clinical Data Management System (CDMS) server in Country B, which also has in place a comprehensive data protection law. A clinical research team in the United States would have only read-- and not write-- access to this information from the CDMS server. The clinical research team would also be able, however, to send manual queries to the clinical trial site.

This process allows a high volume of records to be transferred. Since 2000, the Global Clinical Data Management (GCDM) team has implemented over 350 EDC systems for clinical trials. At this pace, more than eighty new data bases are added each year. In 2008, the clinical trials created more than five million data points. This last statistic suggests that in 2008 more than seventy-two data points were created every minute.

**Beta Corporation.** As already noted above, Beta Corporation developed an information system that is process-oriented, and not simply focused around any

discrete transfer. Rather than concentrating on a database or databases, it developed a networked series of processes to deliver a business result. Here is a further example of this chain of serial processes in action; it involves pan-European email campaigns with information from both Beta and the client. Beta captured email addresses through a consumer survey in which the consumer gave permission for use by a third party for marketing purposes. Information that lacked appropriate permissions was purged. The email address from Beta was combined with other data the client had about previous transactions with consumers. Drawing on segmentation criteria developed by an analytics vendor in India, the client was able to conduct international email marketing campaigns using the Customer Relationship Management (CRM) system.

The information was maintained and campaigns were distributed from the U.S., where email messages were prepared in the local language for each European country. For example, a marketer in an E.U. country, such as the United Kingdom, would draw on the segmentation criteria developed by the analytics vendor in India to identify a list of U.K. consumers to receive a specific email promotion. At the request of the client, the global CRM system housed in the U.S. would then send out an email message to the customers in the U.K. Simultaneously a different campaign for customers in France or Germany could also be taking place driven by the marketing offices of the client in the respective country.

Finally, the client used support personnel from vendors in addition to its own staff. Such support included the client's analytics vendor in India, their external backup facility in the U.S., and various outsourced call centers in places like the U.S., Mexico, Belgium, and India. As the Beta Corporation states, the CRM solution involved data from "hundreds of sources contributing information from dozens of countries."

Beta devoted considerable attention to the mapping of all data flows. It explains:

We start by identifying all data sources, whether directly from the individual or from a third party. Then all data is charted as it flows through all the various processes. This includes data cleansing, data integration, analytics, and the maintenance process for the marketing database. Then all uses and users of the database are identified and permissions are validated. This is a very comprehensive process.

One complexity for the project is that client data about sale transactions may be collected on a client's website in country A, but the transaction may be initiated by customers from countries A, B, C, or D. The data will all be sent to the U.S. to be maintained in the CRM solution. The client in countries A, B, C, and D will have access to the data for analytics and planning marketing campaigns. All these data flows are mapped in advance with the Beta Corporation putting appropriate controls for privacy and security in place.

**Gamma Corporation.** This case study involves a multipoint system as data flows to the vendor in India throughout locations in North America. In contrast to the other case studies, the resulting system does not network the processes themselves.

**Delta Corporation.** On the consumer-side, the three consumer-oriented services of Delta Corporation permit electronic mail, real-time messaging, and online-file storage. In these services, data flows can take place at two different periods. A data flow can occur at the time of data creation when data moves between the consumer and the data center. It can also occur at the time of information retrieval. At that moment, data flows take place between the data center and the message recipient's server (in the case of e-mail), the message recipient's client (in the case of real-time messaging), or the client's computer (in the case of data storage).

At present, Delta generally hosts the consumer-side data in the U.S. This approach means that the consumer information of international customers is necessarily an international transfer as it flows to the U.S. At present, moreover, information is kept within a single location, and load balancing takes place within the same data center. An international hosting of data would permit load balancing to take advantage of different time zones throughout the world. This technique would allow balancing of data loads since data flows tend to exhibit peaks in demand at predictable times in each geographical location. The Delta Corporation report states, "Moving forward, Delta may distribute user data location in order to improve the performance of its services or meet other objectives, including compliance."

On the organization-side, Delta Corporation's case study concerns an Internet-based integrated offering that allows customer access to an online suite of software. North America, Europe, and Asia are the chief markets for this service, and customer data are primarily hosted in the region in which customers register their billing address. For business continuity reasons, these services may already have back-up centers at different locations within a single country. Such system design seeks to secure data in cases of power outages or natural disasters.

**Epsilon Corporation.** The product-based registration in this case study is highly dynamic and involves a networked series of processes. As discussed in the preceding section, Epsilon draws on the product registration information when a registered customer contacts it for support. The goal is to serve customers as quickly as possible. Support agents are located at different international locations, and Epsilon assigns tasks to different locations using an algorithm, which incorporates several factors. The result is that the data flow relating to customer service calls is extremely dynamic and cannot necessarily be predicted in advance.

Some more details about the data flow relating to customer service calls will illustrate these points about the dynamic nature of this process. Part of the model for distributing customer service calls, as reflected in the algorithm, relies on a "follow-

the-sun" approach, which means that Epsilon considers the time of the day in different service locations when a customer calls for support. This element of the approach means a customer requesting support in the middle of the night in one country might be more likely to be assigned to a service center in a country where it is still daytime. There are other elements built-in as well to the Epsilon algorithm for distributing service calls. These include resource loads, the type of call, the load of agents in a certain location, and whether all agents there are busy.

**Zeta Corporation.** Any Zeta manager or authorized HR recruitment personnel may create a job posting on the Global Recruitment Process (GRP) system. Basic contact information is collected from the requisition creator, such as name, title, and business contact data. This information is not, however, displayed to applicants. Any interested party may gain access to the requisition from Zeta Corporation's external website.

Personal information about applicants from all over the world is collected over the Internet in different ways. Applicants can submit personal information in support of their job applications. Recruitment agencies can submit personal information about potential candidates. Zeta employees may refer potential candidates for an opportunity. Each of these parties may be in different countries. For an illustration of the global nature of this system, please refer to Appendix C's discussion of a data flow from it.

If the applicant is already a Zeta employee, in addition to the personal information that she provides directly at the time of the application, certain other personal data already in Zeta's possession and housed in other databases located in various countries may also be sent to the GRP system. For certain data sets which are automatically extracted from other internal databases, the internal applicant is also given the opportunity to decide whether or not this information should be added to her application.

Only personal information which is necessary for a specific stage of the recruitment process will be sent into the GRP system, or otherwise collected. The necessity principle is defined in accordance with local legal recruitments and the internal policies of Zeta Corporation. Moreover, at the time of collection of information, Zeta provides a "click to accept" privacy statement. This statement indicates the manner in which the information is to be used, to whom it may be made available, and that the data may be stored or processed in various locations around the world in connection with the recruitment process. Candidates may at any time update, correct, or delete their personal information.

## C. A Change in Management: The Professionalization of Corporate Data Protection and the Shift to a Process-Oriented Approach

In the recent past, modern corporations largely avoided privacy and security issues and devoted a low level of resources to them. Moreover, to the extent that such issues arose, companies had an ad hoc, reactive approach to handling personal information. The third transformation in this area concerns the management of privacy and security. There has been a professionalization of corporate data protection, which, in turn, has been accompanied by a greater investment of business resources in this area. Finally, there has been a shift to a new process-oriented management approach. Companies now seek to develop forward-looking systems for managing data flows and training personnel.

To trace the path from the past to the present day, we can consider Jeffrey Smith's findings from 1994 in *Managing Privacy*.<sup>16</sup> In his study, Smith identified "a distinct lack of leadership with respect to privacy issues at both corporate and internal levels" throughout the 1980's and early 1990's.<sup>17</sup> This book offers a valuable benchmark for past levels of privacy management. As we will see, moreover, the change today could not be greater. Due to many factors, including regulatory requirements, companies now have chief privacy officers and chief information security officers, who take an active role in developing internal processes for managing data flows.

---

<sup>16</sup> H. Jeff Smith, *Managing Privacy* (1994).

<sup>17</sup> *Id.* at 4.

## 1. From the Past to the Present: the Smith Study and the Rise of the Chief Privacy Officer

In *Managing Privacy*, Smith found that few corporate executives sought to be privacy leaders in their industries, and that within many companies, no employee wanted to be responsible for privacy policies. He observed that executives who handled information systems did not see themselves as "the corporate leaders on information privacy issues."<sup>18</sup> Indeed, some went so far as to adopt "particularly subservient roles in most privacy discussions."<sup>19</sup> In another measure of the lack of priority of privacy management, one corporate officer estimated the overall level of investment in information privacy at his bank as "[a] lot smaller than has been made in company picnics, I can assure you."<sup>20</sup>

In summary then, Smith first identified a low level of investment in privacy, and a lack of specialization in management of this issue. I will now discuss the current professionalization of privacy management and the increase in spending in this area. Then I turn to his second group of findings, which concern the reactive nature of privacy management in the past.

Since the publication of Smith's study, many corporations have come to view information privacy as important and worthy of ongoing attention. These organizations have increased investment in this area, and also sought to assign the development and management of privacy policy to specific employees, who, in turn, increasingly self-identify into categories such as Chief Privacy Officers, or Chief Security Officers. There is even a professional organization for privacy executives, the International Association of Privacy Professionals, which has over 6,000 members across fifty countries. Today, the investment in privacy and security in corporations has also increased. In sum, there is both a greater specialization of those who manage privacy and security, and a greater investment in it.

These changes are likely due to at least five factors. First, there has been a growth in the value of data as a corporate asset. To return to the Smith quotation from the anonymous corporate official of the early 1990's, a corporation's information assets are now recognized as being far more valuable for it than any benefit from the company picnic. The Alpha case study provides an illustration of the high value of data as a company resource. Alpha is a global pharmaceutical company; in its report, it states, "Clinical trials are the keystone for the development of new treatments and a robust product pipeline." The data pertaining to trial subjects, which are de-identified, is considered company proprietary and strictly protected through company policies,

---

<sup>18</sup> Id.

<sup>19</sup> Id.

<sup>20</sup> Id. at 80.

training, and information security practices. Like the other companies of the case studies, Alpha considers its personal information to be a critical company asset. The high value assigned to the asset, in turn, provides an important reason for the companies to provide strong security protections and careful privacy management structures.

Second, reputation costs also are important to companies, especially established ones, and many organizations have come to recognize that their handling of information can have significant reputational effects, positive and negative. Data security lapses provide only one example of the negative potential that publicity can have on a company's reputation.

Third, there has been an increase in the amount of management work required in this area, which has encouraged specialization and, in turn, professionalization. Herbert Simon, the pioneering social scientist, once noted, "The real problem of administration . . . is not to 'specialize,' but to specialize in that particular manner, and along those particular lines, which will lead to administrative efficiency."<sup>21</sup> As the preceding sections have indicated, there have been changes in the scale of the processing of personal information and in the underlying kind of processing. Data transfers are now network-based, and business-oriented processes are part of the network. The consequence is that there is far more management work associated with personal information.

Fourth, some of this management work involves fulfilling legal obligations for the handling of personal information. A good example from the United States is the explosive growth of state laws that require data breach notification letters to be sent to affected parties in the case of data loss.<sup>22</sup> In some countries, in addition to laws that set requirements for privacy and security, and thereby create a need for specialized management, there are also national laws that require a company to have an internal data protection officer. Such requirements are found, for example, in Canada and Germany.<sup>23</sup> In the U.S., which is the focus of Smith's study, whether at the time of his work or today, there is no formal legal requirement of a data protection officer. Nonetheless, the tremendous growth over the last decade in the U.S. of privacy and security statutes have encouraged companies to appoint Chief Privacy Officers. These laws encourage specialization in search of efficiency in privacy and security management.

Fifth, a professionalization of privacy and security management has been encouraged by companies developing "off the rack" models of governance structures in this area. Paul DiMaggio and Walter Powell, two sociologists, have argued that

---

<sup>21</sup> Herbert Simon, *Administrative Behavior* 30 (4<sup>th</sup> ed. 1997).

<sup>22</sup> For a description of these laws in the U.S., see Paul M. Schwartz & Edward Janger, *Notification of Data Security Breaches*, 105 *Michigan Law Review* 913 (2007).

<sup>23</sup> The Personal Information Protection and Electronic Documents Act (PIPEDA)(2000), Schedule 1 (4.1); Bundesdatenschutzgesetz §§4f-4g (2009).

institutions will sometimes copy other organizations in response to uncertainty. Their key insight is as follows: "Organizations tend to model themselves against similar organizations in their field that they perceive to be more legitimate or successful."<sup>24</sup> Due to the International Association of Privacy Professionals, privacy conferences, consulting firms, law firms specializing in information privacy, and other sources, there are now easily accessible models that companies can draw on when building their own structure of privacy management.

Beyond the professionalization of those who work in this area and the increase in corporate investment in it, there is another set of distinctions that can be drawn with the era depicted in Smith's *Managing Privacy*. Smith found a tendency for corporations to have wandering and reactive approaches toward privacy issues. He described a cycle of (1) corporate drift, followed by (2) external threats and crisis, and, finally, (3) an explicit corporate reaction.<sup>25</sup> High level executives first ignored how information was handled in the company as well as other privacy issues. Sometimes privacy issues were simply handed off to a mid-level manager, who crafted practices based on "localized interpretations."<sup>26</sup> Such practices reflected ideas and processes in one department, but did not establish formally developed privacy policies that the company aimed to embody in routines reflected throughout its organization.

As the case studies in this Report show, however, considerable resources and personnel are now devoted from the moment of initial data collection to developing safe and secure processes. Rather than the drift that Smith describes, the companies in the case study seek to go beyond localized interpretations and develop and institute coordinated practices. These practices are then committed into routines and rules for the organization.

There are also notable public examples, independent of the case studies in this Report, of companies that have invested heavily in the development of techniques for the management of privacy. One leading example is the Security Development Lifecycle project of Microsoft's. It seeks to develop processes that allow companies to update their software development process in order to build more secure software.<sup>27</sup>

In addition to processes that may be customized for certain applications and services, companies today seek to create generally applicable policies for privacy and security. As this Report's case studies show, moreover, the resulting processes are highly collaborative. Their development and use can involve chief security officers,

---

<sup>24</sup> Paul J. DiMaggio & Walter W. Powell, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organization Fields, in *The New Institutionalism in Organization Analysis* 63, 70 (Walter W. Powell & Paul J. DiMaggio, eds. 1991). I am grateful to my colleague Ken Bamberger for drawing my attention to this article and related scholarship and for suggesting its applicability to the management of information privacy processes.

<sup>25</sup> H. Jeff Smith, *Managing Privacy* 83-85 (1994).

<sup>26</sup> *Id.* at 56.

<sup>27</sup> Michael Howard & Steve Lipner, *The Security Development Lifecycle* 3 (2006).

chief privacy officers as well as internal boards. The companies in the case studies are also heavily involved in training their employees and, in some circumstances, personnel at clients and vendors.

## 2. Examples from the Case Studies

All the companies in the case studies demonstrate a professionalization of information privacy management, and the development of a process-oriented approach to privacy and data security. Highlights of the approaches at different companies follow.

**Alpha Corporation.** Global IT at Alpha has developed a highly structured governance model with assignment of specific responsibilities to various players to maintain accountability throughout any decision-making process. In brief, governance is executed thorough different councils within the company that are aligned with a business-unit. As necessary, Alpha may divide individual councils into regional sub-councils or committees.

Thus, Alpha Corporation manages privacy and security in part through use of relevant privacy governance bodies. These are segmented out by the kinds of data in their purview, and focus on clinical research and pharmacovigilance, commercial data, and employee data. It has established a distributed, tiered privacy infrastructure with focal points throughout the organization. The Alpha report states, "The purpose is to link business goals with privacy objectives, globally, regionally, and locally."

There are three privacy governance councils at Alpha in the U.S. that strategically address privacy concerns that are relevant to those respective groups. Each council is chaired by a senior executive from the applicable business unit. Periodic meetings are attended by certain leaders of that business unit and respective support functions, such as the legal department, IT, and the compliance unit. The Global Privacy Office plays a key role, including establishing these councils' charters and helping to set the agendas and direction for their periodic strategic meetings. The councils can also aid in "day-to-day issues, such as selection of team members for Safe Harbor Certification due diligence."

Alpha is also engaged in extensive training of its personnel. The Global Privacy Office has developed a privacy training curriculum -- a set of five online training modules that assists in raising awareness of Alpha personnel on the importance of data privacy. The basic general privacy awareness course is directed to new hires and is a pre-requisite for three additional modules that are directed towards specific business areas and tailored to specific business processes based on the types of personal data they process. The fifth course focuses on practical guidance in areas of high risk, including the secured transfer and storage of data. As the Alpha report states, "To date over 19,000 U.S.-based colleagues have taken the basic privacy course." The training takes place through compliance courses maintained in several languages on the corporate intranet.

**Beta Corporation.** There is a corporate privacy team at Beta. It is headed by a Global Privacy Office in the U.S. with three regional privacy officers across the

globe as well as in-country privacy officers. The Beta Corporation's privacy officers report to a chief privacy officer, who is located under and reports to the General Counsel of the company. The role of the privacy team at Beta is to set policy related to information collection and use, oversee all compliance obligations and best practices, and train the different lines of business on the required policies. The membership of the privacy team has been very stable with employees who have been on the job on average for over seven years.

Beta's training of its privacy staff includes the use of primarily in-house training augmented with some external training and International Association of Privacy Professional certification where available. Beta also offers some of its in-house training to clients.

A particular concern for Beta is in identifying the provenance of personal data. As the Beta Corporation stated, "With hundreds of sources contributing information from dozens of countries, it was necessary to map each source and flow to assure all the proper notices and permissions were granted. For any global system, it is critical that there be a means of maintaining all origination and transfer intelligence accurately over time." This task of tracking data provenance becomes essential due to an organizational shift towards process-oriented administration of information. As a specific example from the Beta case study, purchases made by a customer in Australia might have been made on a Malaysian website and transferred to the U.S. for fulfillment of the order. Information about the origins of the consumer data must be collected, if possible, from the start and then follow the information.

Throughout the project, data security was a major consideration. Beta Corporation uses secure data processing centers; regular audits of these centers are carried out by Beta and its clients. Ongoing upgrades are made to system security with a central role played by Beta Corporation's Chief Security Officer and his team. Sensitive data are required to be transmitted in an encrypted manner. Finally, most of the information was transmitted between Beta Corporation and the client over a private leased network and not the Internet.

The shift to the cloud and an information system that is a chain of serial process requires careful attention to access controls and authentication. Beta Corporation controls access by each employee to each of its business systems and client solutions. Only employees working on the account and overall system administrative personnel are permitted access to client data. Beta uses userid/password authentication for employees working from workstations in its office. It uses two-factor authentication for access from external sources, including userid/password plus a randomly generated password from a token. All Beta Corporation passwords are changed every forty-five days.

**Gamma Corporation.** The Gamma Corporation has created a team to monitor the off-shore vendor for its performance and other issues. This team

performs a quarterly review of the access to data in place for people at the vendor to ensure that access is appropriate and will end once no longer appropriate. Their team is located within North America and consists of Gamma employees. The head of the off-shore initiative at Gamma Corporation is accountable for ensuring that complete documentation is in place and that all reviews are carried out. Moreover, all aspects of the outsourced program are subject to ongoing compliance monitoring and independent testing by the Gamma Corporation's internal auditors.

More generally, the Gamma Corporation has management structures and safeguards in place regarding privacy and security compliance that do not apply solely to the program described in the case study, but are part of its overall privacy and security compliance program and are applicable throughout Gamma Corporation. Gamma Corporation has established a "Global Privacy and Information Risk Management Framework." Compliance with this framework rests with the "Executive Head of each platform." The Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) provide "oversight, guidance and support."

Training in privacy and information risk management is required for all new employees at Gamma. This training must be completed within thirty days of joining the company. In addition, different kinds of training are required based on the unit where a specific employee works and based on different responsibilities of the employee. Gamma Corporation has also developed numerous "job aids," including quick reference guides and FAQ's. In addition, every two years, all employees must successfully complete a test based on Gamma Corporation's Code of Conduct. A significant portion of this test is dedicated to privacy and information security requirements.

Gamma carefully considered the kinds of access controls that were necessary for employees and vendors in this case. As an example of the result of this analysis, it requires the off-shore outsourcing company to use only the Gamma Corporation email system for Gamma business. It does not permit remote access to the Gamma network for employees of the off-shore outsource company. All email communication between Gamma and the offshore location is done via the Gamma email network. In consequence, all communication between Gamma and the offshore vendor takes place either through a dedicated private line or through an encrypted tunnel.

**Delta Corporation.** Two groups at Delta Corporation are responsible for attention to policies and standards for the Delta online infrastructure that the case study depicts. These are the Infrastructure Services and Compliance Group and the individual online service groups.

The responsibilities of the Infrastructure Services and Compliance Group include protecting Delta's data centers and making the physical and logical infrastructure for online services secure and reliable. Individual service groups are

responsible for application-level privacy, continuity, and security processes. These groups also adhere to processes defined by the Online Services and Compliance Group and services-specific criteria that are defined at the divisional level.

Training is an important component of Delta's strategy for privacy and information security. The company requires designers, developers and operations personnel to update their skills on an ongoing basis. Key elements of Delta's training approach vary for: (1) teams that develop and manage software components for services, and (2) members of the online service operations team. Both groups must take a clearly defined number of course-hours each year.

Delta Corporation manages data with reference to the company's privacy principles. These include: accountability in handling personal information, notice to individuals about data use, quality assurance steps to ensure that personal information is accurate and relevant, access for individuals who wish to inquire about and, when appropriate, review and update their personal information. Other principles are: enhanced security for personal information, and compliance with Delta privacy policies.

Online service teams are required to pass a security and privacy review for any new service or service updates that bring significant changes in application code or logic. These include meeting a formal security review with defined steps that culminate in a final review. As for the privacy review, it starts with a self-assessment and then progresses through a series of formal milestones. During this process, the online application team and privacy security group draw on resources of the legal department to identify the laws, regulations, and Delta policies that apply to this service.

Delta online services are also subject to an additional process that is carried out by a Delta online risk management team. This group leads each online service team through assessments of privacy, security, compliance with regulation, and other factors. The assessments are focused on specific frameworks and culminate in final reviews of a series of listed categories.

As a central principle in managing data, Delta implements the use of "a need-to-know and least-privilege basis" for Delta full-time employees. It has also centralized access management, which is made through a centralized electronic form. This form is stored and is subject to routine audits. The audits are made at the individual account level and also in terms of checking on requests and responses.

Authorization to information is carried out through a two-tier process. First, one needs an authorized account at Delta. Second, one needs to have access to an individual resource. The Delta owner of that resource evaluates an employee's specific role in deciding which kind of access is appropriate to the account. There are also rules regarding the creation of strong passwords, including rules for minimum

password length. Logging on to the Delta network requires a login account, passwords, and a smartcard with a digital certificate.

**Epsilon Corporation.** At the Epsilon Corporation, the CPO is responsible for global privacy strategy, policy, governance, and operations. The CPO reports into the Ethics & Compliance Office. The Epsilon CPO works for the Chief Ethics and Compliance Officer, who in turn works for the Chief Executive Officer. Epsilon's privacy policies are based on the company's standards of business conduct.

The CPO leads a Privacy and Data Protection Board, which is made up of senior executives from all key businesses, regions, and functions. The Board's charter emphasizes a number of tasks. These begin with the identification, management and mitigation of compliance and reputation risks. The Charter also requires the Board to develop privacy and data protection policies, practices, procedures, and training. Among its other tasks are to provide a process for issue escalation and resolution, and to monitor and audit compliance at Epsilon with laws, policies, plans and "the highest ethical standards."

Epsilon's Privacy Office and legal department have established a process that uses the company's Privacy and Data Protection Board "to assess, rate and prioritize risks and opportunities." It does so through a five step process that involves: (1) trend analysis, (2) input from board members, (3) reasons for proposed decision and in-depth discussion with the board, (4) prioritization related to risks and impact, and (5) formalization of plans and tracking.

Epsilon uses multiple mechanisms for training its employees and partners. In addition to its standard privacy training for all employees, it requires additional training for all employees granted access to systems that contain sensitive personal information. Epsilon has accomplished training of more than 99% of its current workforce in "specific mandatory privacy training."

Regarding vendors, Epsilon requires that the vendor demonstrate the ability to uphold requirements for personal information and sensitive information. The vendor is required to have privacy training, and in some cases Epsilon will supply specific training material or specify the content that it wishes in the vendor's training program.

Epsilon Corporation maintains comprehensive information security standards and policies. It uses appropriate physical, technical, and administrative procedures to safeguard the information that it collects and transfers. Working in close partnership with the CPO, the Chief Information Security Officer is responsible for data security. As noted above, vendors and other service providers are bound by contract to uphold Epsilon policies. All policies, standards, and guidance are documented and available to Epsilon employees.

Epsilon uses a variety of security technologies to help protect personal information from unauthorized access, use, or disclosure. The personal information provided to Epsilon is stored on computer systems located in controlled systems to which access is limited. When Epsilon transmits confidential information, such as credit card numbers or passwords over the Internet, it is protected through the use of encryption, such as SSL. Credit card numbers are used only for processing payments and not for any other purposes. As part of its real-time payment processing, Epsilon subscribes to a fraud management service.

Access controls at Epsilon Corporation vary based on sensitivity of the information in a system. Every sensitive database has an assigned access manager. Access to a database relies on the Epsilon digital badge process, which is multi-layered and includes a token to be inserted into a PC before a database with personal information may be accessed. For access to certain databases, moreover, an Epsilon employee must be onsite even with the highest level digital badge. Epsilon Corporation also enforces specific length and structure requirements for passwords.

**Zeta Corporation.** The GRP business process owner, working with the Human Resources function and support groups such as Legal and Business Controls, is responsible for ensuring that the process is in compliance with internal and legal privacy requirements. This responsibility extends to cross border data flows that may occur as part of the GRP process.

Recruitment agencies and any employees referring a candidate have additional, special requirements. They must confirm that they have obtained the consent of the individual whose personal information they are submitting for the purpose of applying for employment. In addition, they must confirm that notice of international transfers for processing has been provided to the candidate.

More generally, Zeta Corporation's Data Security and Privacy Steering Committee oversees its policies, procedures, and programs relating to data management and data protection. The committee is made up of cross-company senior executives, and co-chaired by two senior leaders. These are Zeta's CPO and the Assistant General Counsel of its IT Delivery group. Both leaders are Vice Presidents at Zeta.

Zeta's CPO also has direct global responsibility for its leadership and compliance in the area of personal data policies and practices. He leads a cross-unit, cross-function and cross-geography privacy organization that includes the participation of leaders and subject matter experts from departments, such as law, compliance, CIO/IT, corporate security, HR, Global Services, and Zeta Research.

Zeta has security leadership teams for IT and physical security. These teams are responsible for Zeta's own enterprise data security standards and practices.

Where suppliers may be granted access to personal information, Zeta makes use of contractual clauses to ensure privacy and security requirements are met. It also assesses suppliers for their ability to meet such requirements before any contract is awarded. Finally, it monitors supplier compliance with requirements for privacy and security.

A central part of the Zeta Corporation strategy for privacy and security is workforce education and awareness. Zeta employees are regularly required to review, and certify their review, of the company's code of conduct. In addition, Zeta makes general and job-specific training in privacy and security available to all of its employees and contractors world-wide. Depending on their job responsibilities, Zeta's employees and contractors are either required or encouraged to engage in privacy and security education. In the specific case of the GRP system, HR recruiters and managers are required to take privacy education before Zeta permits them with access to the system.

Beyond the GRP system, Zeta Corporation has implemented a global data privacy policy. As the Zeta report states, this policy "sets, at a high level, the basic handling requirements that apply to personal information." The privacy policy is supplemented by a number of corporate instructions, guidelines, and standards.

A central element of Zeta's approach to privacy accountability is its program for privacy assessment. This online program uses an automated "smart" self-assessment tool to allow the business process owners to self-assess the degree of risk that their process or IT application poses. Zeta also has a set of complimentary IT security policies.

Zeta Corporation has deployed several technical measures to enable data security. For example, it uses an automatic scanning tool to ensure that all workstations are compliant with security standards. It also requires that sensitive information be encrypted while in transit and while at rest in corporate databases. In addition, portable media containing such information must be encrypted and sent only through approved carriers. Finally, Zeta has implemented a global data incident response process. This process allows prompt identification of potential incidents and their management.

The company also has stringent mechanisms for access control to ensure that only authorized individuals can access data. Access controls for employees and vendors is based on their need to know. A manager must make a requisition request for access for it to be granted. Thus, there must be a match between a function and a need to gain access to the GRP system to be able to log into it. Moreover, there are requirements for length and structure requirements for all passwords. These expire after ninety days.

## **D. New Paths to High Levels of Data Protection?: The Call for Accountability and the Rise of Process-Oriented Corporate Safeguards**

The case studies in this Report depict a transformation of international data transfers in the corporate setting. Global data flows take place in a continuous, multipoint fashion. Moreover, these transfers are made through global networks that can dynamically incorporate different kinds of processes into each transfer. Finally, there has been a professionalization of the management of data privacy and security. This specialization has been accompanied by a greater investment of business resources in this area and a shift to a process-oriented approach.

In the final section of this Report's analytical section, I wish to make one last point by drawing a connection between the case studies and a current policy discussion in data protection law that seeks to use organizational accountability as a touchstone. To develop a context for this final point, I wish first to discuss how changes have been a constant in data protection law as lawmakers, regulators, and scholars propose and make necessary alterations in their approaches as new threats to privacy arise. I then discuss some of the reform proposals that stress accountability and link these ideas to the case studies of this Report.

We begin then by considering two perspectives, one from the United States in 1890 and one from Europe in 2006. In 1890, Samuel Warren and Louis Brandeis argued that the law needed to recognize an invasion of privacy as a legal injury.<sup>28</sup> Their concern was with gossip by the invasive press of their day, and with the development of cameras that allowed candid photography of individuals without their consent. Warren and Brandeis called for further development of the law and establishment of a general right of privacy.

Such a right was eventually established in the United States, and elsewhere. Yet, change has been a constant in the field of information privacy. Beginning in the 1970's, privacy law responded to a new threat, which was that of the computer and its capacity for processing personal information. The rise of PC's and then of the Internet have raised new privacy issues.

In 2006, in the introductory chapter to sixth edition of his magisterial treatise on the Federal Data Protection Law of Germany, Spiros Simitis pointed to recitals in the Data Protection Directive that required member states to continue their development of data protection law at a high level. He wrote, "Data protection regulations, whether in national or in supranational sectors, are never static or even completed regulations. They react to information and communications technologies

---

<sup>28</sup> Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 *Harvard Law Review* 193 (1890).

that are developing ever more quickly.”<sup>29</sup> Simitis called for data protection laws and regulations to draw, in a “continuous and resolute fashion,” on knowledge that is gained through experience.<sup>30</sup> Privacy regulators and lawmakers, in Germany, Europe, and the United States, can heed no better advice.

It can be difficult, however, to decide upon the lessons of experience in the area of information privacy. Fortunately, there is no shortage of possible teachers and suggestions in this regard. Some of the most interesting recent voices in discussions about data protection law offer perspectives regarding the need for “modernization” of data protection law as well as for “accountability” as a central principle regarding international data transfers.

In 2001, the Federal Minister of the Interior in Germany published an independent expert opinion, *Modernization of Data Protection Law*, by Alexander Roßnagel, Andreas Pfitzmann, and Hansjürgen Garstka.<sup>31</sup> Among their many valuable points, the authors argue that it was now obsolete to consider the exchange or transfer of personal data as a somehow exceptional circumstance.<sup>32</sup> They view that past approach as resting in the 1970's roots of data protection law and a paradigm of central governmental data banks built around mainframe computers.

Roßnagel and his co-authors also call for new conceptual approaches to data protection law because personal information is now processed in international data networks by many participants, and frequently without any possibilities for centralized governmental control. They observe, “In the Internet, there is no control at the border.”<sup>33</sup> Data processing, moreover, is no longer taking place in a computer center but on the network itself. The expert opinion identified a series of core tasks as part of a modernization of data protection law, including considering a use of self-regulation by industry when the law itself establishes a legal and regulatory framework for this behavior. They refer to this approach as “regulated self-regulation.”<sup>34</sup>

Our next example comes from North America. In Canada, the Office of the Privacy Commissioner has developed an international guideline, *Processing Personal Data Across Borders*.<sup>35</sup> This document explains how the Canadian data privacy statute, the Personal Information Protection and Electronic Documents Act (PIPEDA), applies to international data transfers. In the document, the Canadian privacy commissioner

---

<sup>29</sup> Spiros Simitis, Einleitung, in Bundesdatenschutzgesetz 147 (Spiros Simitis, ed., 6<sup>th</sup> ed 2006).

<sup>30</sup> Id.

<sup>31</sup> Alexander Roßnagel, Andreas Pfitzmann, and Hansjürgen Garstka, *Modernisierung des Datenschutzrechts* (2001).

<sup>32</sup> Id. at 22.

<sup>33</sup> Id. at 26.

<sup>34</sup> Id. at 158-59.

<sup>35</sup> Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (Jan. 2009), at

[http://www.priv.gc.ca/information/guide/2009/gl\\_dab\\_090127\\_e.cfm](http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm)

stresses "an organization-to-organization approach." As Principle 1 of PIPEDA states, "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing."

More recently, there has been renewed interest in accountability principles. For example, a review of the E.U. Data Protection Directive by RAND Europe, as commissioned by the U.K. Information Commissioner's Office, called for a re-casting of the Directive. The RAND study wished to see clearer descriptions of high level outcomes and implementation of "effective enforcement measures to ensure accountability."<sup>36</sup> There are also two ongoing efforts of interest. First, the Galway project seeks to develop "commonly-accepted accountability principles." This effort is led by a group of international experts, facilitated by the Irish Data Protection Commissioner, and assisted by the Hunton & Williams Centre for Information Policy Leadership, which serves as secretariat to the project. Second, the Swiss and Spanish Data Protection Commissioners are leading a project to develop new international privacy standards. Final details of these two proposals are not yet public as this Report is being completed.

Nonetheless, there is an important connection to be made between the new interest in accountability and a corporate privacy culture focused on a process-oriented approach. The case studies in this report focus on safeguards being built-in to data processing management. Companies are now putting internal policies in place, centered on forward-looking rules of information management and training of personnel. Such policies are, at the least, a necessary precondition for an effective accountability regime that develops a high level of privacy protection.

The key to the merits of an accountability regime will be in the details of any regulation. Nonetheless, it is possible to say that leading corporations have developed the kind of preconditions for a data protection regime whose safeguards and requirements concentrate on institutional privacy outputs rather than managerial inputs. As an example, detailed registration requirements for data processing are unlikely to raise the level and quality of data protection. Rather, regulators might consider an approach that requires companies to develop effective privacy programs and policies and then monitors whether these requirements are followed.

A critical question for the corporation is that of trust. As Palmisano stresses, "A company's standards of governance, transparency, privacy, security, and quality need to be maintained even when its products and operations are handled by a dozen organizations in as many countries."<sup>37</sup> A critical question for regulators, lawmakers, policymakers, and scholars is how to maintain information privacy law at a high level

---

<sup>36</sup> Neil Robinson et al., Review of E.U. Data Protection Directive: Summary, RAND Europe 10 (May 2009).

<sup>37</sup> Palmisano, *The Globally Integrated Enterprise*, 85 *Foreign Affairs* 127, 134 (May/June 2006).

that responds in a meaningful fashion to the challenges and opportunities of global networked data flows.

## Appendix A: Methodology

A number of criteria led to selection of the six companies in this Report as subjects of the case studies. First, all companies in the Report are global companies known for a commitment to developing strong policies, practices, and technologies for information privacy and security. Second, these businesses represent different commercial sectors and are interested in different types of personal data. Third, the firms face varying levels of legal regulation in their underlying enterprise activities. For example, some, but not all, of the companies are engaged in heavily regulated areas, such as providing financial services, or developing pharmaceutical products. Finally, and as noted above, the focus is on leading companies, that is, entities with discrete management resources dedicated to data flows and, moreover, enough knowledge of and documentation regarding these activities to permit development of the case studies.

The basic methodology for eliciting information was structured self-reporting. An initial framework of questions was submitted to the participating companies, and a chief respondent at the organization submitted answers on behalf of the company. All companies were promised that the resulting case studies would not use their real names. The initial responses led to tailored follow-up questions and an additional general framework of questions regarding access and authorization controls. The further set of questions followed because some written responses demonstrated that the issue of access and authorization had become a high profile corporate concern. Follow-up telephone interviews then took place with all companies.

Drawing on this body of material, I then prepared the individual company studies in anonymous form. Each company was randomly assigned a name based on the Greek alphabet, and each anonymized study was shared with the respective individual company. I requested feedback in particular about any possible inaccuracies in the case study and any details that might lead to de-anonymization of the companies.

## Appendix B: Case Studies

### 1. Alpha Corporation

#### Company Profile and an Overview of the Case Study.

The Alpha Corporation is a global health care company. Its report focused on its use of information in clinical trials. Such information as it pertains to clinical research subjects is de-identified. The de-identification of personal data helps to protect the privacy of clinical trial subjects, and also helps to preserve the integrity of the clinical research process. Alpha Corporation has incorporated international standards for clinical research standards as well as privacy and security requirements into its Global Clinical Harmonized Standard Operating Procedures. The Alpha case study demonstrates a system that permits a high volume of ongoing, multi-directional data flows that respond to system-based needs rather than geographical location.

#### Case Study: Clinical Trials.

The underlying information at stake in this case study is essential to the Alpha Corporation and also is highly sensitive. Alpha treats the data in line with firmly established international standards for conducting clinical research studies. As the report states, "Clinical trials are the keystone for the development of new treatments and a robust product pipeline. The large amount of data that is generated by such trials is in many ways the most sensitive data processed on behalf of the company." The data pertaining to trial subjects are de-identified, and the underlying information as a whole is considered company proprietary and confidential. It is strictly protected through company policies, training, and information security practices. Alpha Corporation has developed "strong levels of protection in order to maintain the trust of all of its stakeholders."

Alpha Corporation has shifted to all digital records for its clinical trials. Its Global Clinical Data Management (GCDM) team, keepers of the clinical trial data bases, and Global IT share the responsibility of ensuring security of clinical trial information. GCDM has the task of designing the data collection tools. Data has to be "cleaned, reconciled and then locked in a finalized database" so that quality is built into the process throughout, and not merely verified at the end.

The data flow in a clinical trial system is ongoing, and multi-directional. As the Alpha report states, data transfers "are rarely uni-directional." The report adds, "The data flow cannot be considered a discrete event, but is rather a continuous process." A number of interconnected systems will interact together to produce different data sets that are tailored to the specific user. For example, a Clinical Data Management

System (CDMS) might collect data from clinical sites and also check that data against external sources for cross-verification.

The Alpha report demonstrates a system that permits a high volume of ongoing, multi-directional data flows that respond to system-based needs rather than geographical location. In other words, the flows follow system requirements concerning technology, operations, resources, and administration. As an example, the Alpha report states, “As data servers are located around the world, how data is transferred depends on the geographical region from which the data originates. For example, some Canadian systems might back up to a European-based server, even though the systems are geographically much closer to a United States server.” The physical proximity shared by different company sites in North America becomes less important, and data transfer choices can be made by system engineers to optimize various company processes.

### **The Data Processing System.**

Every Electronic Data Capture (EDC) application at Alpha is developed to meet specific needs of an individual clinical trial. Nonetheless, the components of an EDC process are generally the same. The applications are generally web-based and can be used in a client-server network.

As an example of a data flow, a clinical trial site in Country A, which has in place a comprehensive data protection law, puts de-identified data regarding clinical trial subjects on its EDC client. The information in Country A is then sent to a CDMS server in Country B, which also has in place a comprehensive data protection law. A clinical research team in the United States would have only read-- and not write-- access to this information from the CDMS server. The clinical research team would also be able, however, to send manual queries to the clinical trial site.

Alpha Corporation strictly regulates each user's security settings and access to the data. One reason for such care is the need to ensure that the clinical data retains its integrity throughout the lifecycle process. As an example, a nurse at a clinical trial site might have access to the EDC application for the purposes of initially entering de-identified trial subject data, amending such data and viewing such data, for their trial site, but would not have that same ability in the CDMS system. Conversely, the Alpha Corporation researcher preparing the clinical analysis report would only be able to view the de-identified trial subject data from the CDMS, but would not have access to such data in the EDC application.

This process allows a high volume of records to be transferred. Since 2000, GCDM has implemented over 350 EDC systems for clinical trials. At this pace, more than eighty new data bases are added each year. In 2008, the clinical trials created

more than five million data points. This last statistic suggests that in 2008 more than seventy-two data points were created every minute.

The Alpha report also discusses how it integrates local privacy laws into its process for collecting data. Its corporate policies and procedures are tailored so that compliance with company rules will result in compliance with any applicable law or regulation. Moreover, if the general corporate privacy policy is more restrictive than the local law, or if there is no local law, the stricter corporate rule will control. Conversely, if the local law is stricter, the local law will control.

### **Management of Personnel.**

The CIO at Alpha considers IT at the company not as a “cost center, but a “value provider.” The goal is to make IT a "strategic partner" as it interacts with "people, products, services and processes." All business units are integrated within the Global IT strategy. The goal is to deliver "customized business solutions for each business area in order to drive business transformation.”

Global IT has developed a highly structured governance model with assignment of specific responsibilities to various players to maintain accountability throughout any decision-making process. In brief, governance is executed thorough different councils within the company that are aligned with a business-unit. As necessary, Alpha may divide individual councils into regional sub-councils or committees.

Thus, Alpha Corporation manages privacy and security in part through use of relevant privacy governance bodies. These are segmented out by the kinds of data in their purview, and focus on clinical research and pharmacovigilance, commercial data, and employee data. It has established a distributed, tiered privacy infrastructure with focal points throughout the organization. The Alpha report states, "The purpose is to link business goals with privacy objectives, globally, regionally, and locally."

There are three privacy governance councils at Alpha in the U.S. to strategically address privacy concerns that are relevant to those respective groups. Each council is chaired by a senior executive from the applicable business unit. Periodic meetings are attended by certain leaders of that business unit and respective support functions, such as the legal department, IT, and the compliance unit. The Global Privacy Office plays a key role, including establishing these councils' charters and helping to setting the agendas and direction for their periodic strategic meetings. The councils can also aid in "day-to-day issues, such as selection of team members for Safe Harbor Certification due diligence." These meetings may establish or reinforce the company's strategic approach for certain cross-border data flows, such as Safe Harbor Certifications.

The Privacy Office has also encouraged the development of local data privacy governance bodies to help support the company's Country Operations. These local bodies are established with the assistance of local Data Privacy Stewards, who, among other things, assist with cross-border data flow issues.

As a general matter, the Global Privacy Officer also works closely with the Procurement group, the Law Department, and the IT Compliance department. The Privacy Office also works with a network of privacy-responsible individuals in Alpha's Country Operations to address privacy issues, including training.

A number of entities work together to ensure that all procedural rules are in line with current laws and regulation. IT Compliance works together with the Global Legal Department, the Global Privacy Office, and industry trade groups towards this outcome.

For a Global IT procedure to be updated into a new global policy, four levels of managerial approval are needed. An analyst within IT Compliance works with the business division's manager to create recommendations for a change in policy. The revisions are then submitted to the Director of Information Risk Management for approval. Finally, the CIO is to examine the policy and, if in accord, to approve it. The Alpha Report notes, "This structural framework is efficient enough to provide swift action, yet provides enough layers of review to ensure accountability regarding major procedural shifts."

### **Training.**

Alpha ensures that each clinical site has a monitor, who is responsible for ensuring that a clinical site has privacy practices and processes in place. The company makes sure that the monitor and the trial site are aware of applicable local privacy laws. If there are no applicable local privacy laws, the clinical staff should follow Alpha's own privacy principles, which are also part of the company's policies and procedures. The clinical staff receives extensive EDC training to make sure that data will be of high quality and protected from improper access.

Alpha is also engaged in extensive training of its personnel. The Global Privacy Office has developed a privacy training curriculum -- a set of five online training modules that assists in raising awareness of Alpha personnel on the importance of data privacy. The basic general privacy awareness course is directed to new hires and is a pre-requisite for three additional modules that are directed towards specific business areas and tailored to specific business processes based on the types of personal data they process. The fifth course focuses on practical guidance in areas of high risk, including the secured transfer and storage of data. As the Alpha report states, "To date over 19,000 U.S.-based colleagues have taken the basic privacy course." The training takes place through compliance courses maintained in several

languages on the corporate intranet. In many cases, an Alpha employee has taken two or three of the courses.

Finally, Alpha Corporation draws on external resources in managing its data flow. These resources include outside experts. Among these external resources are industry standard-setting organizations, such as TRUSTe and the International Association of Privacy Professionals. Alpha has also participated in other privacy-related organizations that have focused on data governance issues related to cross-border data flows. These entities include the Center for Information Policy Leadership, The Responsible Information Management Council, the European Privacy Officers Forum and European Privacy Officers Network, and the International Pharmaceutical Privacy Consortium.

### **Management of Data.**

The Alpha Corporation report describes its approach to management of data processes in clinical trials as well as the more general safeguards in place at the company. The first step in protecting a clinical trial subject's personal information is to obtain consent from her or him before any participation in the initial trial screening process. When collecting personal information, the site monitor is responsible for ensuring that the site has established privacy practices and processes. Collection of information is limited to that which is necessary for the clinical trial. The monitor is made aware of applicable local privacy laws as well as Alpha Corporation's privacy principles. De-identification is required of all clinical trial subject's personal information before it is sent to Alpha Corporation, the study's sponsor, or certain vendors.

The Alpha Corporation report also describes how it creates specific requirements for outside vendors as part of its due diligence before contracting with any such parties. In this process, the Alpha Corporation uses a privacy and security risk assessment before engagement of any outside vendors. Its due diligence with vendors includes determining the level of sensitivity of the personal information to be provided, performing a risk assessment when the vendor is processing personal information, and basing the next steps on the result of the assessment.

In its assessment for privacy, Alpha Corporation determines whether the vendor has a documented privacy program and will be able to meet the requirements set forth in the contract. In its assessment for security, Alpha determines whether the vendor has a documented information security program, access controls, authentication tools, encryption for sensitive information, proper training, procedures in cases of security breaches, and is able to comply technologically with the contractual requirements.

The business units, and the legal and procurement departments at Alpha Corporation, also use standardized privacy and security contract language with those

vendors that process personal information on the company's behalf. A required checkpoint is whether cross-border transfers of the information will occur. If so, the contracting party should provide to the legal department information about which countries will be involved so that appropriate contractual provisions may be included.

Alpha Corporation also provides extensive procedures for information security. These include a four-tiered data classification scheme: public, standard, enhanced, and restricted. The company also manages compliance risk through a well-defined process. This aspect of its operations involves IT Compliance, Global IT, the Global Privacy Office, and the business units.

**Access.**

There is a requirement of special training before Alpha Corporation will grant access to its network. Moreover, as part of its information security program, Alpha Corporation provides strong qualifications regarding password strength. There also is a requirement to use a token when connecting to the Alpha network from the outside.

## **2. Beta Corporation**

### **Company Profile and Overview of the Case Study.**

Beta Corporation is a marketing services company. Its report examines a project in which it developed and then helped to manage a global marketing solution for a consumer electronics company. Beta's design and execution of services for a client are at the core of this case study.

### **Case Study: a Global Marketing Database.**

Beta Corporation was hired to develop a global Customer Relationship Management (CRM) solution for its client, which is a multinational consumer electronics firm with headquarters in Europe and over one hundred offices in eighty countries. The client wished to centralize its databases of personal information about its customers to permit the marketing departments across the company to draw on these data. In the past, the client had sold exclusively through retailers. Now, the client wished to sell its products directly to consumers via its own web portal. The information at stake was maintained in many international locations. Over time the client also had acquired numerous brands throughout the world. These brands each had their own CRM system. Each system had different types of customer data with great variation in quality and coverage and different functionality for use of the data.

The client company sought to centralize its global marketing activities to increase revenue, improve usability and reduce the cost involved with multiple systems. It hired Beta Corporation to help it standardize and upgrade its different CRM systems to a single global system across all its brands and international locations. To do so, Beta Corporation created a centralized global CRM solution that it housed in the U.S. This system consisted of three global marketing databases – one that maintained customer data, one for prospect data and one for permissions for use that consumers had provided.

### **The Data Processing System.**

The case study provides a useful example of dynamic international databases in action. The information system that it depicts is process-oriented, and not simply focused around any discrete transfer. Rather, than concentrating on a database or databases, Beta Corporation developed a networked series of processes to deliver a business result. The service that Beta Corporation provides is a chain of serial processes. These processes involve Beta, its client, and, in some cases, other outside vendors, in executing different data management practices as dynamic needs arise. From a legal perspective, Beta used a combination of Safe Harbor (for data from Europe) and contracts to transfer data on an international basis.

As an illustration of this process-oriented, dynamic and international solution, Beta Corporation provides a rich description of its services in action for a typical marketing promotion. It states:

[A] marketer in Spain would use the criteria developed by the analytics vendor in India to select a list of customers from the global CRM system in the U.S. which would be transferred to their call center in Mexico for execution of a telemarketing campaign to consumers in Spain. Results from the telemarketing effort from Mexico would then be fed back to the U.S. to update the information in the global CRM system.

To maintain the global marketing system, frequent batch updates are used. Even daily updates of information are possible. Thus, the services provided by Beta Corporation are highly dynamic, and can respond quickly to client needs.

Another example from the Beta Corporation's report illustrates the chain of serial processes. This second example concerns pan-European email campaigns with information from both Beta and the client. Beta captured email addresses through a consumer survey in which consumers gave permission for use by a third party for marketing purposes. Information that lacked appropriate permissions was purged. The email addresses from Beta were combined with other data the client had about previous transactions with consumers. Drawing on segmentation criteria developed by an analytics vendor in India, the client was able to conduct international email marketing campaigns using the CRM system.

The information was maintained and campaigns were distributed from the U.S., where email messages were prepared in the local language for each European country. For example, a marketer in an E.U. country, such as the United Kingdom, would draw on the segmentation criteria developed by the analytics vendor in India to identify a list of U.K. consumers to receive a specific email promotion. At the request of the client, the global CRM system housed in the U.S. would then send out an email message to the customers in the U.K. Simultaneously a different campaign for customers in France or Germany could also be taking place driven by the marketing offices of the client in the respective country.

Finally, the client used support personnel from vendors in addition to its own staff. Such support included the client's analytics vendor in India, their external backup facility in the U.S., and various outsourced call centers in places like the U.S., Mexico, Belgium, and India. As the Beta Corporation states, the CRM solution involved data from "hundreds of sources contributing information from dozens of countries."

## **Management of Personnel.**

This project drew on privacy and compliance departments from Beta Corporation and its client throughout the world. The client managed the project out of its European headquarters, and Beta managed its part out of the U.S. The result was a complex management process with detailed compliance obligations for both Beta and the client.

There is a corporate privacy team at Beta. It is headed by a Global Privacy Office in the U.S. with three regional privacy officers across the globe as well as in-country privacy officers. The Beta Corporation's privacy officers report to a chief privacy officer, who is located under and reports to the General Counsel of the company. The role of the privacy team at Beta is to set policy related to information collection and use, oversee all compliance obligations and best practices, and train the different lines of business on the required policies. The membership of the privacy team has been very stable with employees who have been on the job on average for over seven years.

In addition, the client's privacy office has a similar structure as Beta Corporation. It has a Global Privacy Officer, who was also a senior legal counsel for the client. Each country has a local privacy officer.

The Beta Corporation worked with a Privacy Impact Assessment (PIA) form that its client supplied. The PIA was designed to ensure that all personnel, including outside vendors, would follow applicable privacy laws and would properly address security issues. The PIA consisted of approximately sixty questions. These questions looked at issues such as the uses of the data, the permissions obtained for these uses, the kinds of security, and the nature of the cross-border transfers that will take place. It also required information to be gathered about who is responsible and accountable for all processing steps, from system design, to implementation, and then ongoing operations.

The PIA was used at different times in the project. It was first utilized when the client approved the project with Beta Corporation. Once the project was implemented and the system was running, the PIA was again executed. Finally, Beta Corporation continues to use the PIA on a periodic basis.

In addition to its use of the PIA on the project, the Beta Corporation experiences numerous onsite audits that other clients carry out on Beta at any given time. Each year, over eighty client audits occur at Beta. At present, there is no single audit approach. For example, highly regulated clients in such sectors as financial, medical or insurance each have their own defined audit processes. Beta Corporation dedicates full-time employees for assisting with these onsite outside audits. Finally, Beta also conducts an independent audit of its security on a regular basis for itself.

## **Training.**

Beta's training of its privacy staff includes the use of primarily in-house training augmented with some external training and International Association of Privacy Professional certification where available. Beta also offers some of its in-house training to clients.

## **Management of Data.**

The use of privacy officers, PIA's, and audits are a central technique for managing personnel. At the same time, these techniques play a key role in managing data processes. Moreover, Beta has numerous other techniques in place to manage its dynamic, international databases in a process-oriented fashion. One of the most important of these techniques is for Beta to map all the data flows and uses for these types of projects.

Beta devoted considerable attention to the mapping of all data flows. It explains:

We start by identifying all data sources, whether directly from the individual or from a third party. Then all data is charted as it flows through all the various processes. This includes data cleansing, data integration, analytics, and the maintenance process for the marketing database. Then all uses and users of the database are identified and permissions are validated. This is a very comprehensive process.

One complexity for the project is that client data about sale transactions may be collected on a client's website in country A, but the transaction may be initiated by customers from countries A, B, C, or D. The data will all be sent to the U.S. to be maintained in the CRM solution. The client in countries A, B, C, and D will have access to the data for analytics and planning marketing campaigns. All these data flows are mapped in advance with the Beta Corporation putting appropriate controls for privacy and security in place.

A particular concern for Beta is in identifying the provenance of personal data. As the Beta Corporation stated, "With hundreds of sources contributing information from dozens of countries, it was necessary to map each source and flow to assure all the proper notices and permissions were granted. For any global system, it is critical that there be a means of maintaining all origination and transfer intelligence accurately over time." This task of tracking data provenance becomes essential due to an organizational shift towards process-oriented administration of information. As a specific example from the Beta case study, purchases made by a customer in Australia might have been made on a Malaysian website and transferred to the U.S. for

fulfillment of the order. Information about the origins of the consumer data must be collected, if possible, from the start and then follow the information.

Throughout the project, data security was a major consideration. Beta Corporation uses secure data processing centers; regular audits of these centers are carried out by Beta and its clients. Ongoing upgrades are made to system security with a central role played by Beta Corporation's Chief Security Officer and his team. Sensitive data are required to be transmitted in an encrypted manner. Finally, most of the information was transmitted between Beta Corporation and the client over a private leased network and not the Internet.

### **Access.**

The shift to the cloud and an information system that is a chain of serial processes requires careful attention to access controls and authentication. Beta Corporation controls access by each employee to each of its business systems and client solutions. Only employees working on the account and overall system administrative personnel are permitted access to client data.

Beta uses userid/password authentication for employees working from workstations in its office. It uses two-factor authentication for access from external sources, including userid/password plus a randomly generated password from a token. All Beta Corporation passwords are changed every forty-five days.

### 3. Gamma Corporation

#### **Company Profile and Overview of the Case Study.**

Gamma Corporation is a diversified financial services companies and among the largest banks in the world. It provides banking services, wealth management services, corporate and investment banking, as well as transaction processing services on a worldwide basis. Its report examines its automation of the mortgage renewal process. The report demonstrates the company's cautious and incremental use of a third party vendor in India.

#### **Case Study: Moving Elements of an Operation Offshore.**

In the 1990's, Gamma Corporation moved from a local branch model in its banking operations to a centralized domestic model. As part of this process, it changed from handling mortgage renewals at local branch offices to using central computers to store key information about mortgages. In its subsequent waves of automation, Gamma introduced online banking to allow clients to access information on their own and to contact support teams via a secure messaging system.

Beginning in 2007, Gamma Corporation then began to use "a global third party vendor processing model." At first, Gamma Corporation moved only its "midnight-shift team" to India. It then continued "to move some additional mortgage renewal processing offshore to India." The company sought to identify processes that did not add value in the company's relationship with the client. It wished to focus on "high touch" services, such as providing advice to clients, or creating an "advice-driven platform" for client services. As part of the goal, it was also interested in finding ways to make it easier for the front line staff to service its customers. The operation of mortgage renewal processing is not considered to be a core competency of the Gamma Corporation. By shifting it offshore, the company sought to "free up" resources to improve overall service to its customers. At the same time, Gamma personnel continue to have all direct contact with the bank's clients. As Gamma notes, "No tasks that work directly with our clients have been moved offshore."

Gamma has also been careful regarding information security. It originally sought to have no personal information stored by the overseas vendor. Nonetheless, it found "some challenges relating to the way our computer system handled 'temporary files.'" As a result, "some systems had to store temporary copies of individual records on the local hardware to operate correctly." Gamma Corporation chose to limit the storage of mortgage renewal information overseas to "individual records" on encrypted devices. By the term "individual records," it draws a distinction with "entire list of renewals." Such lists are not stored overseas.

Finally, the company put processes in place “to ensure that all escalations relating to the employees or to items that can affect the service to Gamma Corporation’s clients are sent to Gamma Corporation people located in North America.” Examples of possible types of escalation include challenges that the off-shore vendor finds related to computer, privacy, or information processes.

### **The Data Processing System.**

The Gamma case study demonstrates a limited, highly targeted use of international offshoring. Gamma Corporation's analysis led to a conclusion that its processing mortgage renewals in-house did not provide value for the relationship with the client. Indeed, Gamma concluded that if it shifted this activity offshore, it would in fact "free up" company resources for services that would add value. Gamma identified a need, however, to have strong processes in place to make sure that its use of international outsourcing would be accompanied by robust protections for privacy and security.

### **Management of Personnel.**

The Gamma Corporation has created a team to monitor the off-shore vendor for its performance and other issues. This team performs a quarterly review of the access to data in place for people at the vendor to ensure that access is appropriate and will cease once no longer appropriate. The monitoring team is located within North America and consists of Gamma employees. The head of the off-shore initiative at Gamma Corporation is accountable for ensuring that complete documentation is in place and that all reviews are carried out. Moreover, all aspects of the outsourced program are subject to ongoing compliance monitoring and independent testing by the Gamma Corporation's internal auditors. As noted above, the company has put processes in place to ensure that all performance issues related to the offshore vendor are escalated to appropriate people at Gamma Corporation.

More generally, the Gamma Corporation has management structures and safeguards in place regarding privacy and security compliance that do not apply solely to the program described in the case study, but are part of its overall privacy and security compliance program and are applicable throughout Gamma Corporation. Gamma Corporation has established a “Global Privacy and Information Risk Management Framework.” Compliance with this framework rests with the “Executive Head of each platform.” The Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) provide “oversight, guidance and support.” I will discuss the Global Framework in more detail below in this section as well as in the next section concerning management of data processes.

Training in privacy and information risk management is required for all new employees at Gamma. This training must be completed within thirty days of joining the company. In addition, different kinds of training are required based on the unit

where a specific employee works and based on different responsibilities of the employee. Gamma Corporation has developed numerous “job aids,” including quick reference guides and FAQ’s. In addition, every two years, all employees must successfully complete a test based on Gamma Corporation’s Code of Conduct. A significant portion of this test is dedicated to privacy and information security requirements.

Gamma Corporation created special controls to manage the mortgage renewal information at the center of its case study. There are also general controls that are in place for all Gamma projects involving personal data. The Global Privacy and Information Risk Management Framework is focused on creating “a holistic approach to managing information” throughout the information lifecycle. This management tool looks at four stages: (1) the creation and collection of information, (2) its use and disclosure, (3) its retention, and (4) its disposition or destruction.

The Gamma Corporation also has two sets of governing policy documents that relate to information management and that support its Global Privacy and Information Risk Management Framework. These are its Privacy & Information Risk Management Policy and its Information Security Policy. In addition, Gamma Corporation has established a risk assessment approach for all business processes to be considered for offshoring. The risk assessment is divided into four sections: (1) a Program Level Risk Assessment, (2) a Country Level Risk Assessment, (3) a Vendor Level Risk Assessment, and (4) a Project Level Risk Assessment.

Gamma carefully considered the kinds of access controls that were necessary for employees and vendors in this case. As an example of the result of this analysis, it requires the off-shore outsourcing company to use only the Gamma Corporation email system for Gamma business. It does not permit remote access to the Gamma network for employees of the off-shore outsource company. These employees cannot use a VPN, but rather must work on dedicated workstations on their offshore site. All email communication between Gamma and the offshore location is done via the Gamma email network. In consequence, all communication between Gamma and the offshore vendor takes place either through a dedicated private line or through an encrypted tunnel.

## 4. Delta Corporation

### Company Profile and Overview of the Case Study.

Delta Corporation is a developer and provider of Internet-based software and online services. Its report first looks at data flows identified in three consumer-oriented online services. These are (1) an electronic mail service, (2) a real-time messaging service, and (3) an online file-storage service. The Delta report then examines its organization-oriented services. This second group concerns an Internet-based integrated offering that permits access to an online suite of software.

### Case Study: Online Systems for Consumer-Oriented and Business-Oriented Services.

On the consumer-side, the three consumer-oriented services permit electronic mail, real-time messaging, and online-file storage. In these services, data flows can take place at two different periods. A data flow can occur at the time of data creation when data moves between the consumer and the data center. It can also occur at the time of information retrieval. At that moment, data flows take place between the data center and the message recipient's server (in the case of e-mail), the message recipient's client (in the case of real-time messaging), or the client's computer (in the case of data storage).

At present, Delta generally hosts the consumer-side data in the U.S. This approach means that the consumer information of international customers is necessarily an international transfer as it flows to the U.S. At present, moreover, information is kept within a single location, and load balancing takes place within the same data center. An international hosting of data would permit load balancing to take advantage of different time zones throughout the world. This technique would allow balancing of data loads since data flows tend to exhibit peaks in demand at predictable times in each geographical location. The Delta Corporation report states, "Moving forward, Delta may distribute user data location in order to improve the performance of its services or meet other objectives, including compliance."

On the organization-side, Delta Corporation's case study concerns an Internet-based integrated offering that allows customer access to an online suite of software. North America, Europe, and Asia are the chief markets for this service, and customer data are primarily hosted in the region in which customers register their billing address. For business continuity reasons, these services may already have back-up centers at different locations within a single country. Such system design seeks to secure data in cases of power outages or natural disasters.

## **The Data Processing System.**

The Delta case study reveals a system of data flows, whether oriented towards consumers and businesses, that are international. These flows are generally from the consumer's location, wherever in the world the customer is located, towards the U.S. At the same time, data locations of the Delta Corporation may be distributed to an even greater extent throughout the world in the future. Already, its organization-oriented services are hosted on a regional level, which means these customer's data are crossing national lines.

Delta believes that the services at the center of its report mark only the beginning of its movement as a company to sharing data on a global basis. It views the cloud as especially important for the future of its services on the organization-side. Delta is concerned about regulatory challenges at present to this kind of service model. Accordingly, it views the need for global harmonization of regulation as extremely important.

## **Management of Personnel.**

Two groups at Delta Corporation are responsible for attention to policies and standards for the Delta online infrastructure that the case study depicts. These are the Infrastructure Services and Compliance Group and the individual online service groups.

The responsibilities of the Infrastructure Services and Compliance Group include protecting Delta's data centers and making the physical and logical infrastructure for online services secure and reliable. Individual service groups are responsible for application-level privacy, continuity, and security processes. These groups also adhere to processes defined by the Online Services and Compliance Group and services-specific criteria that are defined at the divisional level.

Delta Corporation has a staff of full-time privacy professionals across the different business units, and other employees who help to ensure that appropriate and effective privacy policies, procedures, and technologies are used in the business units in which they work. Delta also has a group that is devoted to defining corporate-wide policies for data security and privacy. The security and privacy group is responsible for tasks including: establishing general principles and guidelines for data collection, retention, and data use; creating incident response plans for privacy and security related incidents, as well as defining appropriate escalation paths; developing and documenting best practices that are to be integrated into the company's software and online services development lifecycles. The security and privacy group has embodied its principles and guidelines in a series of internal standards and guidelines.

## **Training.**

Training is an important component of Delta's strategy for privacy and information security. The company requires designers, developers and operations personnel to update their skills on an ongoing basis. Key elements of Delta's training approach vary for: (1) teams that develop and manage software components for services, and (2) members of the online service operations team. Both groups must take a clearly defined number of course-hours each year. Employees in the teams that develop and manage the software components must also take course that cover topics relating to Delta's privacy standards for developers and its process standard that describes how application and data security are to be built in to the development lifecycle for software. Members of the online services team are required to take an online training course that provides a detailed description of current security and privacy processes, as well as mandated approaches to incident response and compliance response.

## **Management of Data.**

Delta Corporation manages data with reference to the company's privacy principles. These include: accountability in handling personal information, notice to individuals about data use, quality assurance steps to ensure that personal information is accurate and relevant, access for individuals who wish to inquire about and, when appropriate, review and update their personal information. Other principles are: enhanced security for personal information, and compliance with Delta privacy policies.

Online service teams are required to pass a security and privacy review for any new service or service updates that bring significant changes in application code or logic. These include meeting a formal security review with defined steps that culminate in a final review. As for the privacy review, it starts with a self-assessment and then progresses through a series of formal milestones. During this process, the online application team and privacy security group draw on resources of the legal department to identify the laws, regulations, and Delta policies that apply to this service. Based on this review, the online application team and privacy security group take steps to comply with all applicable laws, regulations and Delta policies. Additional safeguards apply to personal information that is sensitive, such as health information, social security numbers, or other national identifier numbers. These data are subject to Delta standards for physical and logical security, including placing servers in physical cages in data centers, and using encryption on data at rest.

Delta online services are also subject to an additional process that is carried out by a Delta online risk management team. This group leads each online service team through assessments of privacy, security, compliance with regulation, and other factors. The assessments are focused on specific frameworks and culminate in final reviews of a series of listed categories.

The Security and Compliance Group for online services has also established a comprehensive framework that looks at making controls efficient and effective. The framework is based on a five-step methodology that requires: (1) identification and integration of requirements, (2) identifying and remedying gaps in process and technology controls, (3) testing and measuring the effectiveness of proposed controls, (4) engaging with third-party certification authorities and auditors, and (5) documenting instances of non-compliance, assessing the root cause, and tracking until fully remediated.

### **Access.**

As a central principle in managing data, Delta implements the use of “a need-to-know and least-privilege basis” for Delta full-time employees. It has also centralized access management, which is made through a centralized electronic form. This form is stored and is subject to routine audits. The audits are made at the individual account level and also in terms of checking on requests and responses.

Authorization to information is carried out through a two-tier process. First, one needs an authorized account at Delta. Second, one needs to have access to an individual resource. The Delta owner of that resource evaluates an employee’s specific role in deciding which kind of access is appropriate to the account. There are also rules regarding the creation of strong passwords, including rules for minimum password length. Logging on to the Delta network requires a login account, passwords, and a smartcard with a digital certificate.

## 5. Epsilon Corporation

### **Company Profile and Overview of the Case Study.**

Epsilon Corporation is a provider of technology solutions and services for a range of customers, including consumers, the public sector, and businesses. This report looks at its product registration process as an example of a data flow within Epsilon's consumer PC business. This case study also demonstrates how product registration information is used within the customer support process.

### **Case Study: Product Registration and Customer Support Service.**

The Epsilon report shows how the data generated through product registration supports multiple businesses processes. These processes are consumer support, warranty, “Customer Knowledge Management”; and “Consumer Relationship Management.” Through the product-based registration data flow, Epsilon seeks to: provide more efficient and accurate support and warranty experiences, understand more about its customers, and deliver relevant information to those customers who choose to receive it.

The product-based registration data flow originates from data that customers provide when completing the registration form presented during the product's setup. The relevant data can also be generated during a subsequent registration reminder if a customer chooses the "register later" option during the setup. The information collected includes: name, PC set-up language selected, contact consent, product model ID and serial number, email, postal address, phone contact, and “born-on date.” This last term refers to the date of the registration.

At the time of the customer's product registration, Epsilon presents her with its online privacy statement. For customers in other regions, this policy is available in 32 different languages. If the customer is not connected to the Internet at the time of setup, an offline version of the privacy statement is presented. In addition, there is a "Learn More" link that provides additional information about product data that is collected and transmitted along with the registration data that the customer provides.

Before the registration record is transferred from the product-based application to the Epsilon servers, the registration application encrypts it and stores it on the customer's PC. Once there is an active Internet connection with the customer's PC, the device transmits the encrypted file automatically to Epsilon using SSL.

Following a consumer's registration of her PC with Epsilon, a support agent is able to access the registration data should the consumer contact Epsilon, whether via

online chat or phone. Depending on the location of the customer and the time of the day, the customer will be automatically directed to a specific global support center. Epsilon has international support centers in India, Costa Rico, and Bucharest. More details about the global support centers are provided in the next section.

### **The Data Processing System.**

The Epsilon report offers a rich illustration of a product-based registration flow. Transfers from a consumer's PC respect local laws. For cases of transfers from the European Economic Area, Epsilon utilizes the Safe Harbor framework and has comprehensive intercompany agreements in place between all Epsilon entities and countries to ensure that original commitments are understood and upheld.

The product-based registration data flow is multi-directional. It moves from the consumer's PC to various Epsilon and vendor databases.

All registration data flows to Epsilon Corporation are encrypted and transferred in a secure fashion. Registration information is warehoused exclusively in U.S. data centers. Access to that data by Epsilon employees takes place through secure internal transmissions and is subject to company policies and intercompany agreements. The privacy and security regulations that Epsilon places on the information follow it. As the company's report concludes, "The original obligations are respected no matter where the data is accessed, viewed or transmitted within Epsilon."

Note as well that third party vendors, acting on behalf of Epsilon, may participate in this data flow scenario. Epsilon places the third parties under contractual agreements, which require the third party to uphold Epsilon policies and use any personal data only to perform the contracted work.

As discussed in the preceding section, Epsilon draws on the product registration information when a registered customer contacts it for support. The goal is to serve customers as quickly as possible. Support agents are located at different international locations, and Epsilon assigns tasks to different locations using an algorithm, which incorporates several factors. The result is that the data flow relating to customer service calls is extremely dynamic and cannot necessarily be predicted in advance.

Some more details about the data flow relating to customer service calls will illustrate these points about the dynamic nature of this process. Part of the model for distributing customer service calls, as reflected in the algorithm, relies on a "follow-the-sun" approach, which means that Epsilon considers the time of the day in different service locations when a customer calls for support. This element of the approach means a customer requesting support in the middle of the night in one country might be more likely to be assigned to a service center in a country where it is

still daytime. There are other elements built-in as well to the Epsilon algorithm for distributing service calls. These include resource loads, the type of call, the load of agents in a certain location, and whether all agents there are busy.

### **Management of Personnel.**

At the Epsilon Corporation, the CPO is responsible for global privacy strategy, policy, governance, and operations. The CPO reports into the Ethics & Compliance Office. The Epsilon CPO works for the Chief Ethics and Compliance Officer, who in turn works for the Chief Executive Officer. Epsilon's privacy policies are based on the company's standards of business conduct.

The CPO leads a Privacy and Data Protection Board, which is made up of senior executives from all key businesses, regions, and functions. The Board's charter emphasizes a number of tasks. These begin with the identification, management and mitigation of compliance and reputation risks. The Charter also requires the Board to develop privacy and data protection policies, practices, procedures, and training. Among its other tasks are to provide a process for issue escalation and resolution, and to monitor and audit compliance at Epsilon with laws, policies, plans and "the highest ethical standards."

The CPO is supported by three senior regional privacy officers, legal counsel in each region and major country, and government affairs representatives in the U.S., Canada, Latin America, Europe and Asia. The CPO and regional privacy officers maintain regular contact with key thought leaders, advocates, and regulators throughout the world.

Epsilon's Privacy Office and legal department have established a process that uses the company's Privacy and Data Protection Board "to assess, rate and prioritize risks and opportunities." It does so through a five step process that involves: (1) trend analysis, (2) input from board members, (3) reasons for proposed decision and in-depth discussion with the board, (4) prioritization related to risks and impact, and (5) formalization of plans and tracking.

### **Training.**

Epsilon uses multiple mechanisms for training its employees and partners. In addition to its standard privacy training for all employees, it requires additional training for all employees granted access to systems that contain sensitive personal information. Epsilon has accomplished training of more than 99% of its current workforce in "specific mandatory privacy training."

Regarding vendors, Epsilon requires that the vendor demonstrate the ability to uphold requirements for personal information and sensitive information. The vendor

is required to have privacy training, and in some cases Epsilon will supply specific training material or specify the content that it wishes in the vendor's training program.

### **Management of Data.**

Epsilon Corporation maintains comprehensive information security standards and policies. It uses appropriate physical, technical, and administrative procedures to safeguard the information that it collects and transfers. Working in close partnership with the CPO, the Chief Information Security Officer is responsible for data security. As noted above, vendors and other service providers are bound by contract to uphold Epsilon policies. All policies, standards, and guidance are documented and available to Epsilon employees.

Epsilon uses a variety of security technologies to help protect personal information from unauthorized access, use, or disclosure. The personal information provided to Epsilon is stored on computer systems located in controlled systems to which access is limited. When Epsilon transmits confidential information, such as credit card numbers or passwords over the Internet, it is protected through the use of encryption, such as SSL. Credit card numbers are used only for processing payments and not for any other purposes. As part of its real-time payment processing, Epsilon subscribes to a fraud management service.

### **Access.**

Access controls at Epsilon Corporation vary based on sensitivity of the information in a system. Every sensitive database has an assigned access manager. Access to a database relies on the Epsilon digital badge process, which is multi-layered and includes a token to be inserted into a PC before a database with personal information may be accessed. For access to certain databases, moreover, an Epsilon employee must be onsite even with the highest level digital badge. Epsilon Corporation also enforces specific length and structure requirements for passwords.

## 6. Zeta Corporation

### **Company Profile and Overview of the Case Study.**

The Zeta Corporation is a globally integrated enterprise that helps public and private sector organizations through the use of business insight and advanced technology solutions. Its capabilities include services, software, hardware, research, and financing. The Zeta Report examines its global recruitment process (GRP) system. This web application is used to support Zeta's recruitment process throughout the world.

### **Case Study: A Web-Based Global Recruitment Process.**

The GRP system permits interested individuals to apply for an employment position, independent of the country in which they are located or the country from which the opportunity originates. It allows "a world-wide view into available jobs at Zeta Corporation" that leads to unique benefits for the individual and Zeta Corporation. The GRP system allows Zeta and its wholly-owned subsidiaries to assist in identification and selection of candidates, both internal and external, for employment opportunities. It also assists in the employment process by allowing HR recruiters, hiring managers and other participating parties to manage employment offers and acceptances. This system is used as well for managing Zeta's equal opportunity requirements.

A third party vendor located in Zurich, Switzerland hosts the GRP system application. The Zeta report notes, "Cross border data flows occur dynamically as part of this system." As the report also states, the GRP system leads to "data transfers on demand."

These data transfers cannot necessarily all be predicted in advance of a job posting. A job can be posted from South Africa to the GRP system server in Zurich, and then accessed by Zeta employees in over 100 countries. Some of these employees will send their personal data to the system. In addition, outside recruiters from these or other countries might send in data. In Appendix C to this study, I have included a longer illustration from the Zeta Report of how data within the GRP system can flow dynamically and in an international fashion.

Within Zeta, second level application support and HR recruitment support are provided to applicants and hiring managers from Zeta's India office. System and application technical support for the GRP system are provided from Zeta service centers in Hungary and South Africa. The GRP system may also supply data to other Zeta data systems, which are located in various countries, and which support the recruitment process. These information systems concern areas such as government reporting requirements, compensation, and the ordering of IT equipment.

## **The Data Processing System.**

Any Zeta manager or authorized HR recruitment personnel may create a job posting on GRP. Basic contact information is collected from the requisition creator, such as name, title, and business contact data. This information is not, however, displayed to applicants. Any interested party may gain access to the requisition from Zeta Corporation's external website.

Personal information about applicants from all over the world is collected over the Internet in different ways. Applicants can submit personal information in support of their job applications. Recruitment agencies can submit personal information about potential candidates. Zeta employees may refer potential candidates for an opportunity. Each of these parties may be in different countries. For an illustration of the global nature of this system, please refer to Appendix C's discussion of a data flow from this system.

If the applicant is already a Zeta employee, in addition to the personal information that she provides directly at the time of the application, certain other personal data already in Zeta's possession and housed in other databases located in various countries may also be sent to the GRP system. For certain data sets which are automatically extracted from other internal databases, the internal applicant is also given the opportunity to decide whether or not this information should be added to her application.

Only personal information which is necessary for a specific stage of the recruitment process will be sent into the GRP system, or otherwise collected. The necessity principle is defined in accordance with local legal recruitments and the internal policies of Zeta Corporation. Moreover, at the time of collection of information, Zeta provides a "click to accept" privacy statement. This statement indicates the manner in which the information is to be used, to whom it may be made available, and that the data may be stored or processed in various locations around the world in connection with the recruitment process. Candidates may at any time update, correct, or delete their personal information.

## **Management of Personnel.**

The GRP business process owner, working with the Human Resources function and support groups such as Legal and Business Controls, is responsible for ensuring that the process is in compliance with internal and legal privacy requirements. This responsibility extends to cross border data flows that may occur as part of the GRP process.

Recruitment agencies and any employees referring a candidate have additional, special requirements. They must confirm that they have obtained the consent of the

individual whose personal information they are submitting for the purpose of applying for employment. In addition, they must confirm that notice of international transfers for processing has been provided to the candidate.

More generally, Zeta Corporation's Data Security and Privacy Steering Committee oversees its policies, procedures, and programs relating to data management and data protection. The committee is made up of cross-company senior executives, and co-chaired by two senior leaders. These are Zeta's CPO and the Assistant General Counsel of its IT Delivery group. Both leaders are Vice Presidents at Zeta.

Zeta's CPO also has direct global responsibility for its leadership and compliance in the area of personal data policies and practices. He leads a cross-unit, cross-function and cross-geography privacy organization that includes the participation of leaders and subject matter experts from departments, such as law, compliance, CIO/IT, corporate security, HR, Global Services, and Zeta Research.

Zeta has security leadership teams for IT and physical security. These teams are responsible for Zeta's own enterprise data security standards and practices.

Where suppliers may be granted access to personal information, Zeta makes use of contractual clauses to ensure privacy and security requirements are met. It also assesses suppliers for their ability to meet such requirements before any contract is awarded. Finally, it monitors supplier compliance with requirements for privacy and security.

### **Training.**

A central part of the Zeta Corporation strategy for privacy and security is workforce education and awareness. Zeta employees are regularly required to review, and certify their review, of the company's code of conduct. These guidelines contain sections on privacy and security. Zeta employees are also required to complete a companion course with materials related to privacy and security.

In addition, Zeta makes general and job-specific training in privacy and security available to all of its employees and contractors world-wide. Depending on their job responsibilities, Zeta's employees and contractors are either required or encouraged to engage in privacy and security education. In the specific case of the GRP system, HR recruiters and managers are required to take privacy education before Zeta permits them with access to the system. The company's report observes, "[T]his education offering focuses on the personal information management requirements such as the need for notice and consent; the Zeta policies which are applicable; the global processes we have in place in support, such as our access request process, our data incident reporting and management process; etc."

## **Management of Data.**

The GRP system implements controls “to provide an adequate level of protection to the personal information being collected, accessed and otherwise transferred.” Basically, Zeta limits access to selected data fields to certain categories of individuals, and further restricts access “only to those individuals within those categories who must access the data in relation to the purpose for which it was collected.”

Depending on the country from which the data originates and where the processing will occur, Zeta will put in place different kinds of data transfer agreements. These agreements include the E.U. Model clauses. The goal is to satisfy the legal requirements of all jurisdictions that are involved.

Beyond the GRP system, Zeta Corporation has implemented a global data privacy policy. As the Zeta report states, this policy “sets, at a high level, the basic handling requirements that apply to personal information.” The privacy policy is supplemented by a number of corporate instructions, guidelines, and standards.

A central element of Zeta’s approach to privacy accountability is its program for privacy assessment. This online program uses an automated “smart” self-assessment tool to allow the business process owners to self-assess the degree of risk that their process or IT application poses. The privacy assessment program measures these risks, moreover, against internal policies and applicable laws. The Zeta Report states, “The tool allows these actions to be tracked to their completion by both the process owner as well as the privacy team.”

Since the assessments are conducted online, the results can be collected and analyzed in real time. As a consequence, it is possible for privacy leaders to provide immediate feedback to business process owners. Moreover, assessment results can be summarized into “scorecards.” This documentation provides highly useful information for business process leaders and for Zeta leaders at the global, regional, and country-wide levels. The scorecards reveal important privacy-related information at a glance.

Zeta also has a set of complimentary IT security policies. These policies establish requirements for protection of Zeta’s worldwide IT systems and the information assets that they contain. In addition, Zeta maintains a corporate security policy, which concerns matters such as physical security and information protection.

Zeta Corporation has deployed several technical measures to enable data security. For example, it uses an automatic scanning tool to ensure that all workstations are compliant with security standards. It also requires that sensitive information be encrypted while in transit and while at rest in corporate databases. In addition, portable media containing such information must be encrypted and sent only

through approved carriers. Finally, Zeta has implemented a global data incident response process. This process allows prompt identification of potential incidents and their management.

### **Access.**

Before gaining access to the privacy assessment program, process owners at Zeta must register with the Corporate Privacy office and respond to a series of questions. These questions allow the privacy office to identify processes which may represent increased risks due to the nature of the personal information involved, the purpose for the processing, or other factors. In addition, a process owner whose assessment is not fully compliant will often approach the team for further consultations. Such consultation may also occur before a privacy assessment is finished, or as it is being carried out.

The company also has stringent mechanisms for access control to ensure that only authorized individuals can access data. For example, as noted above, candidates may at any time update, correct, or delete their personal information. Before individuals can apply for a position, however, they must register with Zeta and choose a secure password, which will then permit them to create a profile and apply for a job. Using this same user name and password, the individuals can access and update their information into the GRP system.

Access controls for employees and vendors is based on their need to know. A manager must make a requisition request for access for it to be granted. Thus, there must be a match between a function and a need to gain access to the GRP system to be able to log into it. Since GRP is a HR function, HR created the documented process concerning who has access to the system as well as specific data fields within it. Moreover, there are requirements for length and structure requirements for all passwords. These expire after ninety days.

## Appendix C: An Illustrative Data Flow from the Zeta Hiring System

A Hiring Manager in Sydney, Australia needs to hire a SAP Consultant. He contacts his local HR recruiter and provides the recruiter with the details for the position. The local recruiter sends the information to Recruiting Support in Kuala Lumpur, Malaysia to create the requisition in the Global Recruitment Process system. Recruitment Support creates the requisition and posts the requisition both internally and externally. The posting is now viewable worldwide.

John, a Zeta U.S. employee logs onto the GRP system to see what SAP opportunities are available globally. He spots the Sydney, Australia role and applies. The recruiter and hiring manager for the role receive an auto-notification that a new internal applicant has applied and that the new applicant, applying from out of country will need appropriate work authorization. John's manager also receives a notice that John has applied for the post.

The hiring manager and recruiter are able to review information provided by John for the job as well as basic employee data available to that employees via Zeta's "about you" tool. After an initial interview John determines that he is not ready to localize to Australia, but instead he thinks that his sister, Jane, who currently lives in New Zealand would be a great match for the role. John completes an employee referrals from within Global RP and assigns his sister to this requisite.

John's sister Jane receives an email notice, in New Zealand, that she has been referred by a Zeta employee for a specific requisition and is asked if she wishes to complete her application. Jane applies for the job.

John is able to see within the employee portal of GRP, under "My referrals" the status of his referral is now "applied, under review." The hiring manager and recruiter review the Jane's application and decide to schedule an interview. The recruiter sends a request to recruiting support in Kuala Lumpur, Malaysia to schedule the interview.

Recruiting support contact Jane. After several interviews the hiring manager decides to hire Jane for the job. The offer information is sent to recruiting support in Kuala Lumpur, Malaysia to create and send the offer letter to Jane who lives in New Zealand.

Jane accepts the offer. John, from the U.S., checks the status of his referrals and sees that Jane has "accepted offer." Because Jane was an employee referral, recruiting support in Kuala Lumpur, Malaysia need to work with the U.S. recruiting team to arrange for payment of the employee referral bonus to John. U.S. recruiting

will work with their recruiting support in Bangalore, India to process the employee referral payment for John's referral hire into Sydney, Australia.

## About the Author

**Paul M. Schwartz** is Professor of Law at UC Berkeley School of Law. A leading international expert on informational privacy and information law, he has published widely on these topics.

In this country, his articles and essays have appeared in periodicals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, Columbia Law Review, Chicago Law Review, Michigan Law Review, and N.Y.U. Law Review. His co-authored books include the casebook INFORMATION PRIVACY LAW (3d ed. 2009), DATA PRIVACY LAW (1996), and DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES (1998), a study carried out for the Commission of the European Union that examined emerging issues in Internet privacy in four European countries.

Professor Schwartz has provided advice and testimony to numerous governmental bodies in the United States and Europe. During 2002-2003, he was in residence as a Berlin Prize Fellow at the American Academy in Berlin and as a Transatlantic Fellow at the German Marshall Fund in Brussels. He has also acted as an advisor to the Commission of the European Union on privacy issues and is a member of the American Law Institute.

Paul Schwartz is a graduate of Yale Law School, where he served as a senior editor of the Yale Law Journal. He received his undergraduate education at Brown University. More information about the author can be found at [www.paulschwartz.net](http://www.paulschwartz.net).

## **About The Privacy Projects**

The Privacy Projects is a non-profit research organization and think tank dedicated to enhancing the policies, practices, and technologies of personal information management. More information about the organization can be found at [theprivacyprojects.org](http://theprivacyprojects.org).