1-1-2006

# The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection

Horace E. Anderson
*Elisabeth Haub School of Law at Pace University*

VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW

VOLUME 9 FALL 2006 NUMBER 1

# The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection

*Horace E. Anderson, Jr.* *



"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[1]

- Samuel Warren and Louis D. Brandeis, 1890

* Associate Professor, Pace Law School. I would like to thank Mandy Tran and Paul Babchik for their able research assistance, and Don Doernberg, James Fishman, and Gayl Westerman for their insightful comments.

1. Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

"You have zero privacy anyway. Get over it."[2]
- Sun Microsystems CEO Scott McNealey, 1999

"Privacy" doctrine is currently one of the most high profile and most vexing areas of the law. Its recent prominence is due at least in part to the explosion of the Internet over the past decade[3] — a new wave of "recent inventions and business methods" to rival developments in the fields of photography and publishing in the time of Warren and Brandeis.[4] Its vexatious nature is due to the inconsistent comparisons that are sometimes drawn between the various flavors of privacy in the public discourse.

When we speak of privacy in the Internet age, a distinction needs to be drawn between what this article will refer to as "traditional privacy," the law of whether and to what extent the state can intrude in the private sphere of an individual[5], and "data protection" or "information privacy," the regulation of the use of personal information about individuals by non-state interests, such as corporations.[6] Unfortunately, much of the public discourse on the

---

2. *See* Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED NEWS, Jan. 26, 1999, http://www.wired.com/news/politics/0,1283,17538,00.html.

3. *See, e.g.*, Patricia Buckley, *Technology Consulting Forum: Electronic Commerce in the Digital Economy*, ACCOUNTING TODAY, July 26, 1999, *available at* 1999 WLNR 5561547.

4. Warren & Brandeis, *supra* note 1, at 195.

5. Examples of U.S. Federal legislation in this sphere include: the Privacy Act of 1974, 5 U.S.C. § 552 (2000) (regulating the collection, use, and transfer of personal information by federal government agencies); the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2000) (limiting access to, and release of, customer financial records by financial institutions); the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 (2000) (prohibiting interception and disclosure of certain electronic, wire, and oral communications); the Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2701-2711 (2000) (same). Additionally, and importantly, these rights are protected by the First, Fourth, and Fifth Amendments to the U.S. Constitution and the jurisprudence interpreting them. *See, e.g.*, McIntyre v. Ohio Election Comm'n, 514 U.S. 334 (1995) (finding First Amendment protection for the distribution of anonymous leaftlets); Katz v. United States, 389 U.S. 347 (1967) (finding that "the Fourth Amendment protects people, not places" and "what [a person] seeks to preserve as private, even in an area that is accessible to the public, may be constitutionally protected"); Griswold v. Connecticut, 381 U.S. 479 (1965) (invalidating a Connecticut law which prohibited the use of contraceptives as violative of the constitutional "right of privacy"); NAACP v. Alabama, 357 U.S. 449 (1958) (finding that an Alabama law which required the NAACP to produce a list of members' names and addresses violated the First Amendment's "freedom of association"). *But see, e.g.*, Whalen v. Roe, 429 U.S. 589 (1977) (finding that a New York law requiring the recording of personal information in connection with prescription drugs was not an unconstitutional exercise of state power).

6. In the area of information privacy, the federal government has enacted, for example: the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2000); the Health Insurance

subject of information privacy adopts a framework (and a concomitant set of expectations) more suitable to traditional privacy: an inviolable "right to be let alone" by the state.[7] As a number of commentators have recognized, the modern incarnation of privacy, rather than creating or reinforcing a sacrosanct right against the government, actually creates a quasi-property right, where personal data is a valuable commodity and access to it is negotiable.[8]

Given the negotiable nature of information privacy, concepts from economics in general, and game theory in particular, can be useful in framing and explaining the ways in which actors in our information privacy "system" actually conduct themselves *vis-à-vis* personal information. Scott McNealey's opinion notwithstanding,[9] individuals in today's society do have some measure of privacy protection. The potency of that protection ebbs and flows, depending in part on the strategic choices made by a number of individual and institutional actors, including the individual him- or herself.

This article briefly explores several scenarios in which economic actors compete and cooperate in order to capture the value in personal information. The focus then shifts to one particular scenario: the ongoing interaction between the United States and the European Union in attempting to construct data protection regimes that serve the philosophies and citizens of each jurisdiction as well as provide a strategic economic advantage. A game theoretic model is presented to explain the course of dealings between the two actors, including both unilateral and bilateral actions. Part I ends with an exploration of opportunities for seizing competitive advantage, and for fostering cooperative mutual advantage, through government action. Several likely equilibrium states are posited, and a single ultimate equilibrium is predicted.

Part I explores the literature on commodification and negotiability of information in order to explain the contextual nature of modern privacy and, further, introduces a number of the contexts

---

Portability and Accountability Act of 1996, 42 U.S.C. § 1320(d) (2000); the Children's Online Privacy Protection Act, 5 U.S.C. § 6501 (2000); and the Federal Financial Modernization Act (Gramm-Leach-Bliley Act), 15 U.S.C. § 6801 (2000).

7. *See, e.g.*, Susan Llewelyn Leach, *Privacy Lost With the Touch of a Keystroke?*, CHRISTIAN SCI. MONITOR, Nov. 10, 2004, at 15; William Safire, Editorial, *Medical Intrusiveness Puts Privacy Rights on the Ropes*, SAN MATEO COUNTY TIMES (Cal.), Mar. 11, 2004.

8. *See generally* Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899 (2003); Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 230 (2004); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996).

9. *See* Sprenger, *supra* note 2.

and actors among which information interactions take place. Then, Part II focuses on a single context and a single pair of actors, the United States and European Union. This part describes their divergent philosophies regarding data protection, the conflicting legislative results that have flowed from those philosophies and the attempts at "solving" the privacy conflict between these two actors via negotiation.

Part III expresses the U.S.-E.U. privacy conflict as an extensive form game, explains the history of interaction between the actors in terms of such game and assesses the current negotiated "solution." Finally, the article concludes with a consideration of the traditional game theoretic underpinnings of the alternative outcomes and assesses the likely stability of the equilibrium achieved.

## I. NEGOTIABILITY AND CONTEXTUALITY OF PRIVACY

### *A. Commodification and Negotiability of Information*

It is no secret that for many of the more developed participants in the global economy (including the United States), knowledge goods or information have supplanted manufactured goods as the main engine of commerce.[10] Increasingly, the "commodity production of knowledge" is the focus of advanced economies.[11] Even in the manufacturing sectors, the processing of information about the goods sold, and about those who purchase and use them, is as important as the production and shipping of the goods themselves.[12] In what has been called an "unprecedented proliferation of records and data," vast

10. By some estimates, "[a]s much as three-quarters of the value of publicly traded companies in America comes from intangible assets," leading Federal Reserve Chairman Alan Greenspan to deem America's economic output "predominantly conceptual." *See* Kenneth Cukier, *A Market for Ideas*, THE ECONOMIST, Oct. 22, 2005, at 67.

11. *See* Paula Baron, *Databases and the Commodification of Information*, 49 J. COPYR. SOC'Y U.S.A. 131 (2001).

12. One example of this development is the increased research by manufacturers into the use of Radio Frequency Identification ("RFID") technology to track the movement of consumer goods. A product embedded with an RFID tag can transmit information about when it leaves the factory, when it leaves the warehouse, when and where it is purchased at retail, and, in combination with credit card information collected at the point of purchase, by whom it is purchased at retail. Wal-Mart, the world's largest retailer, is in the midst of an initiative that, by the end of 2006, will require all of its suppliers to use RFID technology on products shipped to Wal-Mart and Sam's Club stores. *See, e.g.*, *Wal-Mart Expands RFID Mandate*, RFID JOURNAL, Aug. 18, 2003, *available at* www.rfidjournal.com/article/articleview/539/1/1/; Laurie Sullivan, *Wal-Mart Outlines RFID Expansion Plans*, INFO. WK., June 17, 2004, *available at* www.informationweek.com/story/showArticle.jhtml?articleID=22100511.

fields of information about people and their activities populate large and valuable databases.[13] In the modern information economy, even navigating ostensibly non-commercial activities may involve perusing databases for pertinent (and thus currently valuable) information. So, not only do we contribute information to commercial databases every time we buy a DVD online or use a frequent shopper card at the market, we also make use of information stored in databases when we search TiVo for the particulars of a favorite program or peruse a bus schedule.[14] Individuals are both producers and consumers of commodity information.

Although, as discussed above, personal information has become a valuable commodity, its value is not necessarily inherent at its most granular level. That is, a single piece of information (such as a last name), or information about a single individual, or even information about a single transaction involving an individual, may not be interesting or valuable in isolation. Personal information is actually the building block of a value-added asset, such as the sort of robust database of customer profiles and preferences that allows Amazon.com to provide "1-Click" ordering, Wish Lists, and product recommendations for its regular customers.[15] As with other valuable assets and their inputs, private actors vie to monetize, trade, and capture the value of information assets, including personal information. As with bananas or steel, states may seek to benefit from the trade in these valuable assets among private actors.

---

13. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394 (2001).

14. *See* Baron, *supra* note 11, at 135 (citing Andrew Oram, *The Sap and Syrup of the Information Age: Coping with Data Protection Laws*, at 1, http://www.oreilly.com/~andyo/professional/collection_law.htm (last visited Jan. 11, 2002)); Solove, *supra* note 13, at 1394.

15. Amazon's 1-Click ordering allows the user to accelerate the purchase process by storing credit card, billing address, and shipping address information in a customer profile. *See* Amazon.com, Ordering via 1-Click, http://www.amazon.com/gp/help/customer/display.html?nodeId=468480 (last visited Oct. 6, 2006). The order can be processed with the click of a single on-screen button. *Id.* Wish Lists allow users to store their shipping information along with a list of gifts that they would like to receive. *See* Amazon.com, Wish Lists, http://www.amazon.com/gp/help/customer/display.html?nodeId=897204 (last visited Oct. 6, 2006). The user's friends and family can then presumably be directed to amazon.com, where they purchase a desired item, which is shipped automatically, using the stored information. *Id.* Amazon provides its "Recommendations" service by examining a user's past purchases and past ratings of items. *See* Amazon.com, Recommendations, http://www.amazon.com/gp/help/customer/display.html?nodeId=13316081 (last visited Oct. 6, 2006). By comparing purchasing behavior of other users whose purchase history overlaps with that of the first user, the company recommends future items for consideration. *Id.*

Given information's status as a commodity that can be built into a valuable asset, characterizations of information privacy rights as stark and inviolable, especially as against private actors, seem incomplete at best. Actors in the marketplace for information assets, including individual data subjects, negotiate, sometimes overtly and sometimes tacitly, over access to personal information and its attendant value. Examples of these negotiations are legion. Consumers routinely provide personal financial data to financial services companies in exchange for credit, or at least a chance at credit (no mortgage applicant seriously expects to receive access to hundreds of thousands of dollars without providing reams of such personal information). Customers of consumer products companies provide their e-mail addresses in exchange for notification of a merchant's sales and special offers. Registered users of e-commerce sites such as Amazon.com register as a prerequisite to the company's collecting the type of purchase history data that makes product recommendations possible. Even outside the consumer context, individuals often provide personal data regarding previous employment (including salary and performance data), in exchange for an opportunity for new employment.

It is not the case that all uses of personal data smack of either Big Brother or pernicious spam. Many uses are a result of some give and take among participants in an information marketplace, who, given the structure of the modern economy, might be seen as inevitable dealers in information assets.[16] Without some dealing in data, search costs would be higher for both merchants and consumers, pricing would be less efficient, merchants would have less accurate portraits of their customers, and there might even be higher incidence of fraud.[17] Absent a negotiation over use of personal data, many on-line transactions could not occur at all.[18] Overall, the marketplace in personal information has been said to promote lower costs for businesses and for society as a whole.[19]

---

16. *See* Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. CHI. L. SCH. ROUNDTABLE 75, 79 (2002).

17. *Id.* at 80-81.

18. On many e-commerce sites, a customer must reveal an e-mail address in order to create a "paper" trail that allows for tracking of the order and notification of delivery date. Although some sites provide for alternative payment information, the bulk of e-commerce transactions require use of a credit card.

19. Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 86-87 (2002). *See also id.* at 106 (describing how information collection and credit reporting facilitate pooling of loans, increasing creditor liquidity and making more funds available to borrowers at lower cost).

This notion of negotiability of privacy is not without its problems. Imposing a negotiation framework on the privacy question implies arms-length dealings where the parties have information about, and are constrained by, for example, their respective costs, target prices, and reserve prices.[20] However, while the "price" of an individual's data may be readily apparent in some situations (in order to receive a confirmation/receipt, a consumer must provide an e-mail address), in many other situations it is far from obvious. The consumer may have no idea what price she should charge a merchant for her data and thus may have a difficult time receiving true "market value."[21]

Further, the "negotiation" may often be forced on the consumer. Think of the confirmation/receipt example given above. What if the consumer does not care about receiving a confirmation and does not want to hear from the merchant until the product is delivered? Requiring an e-mail address to complete the transaction forces the consumer into the information exchange. Finally, the collection of data by companies may impose an externality on the consumer: the company benefits from each collection, but does not bear much in the way of cost. Merchants may tend to over-collect personal information in many cases.[22] According to Daniel Solove, the explosion of the use of targeted marketing rather than mass marketing has led to data collection that "extends beyond information about the consumer's views of the product to information about the consumer herself, often including lifestyle details and even a full-scale psychological profile."[23]

As a practical matter, the negotiability of privacy will turn on issues of power and leverage. Solove uses Kafka's *The Trial* to conceptualize the privacy problem:

> Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process. This lack of control allows the trial to completely take over Joseph K.'s life. *The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life.[24]

---

20. The target price is the price at which each side would ideally like to conclude the transaction. The seller's reserve price is the minimum price that she will accept, and the buyer's reserve price is the maximum price that he will pay.

21. *See* Hahn & Layne-Farrar, *supra* note 19, at 103.

22. *See id.* at 102.

23. Solove, *supra* note 13, at 1404.

24. *Id.* at 1421.

The frustration described by Solove explains the periodic public outcry over a particular announced use or misuse of personal information,[25] as well as attempts by users of personal information to assuage that frustration. An example of such an attempt is the corporate website privacy policy.[26] Compounding the control issue is the question of who deserves control, or, rather, who deserves to capture the value associated with the information? Is the individual the sole architect of the value of the information? Or is the information formed in relationships with others and given value through the consolidation and categorization functions performed by advertisers and marketers?[27] Paula Baron characterizes the debate over privacy and the use of data as being "about the struggle for ownership in pure information."[28] The struggle may also be characterized as one for the

---

25. For example, in 2000, Internet advertising company DoubleClick stirred up controversy, and attracted the scrutiny of the New York State Attorney General and the Federal Trade Commission, when it announced plans to purchase a company called Abacus. *See* Jeri Clausing, *U.S. Investigating DoubleClick Over Privacy Concerns*, N.Y. TIMES, Feb. 16, 2000, *available at* http://www.nytimes.com/library/tech/00/02/cyber/articles/17doubleclick.html; *Crisis Control @ DoubleClick: FTC, Michigan & NY; Stock Takes a Hit*, PRIVACY TIMES, Feb. 18, 2000, *available at* http://www.privacytimes.com/NewWebstories/doubleclick_priv_2_23.htm. The acquisition would have led to the mingling of non-personally-identifiable information long collected by DoubleClick, and personally-identifiable information on many of the same individuals residing in Abacus's databases. Clausing, *supra*. At the time, DoubleClick's privacy policy promised users that the company would never merge information it collected in such a way as to identify an individual. *Id.* Faced with possible action by the FTC and by various states because of the inconsistency in its stated policy and its actions, DoubleClick abandoned the plan to merge the data. *See* Letter from Joel Winston, Acting Associate Director, Divison of Financial Practices, Bureau of Consumer Protection, Federal Trade Commission, to Christine Varney, Esq., Hogan & Hartson, Attorney for Double-Click, Inc. (Jan. 22, 2001), *available at* http://www.ftc.gov/os/closings/staff/doubleclick.pdf. In 1997, several database companies, including LEXIS-NEXIS, came under fire for providing their customers with database access to personal information about individuals, including Social Security numbers. *See* Timothy Burn, *Database Companies Agree to Police On-line Information on Net Users*, THE WASH. TIMES, June 11, 1997, at B12. In response to consumer complaints and the threat of legislative and regulatory action, LEXIS-NEXIS pulled much of the most sensitive information from its P-Track service. *Id.* Also in 1997, online portal Yahoo! discontinued its reverse telephone directory, which had allowed users to access the name and address of an individual by entering that person's telephone number. *See, e.g., Yahoo Pulls Phone Search*, CNET NEWS.COM, Jan. 3, 1997, http://news.com.com/Yahoo+pulls+phone+search/2100-1023_3-259291.html. The company cited e-mail complaints received from users as the reason for abandoning the service. *Id.*

26. Some commentators have criticized such policies as a meaningless exercise. *See* Solove, *supra* note 13 at 1451 (decrying privacy policies as "self-indulgent, making vague promises such as the fact that a company will be careful with data; that it will respect privacy; that privacy is its number one concern" and "phrased in a vague, self-aggrandizing manner to make the corporation look good").

27. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1113 (2002).

28. Baron, *supra* note 11, at 131.

economic/marketing value represented by personal information. As discussed further in Sections I.B and C, the struggle defined by Baron is ongoing and contextual, and it is advanced by a potential host of players beyond the individual and his bookseller.[29]

### *B. Contextuality of Privacy*

Because neither the negotiability of data privacy, nor the marketplace in which individuals negotiate for the value of their information, is inherently or entirely good or evil, examinations of information privacy rights should not be made in isolation. Rather, data privacy rights must be assessed in view of the circumstances surrounding the data transaction. Solove emphasizes that privacy should be viewed pragmatically, as a contextual and dynamic legal phenomenon, rooted in the "concrete, historical, and factual circumstances of life."[30] Privacy, and information privacy in particular, "is not reducible to a single set of neutral conditions that apply to all matters we deem private."[31] Rather than possessing a singular, immutable "universal value" across all contexts, privacy rights depend on their particular social context and the relative importance of the information practices comprising that context.[32]

If we are to deal with the privacy issues raised in the modern information environment, we must accept the contextual nature of privacy rights. If we are to navigate the contextual nature of privacy rights, we must recognize the limitations of traditional paradigms for analyzing those rights. Using the example of *U.S. West, Inc. v. Federal Communications Commission*, Solove points out that part of the difficulty experienced by courts adjudicating privacy cases is that they are conceptualizing issues regarding the modern collection and use of personal information by companies as if there is no difference between that context and that of any other privacy problem.[33] In *U.S. West*, the telecommunications carrier used First Amendment grounds to challenge FCC rules implementing consumer privacy provisions of the Telecommunications Act of 1996.[34] Using the *Central Hudson*

---

29. *See* discussion *infra* Parts I.B-C.

30. *See* Solove, *supra* note 27, at 1091.

31. *Id.* at 1092.

32. *Id.* at 1093.

33. *Id.* at 1152 (citing 182 F. 3d 1224 (10th Cir. 1999)).

34. 47 U.S.C. § 222, enacted as part of the Telecommunications Act of 1996, restricts use of, disclosure of, and access to Customer Proprietary Network Information, stating that:

intermediate scrutiny test, the Tenth Circuit held that the FCC's restriction on commercial speech did not directly and materially advance a substantial state interest.[35] In questioning the substantiality of the state's interest in protecting privacy, the court fell back on familiar and traditional ways of thinking about the harms that flow from inadequate privacy protection, specifically, the traditional tort paradigm.[36] The court was "fixated on a conception of privacy that views its invasion as a discrete harm, . . . where the individual is left with specific injuries that can be readily translated into damages . . ."[37] In an information environment where some uses of personal information may cause harm, and some may be harm-neutral (or even beneficial) to the individual, it is clear that the old paradigms will not fit all modern contexts.

Even Judge Richard Posner's economic conception of privacy as secrecy does not always neatly fit the economic reality of usage of personal data in the Information Age.[38] Although one way of looking at privacy is as the right to secrecy, or the right to "conceal discreditable facts,"[39] facts do not have to be discreditable for the individual to have an economic interest in concealing them. Selective disclosure of facts about oneself may be beneficial to the individual even if the facts are neutral. For example, my e-mail address or snail mail address are neutral pieces of information without regard to my virtue, trustworthiness, or sense of honor. Nevertheless, I might be selective about revealing this information to an interested party

---

> [e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

47 U.S.C. § 222(c)(1) (2000). The statute provides exceptions for, *inter alia,* billing, fraud prevention, and inbound telemarketing and administrative services. *See id.* § 222 (d). The challenged FCC rules required an "opt-in" approach to customer consent, in which a customer's prior express approval would have to be obtained before her information could be used for marketing purposes. *See* U.S. West, Inc. v. Fed. Commc'ns Comm'n, 182 F. 3d 1224, 1230 (10th Cir. 1999).

35. *U.S. West, Inc.*, 182 F. 3d at 1240.

36. *See id.* at 1235 (characterizing a "substantial" state interest in privacy as one where the state protects against infliction of "specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity").

37. Solove, *supra* note 27, at 1153.

38. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 40 (6th ed. 2003).

39. *Id*; *see also* Solove, *supra* note 27, at 1106.

unless I gain some advantage from the revelation. Will I receive discount coupons for giving my e-mail address to Old Navy? Will I receive advance notice of sales in exchange for allowing Macy's to mail me catalogs? If I cease to be interested in Amazon.com's book recommendations, can I remove my information from their active database at some future date? The facts and situations within which an actor within the information system chooses disclosure are varied and mutable. A mere pouring of new wine into old bottles will not suffice, and updated paradigms of how multiple actors (including individuals, companies, agents, administrative bodies, states, and supra-national organizations) actually treat personal information under various circumstances must be part of any privacy framework. It is necessary to bear in mind always the "context and contingency" of uses of personal information.[40]

### *C. Key Privacy Contexts, Characters, and Contours of Competition*

What then are the contexts with which we should be concerned in understanding how the value of information is apportioned in the modern privacy landscape? We may define these contexts in terms of a cast of characters vying to capture the value of the information, and also in terms of the structure of their struggle over that value. Often, the characters are paired in a binary struggle. For our purposes, we will consider the following characters, or types of actors within the privacy system: Individuals, Legitimate Businesses, Illegitimate Businesses, Domestic Governments and Foreign Governments. Individuals are just that, individuals who are either the subjects of the personal data in question, or interested in using the personal data of others. Legitimate Businesses are those businesses with which an Individual may have a relationship, or with whom an Individual would not categorically reject having a relationship in the future. Illegitimate Businesses are those who would like to use an Individual's data, but whom the Individual would reject as inappropriately risky users of that data. A Domestic Government is the government of the state where an Individual or Business is domiciled, and a Foreign Government is the government of any other state.

The first pairing of interest in the competition over the value of personal information is that of the Individual vs. the Domestic Government. This is the first type of privacy scenario many people think about when they think about privacy, especially the

40. Solove, *supra* note 27, at 1127.

"traditional" privacy mentioned earlier in this article.[41] Although this pairing is typically discussed in terms of civil liberties, individual rights, or constitutional rights,[42] it may also be viewed through an economic lens. In many situations in which a government may seek information about an individual, the information has value, and each actor may be characterized as trying to capture or retain the value of that information. Think of the example of police surveillance of a criminal organization. The identity and movement patterns of the boss of the organization would be of great value to the state in seeking to prosecute him as the head of a criminal enterprise and to dismantle his gang. Information about meetings and conversations with known perpetrators of crimes would similarly be valuable to the state and its law-abiding citizenry. The boss and the members of his organization, however, derive great value from limiting the disclosure of such information. If the information can be kept from the police, the boss can continue to lend his acumen to the enterprise, and the organization can continue to reap illegal profits. Each side will take steps to secure the value of the information for its own "account," including use of video and audio surveillance, informants, and undercover operatives on one side, and use of code words and intermediaries on the other.

A second pairing of competitors for the value in personal information involves an Individual versus a Legitimate Business. This is the classic case of a company coming into possession of a person's information legitimately and seeking to make a marketing use of such information. The information may be valuable because it allows the marketer to understand the customer better, and leads to further sales to a particular Individual. An example of this type of value is the value of collecting and keeping purchase history information about a customer in order to make purchase recommendations to that same customer in the future. The Business also may derive value from the information by combining it with information about other customers. This allows the Business to recognize macro trends in the purchasing behavior of its entire customer base or of relevant segments. The Individual attempts to capture or reserve the value of her personal information by withholding certain information from the Business or by extracting

41. *See* introduction *supra* pp. 2-3.

42. Examples of this view are: the right of the Individual not to have his telephone conversations monitored and/or recorded, the right not to be compelled by the state to reveal political or interest group affiliation, and the right to make certain personal decisions, such as the decision to use contraception, without state scrutiny or interference.

some benefit in exchange for the information. In the latter circumstance, even though the Individual extracts a benefit, it is often the Business that sets the terms of the exchange and makes the offer. For example, a Business may give a discount (or ongoing discounts) in exchange for an application for a store credit card or membership card. The Individual would also like to retain the value in her information by compelling the Business to offer an additional benefit for each use, for each new use, or for each request for additional information. For example, the Individual would like to receive a discount for signing up for a credit card, but there is no necessity for an e-mail address to be included in the information requested on the application. In exchange for providing an e-mail address, the Individual may want some ongoing benefit, such as periodic "members only" sales or previews.

Of more concern to the Individual is her competition with Illegitimate Businesses for the value in her personal information. For our purposes, an Illegitimate Business is one that may have acquired the personal information without the knowledge of the Individual and that the Individual would likely reject as a holder or user of her information. The classic case of this pairing is unsolicited commercial e-mail, or spam. The Illegitimate Business seeks to capture the value of the information (often, in the spam context, e-mail addresses) by adding it to bulk e-mail mailing lists. With very large bulk e-mail lists, the cost of sending each e-mail message is infinitesimal.[43] As the size of a bulk e-mail list grows, the probability of the Illegitimate Business receiving a positive response, and a potential sale, increases. Even though response rates to bulk marketing (including bulk mail and bulk e-mail) are extremely low,[44] expansion of the mailing list allows the Illegitimate Business to apply its low response percentage to a larger base. Meanwhile, the probability that the Individual wants to actually receive a solicitation from an Illegitimate Business is also extremely low.[45] It is in the Individual's interest not to have her information revealed to the Illegitimate Business at all, and she "wins" the competition and retains the value of her information when the information remains unknown to the Illegitimate Business. She

43. *See* Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 364 (2000).

44. By some estimates, bulk mail response rates are as low as 0.6%, and bulk e-mail response rates are similarly less than 1%. *See* Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77, 90-91 (2003).

45. *See* Fisher, *supra* note 43, at 365 (describing public complaints regarding spam received by the Federal Trade Commission and Securities Exchange Commission, and public calls for limits on electronic junk mail).

may also score a limited win when she has the ability to spot and ignore, or filter out, e-mail messages from the Illegitimate Business, minimizing the costs imposed upon her and her e-mail service provider by the Illegitimate Business.[46] In the United States, the Domestic Government has entered this competition on the side of the Individual, passing the CAN-SPAM Act in 2003, and requiring, among other things, that advertising e-mails be labeled as such, that header information and subject lines not be misleading or deceptive, and that recipients be given the choice to opt out of receiving future e-mail messages from the sender.[47] While measures such as CAN-SPAM are applicable to those Illegitimate Businesses that are domiciled domestically, they provide no aid to the Individual struggling against a foreign Illegitimate Business that is beyond the jurisdiction of the Domestic Government.[48]

The Individual does not struggle only against organizations or companies over the value of her information. Other Individuals seek to capture the value of the personal data as well. Identity theft is an example of this privacy context.[49] 'The Identity Thief who is able to learn the right type of personal information about the data subject (name, address, telephone, Social Security number, credit card account numbers, etc.) can derive benefits from posing as the Data Subject. The Identity Thief can present himself as a creditworthy person with a stable well-paying job, and therefore qualify for a large one-time purchase, a consumer credit account, or even a loan. Of course, because the Thief is merely posing as a creditworthy individual, he does not care about maintaining that creditworthiness. He has incentives to default on whatever obligations he "assumes" while wearing his new identity. Such inattention to maintaining the status of the Data Subject ultimately leads to losses for the Data Subject.[50] The Data Subject's main options for retaining the value of

---

46. The costs of spam are particularly irksome to Individuals, because such costs are almost completely externalized by the sender. *See* Ayres & Funk, *supra* note 44, at 136. The marginal cost to the Illegitimate Business will tend toward zero. *Id.*

47. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2719 (codified at 15 U.S.C. § 7701 (Supp. III 2003)).

48. Generally, only bulk e-mail senders that are subject to the jurisdiction of the Federal Trade Commission or certain other federal regulators such as the Securities Exchange Commission or Federal Communications Commission will have the CAN-SPAM Act enforced against them. *See* 15 U.S.C. § 7706(b) (Supp. III 2003).

49. Identity theft is "the illegal use of someone else's personal information . . . in order to obtain money or credit." *See* Meriam Webster Online Dictionary, Identity Theft, http://www.m-w.com/dictionary/identity%20theft (last visited Nov. 4, 2006).

50. The Federal Trade Commission has reported that nearly 10 million Americans were victims of identity theft in 2003, resulting in losses of approximately $5 billion. *Do*

her information are being judicious about sharing of the information with others and policing her credit reports for evidence that her information has been misappropriated.

Finally, the competition over the value in an Individual's information (or, more accurately, the information of many Individuals), may be played out between two States. Commodification of personal data allows such data to be treated like other commodities in some ways. Information may become an object of the trade strategy and goals of a state or multi-state trade alliance. Protection of the privacy rights of its citizens, or preservation of the value of that information for domestic users, may become part of a government's foreign policy. As such, the potential advantage inherent in valuable information may cause a State to enact new laws, vigorously enforce existing ones, seek to influence the lawmaking of its trading partners, reward its friends, and punish its rivals.[51] As this article will establish in Section II, information policy can be used to reinforce the cohesion of a trade alliance.[52] Section II explores the relationship between two governments, the supranational government of the European Union and the national government of the United States, with regard to information privacy policy.[53] As with the other contexts previously discussed in this Section, the essence of the relationship is a contextual and ongoing negotiation and competition over the value in the personal information of Individuals.[54]

---

*You Know Where Your Identity Is? Personal Data Theft Eludes Easy Remedies*, KNOWLEDGE@WHARTON, Apr. 20, 2005, http://knowledge.wharton.upenn.edu/index.cfm?fa=printArticle&ID=1176. The companies that did business with identity thieves (by selling them goods and services, and/or extending them credit), lost upwards of $47.6 billion on such transactions. *Id.*

51. For example, the European Union is viewed by many as heavily impacting commercial regulation beyond its borders, particularly in the areas of consumer protection, software, and technology, telecommunications, and data privacy. *See, e.g.*, Brandon Mitchener, *Standard Bearers: Increasingly, Rules of Global Economy Are Set in Brussels --- To Farmers and Manufacturers, Satisfying EU Regulators Becomes a Crucial Concern --- From Corn to SUV 'Bull Bars'*, WALL ST. J., Apr. 23, 2002, at A1.

52. *See* discussion *infra* Part II.

53. *Id.*

54. *See* discussion *supra* Part I.

## II. THE UNITED STATES, THE EUROPEAN UNION, AND THE STATE VS. STATE CONTEXT

### *A. Divergent Philosophies*

The United States and the nations of the European Union have traditionally held starkly different positions on data privacy, including the appropriateness of government regulation of the collection and use of personal information by the private sector.[55] The essence of these differences can be understood by appreciating how each jurisdiction might answer two basic questions. First, to what extent is government regulation perceived as an effective and desirable way to provide for the needs of individuals? Second, to what extent is data privacy (as against private actors) considered a fundamental right of individuals? The contrasting philosophies of the two jurisdictions[56] set the stage for the dissimilar privacy approaches and outcomes that occur in practice.

Data protection in the European Union countries can be characterized as adhering to a philosophy of a high degree of government involvement in the protection of a fundamental right.[57] Stephen Kobrin has described the European approach to privacy as "put[ting] the burden of protection on society rather than the individual."[58] Others have noted that

> [g]overnment on the European continent is perceived ... more as the protector of individual needs, rather than an entity who interferes with those needs. Europe is more comfortable with a socialist approach where government protects an individual's liberties, basic needs such as food and shelter, and continuing rights to employment.[59]

Still others have gone as far as to call the European privacy model a "command and control model with precise rules governing the handling of personal information."[60] James Whitman mines the

---

55. *See infra* text accompanying notes 58 & 61.

56. *Id.*

57. *See* Alexander Zinser, *The Safe Harbor Solution: Is It An Effective Mechanism For International Data Transfers Between The United States And The European Union?*, 1 OKLA. J. L. & TECH 11 (2004), http://www.okjolt.org/articles/2004okjoltrev11.cfm.

58. Stephen J. Kobrin, *Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, 30 REV. INT'L STUD. 111, 116 (2004) (contrasting the European approach with the American approach to privacy, which emphasizes individual ownership and control over, and alienability of, personal information).

59. Carl Felsenfeld, *Unnecessary Privacy*, 25 SUFFOLK TRANSNAT'L L. REV. 365, 370 (2002).

60. Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law For Europe and America*, 5 J. HIGH TECH. L. 13, 60 (2005).

European historical and cultural context to declare that European privacy is ultimately most concerned with human dignity, and thus "avidly" protects a wide range of types of privacy in many areas of day-to-day life.[61] The E.U. Data Protection Directive made clear the approach expected of its Member States when it declared that "data-processing systems are designed to serve man" and must "respect their fundamental rights and freedoms, notably the right to privacy."[62]

By contrast, privacy law in the United States is generally concerned with upholding privacy rights against the government.[63] "At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home."[64] Regarding private actors, the information privacy philosophy of the United States, at least for most of the nation's history, is most often characterized as a market-based or largely *laissez-faire* type of approach.[65] In this view, privacy rights are property-like; they are alienable, tradable, and waivable.[66] Such an approach is consistent with Whitman's argument that American notions of privacy are grounded in liberty, rather than dignity.[67] The most important thing is to protect the individual from state intrusion into the choices she

---

61. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1156-58 (2004) (describing European protection in the areas of "consumer data, credit reporting, workplace privacy, discovery in civil litigation, the dissemination of nude images on the Internet, [and] shielding criminal offenders from public exposure" (internal citations omitted), and further describing underpinnings of European privacy culture in the European Convention on Human Rights).

62. Council Directive 95/46, pmbl. ¶ 2, The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC) [hereinafter Council Directive 95/46].

63. Kobrin, *supra* note 58, at 115; *see also* Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1228 (2000) (citing examples from traditional American definitions of privacy, such as freedom from government searches, and freedom from government interference in individual decision-making).

64. Whitman, *supra* note 61, at 1161 (citing Jeffrey Rosen, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 5 (2000)).

65. *See, e.g.*, Steve Lohr, *Seizing the Initiative on Privacy: Online Industry Presses its Case for Self-Regulation*, N.Y. TIMES, Oct. 11, 1999, at C1 (describing concerns raised by the Federal Trade Commission regarding efficacy of the traditional U.S. self-regulatory model of data protection).

66. *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, at 1246-49 (1998); Murphy, *supra* note 8, at 2402.

67. Whitman, *supra* note 61, at 1162-64. Whitman describes American anxieties about privacy as being concerned with "maintaining a kind of private sovereignty within our own walls." *Id.* at 1162. In his conception of comparative U.S.-E.U. privacy, "American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity." *Id.* at 1163.

makes regarding her personal information. Self-regulation by private users of personal information is the American ethos, with government stepping in to fill gaps reactively, and narrowly.[68] Preserving both individual autonomy and commercial flexibility has traditionally been paramount, and industry has historically been trusted to police itself, particularly where such self-policing would support continued growth and development of the Internet.[69] The Clinton Administration's Framework for Global Electronic Commerce, one of the early and few comprehensive federal government statements on Internet privacy issues, enumerated encouragement of self-regulation and government restraint as two of its core principles.[70]

### *B. Conflicting Legislative Results*

Not surprisingly, the legislative regimes of the two jurisdictions in question evolved in markedly different directions.[71] The laws of the United States regarding data protection have justifiably been called a "legal patchwork,"[72] "fragmented,"[73] a "discordant morass,"[74] "reactive,"[75] "a crazy quilt of piecemeal statutes,"[76] "sporadic,"[77] and "inchoate."[78] Although Congress has considered a number of bills in this area,[79] there is to date no

---

68. *See* Zinsner, *supra* note 57, ¶ 3 (characterizing U.S. policymaking as "reactive," and favoring targeted solutions to privacy problems).

69. *See, e.g.*, Lohr, *supra* note 65. *See generally* FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf; Chris J. Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment* (Electronic Privacy Information Center, Wash., D.C.), Mar. 4, 2005, http://www.epic.org/reports/decadedisappoint.html.

70. *See* Felsenfeld, *supra* note 59, at 365-66; A Framework for Global Electronic Commerce, The White House (July 1, 1997), http://www.technology.gov/digeconomy/framewrk.htm.

71. *Compare* text accompanying notes 72-78 *with* text accompanying notes 92-97.

72. *See, e.g.*, Zittrain, *supra* note 63, at 1229.

73. *See, e.g.*, Gregory Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29, 61 (2002).

74. Stephen J. Davidson & Daniel M. Bryant, *The Right of Privacy: International Discord and the Interface with Intellectual Property Law*, COMPUTER & INTERNET LAW. Nov. 2001, at 1, 1.

75. *See* Kobrin, *supra* note 58, at 117; Zinsner, *supra* note 57, ¶ 3 (quoting William J. Long & Marc Peng Quek, *Personal Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, 9 J.EUR. PUB. POL'Y 325, 332 (2002)).

76. Rustad & Koenig, *supra* note 60, at 39.

77. Kobrin, *supra* note 58, at 117.

78. *Id.*

79. Recent attempts have included the proposed Personal Data Privacy and Protection Security Act of 2005, S. 1789, 109th Cong. (2005); the proposed Online Privacy

comprehensive federal information privacy statute. Instead, there are sector specific laws designed to address specific types and uses of personal information.[80] As a matter of national statutory law, the United States protects, for example, financial information,[81] information about children,[82] health-related information,[83] information contained in credit reports,[84] video rental information,[85] and certain information regarding cable television subscribers.[86] Unless a piece of personal information fits within one of the above types, it is likely not covered by any specific federal statute. Some protection has been provided by the role played by the Federal Trade Commission ("FTC") in protecting against unfair trade practices. The FTC is authorized to investigate "the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce . . ."[87] More specifically, the FTC Act authorizes the FTC to pursue complaints of "unfair or deceptive acts or practices in or affecting commerce," including deceptive practices relating to the collection and use of personal data.[88] Additionally, protection against certain specific and intrusive uses has been provided by recent federal action in the areas of SPAM[89] and unwanted telemarketing calls.[90] By and large, however, most of the immense amount of data collected by private interests in the United States slips through the statutory cracks.[91]

---

Protection Act of 2005, H.R. 84, 109th Cong. (2005); and the proposed Consumer Privacy Protection Act of 2005, H.R. 1263, 109th Cong. (2005).

80. *See* sources cited *infra* notes 81-86.

81. *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2000).

82. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2000).

83. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of the U.S. Code).

84. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2000).

85. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000).

86. *See* Telecommunications Act of 1996, 47 U.S.C. § 222(c) (2000).

87. 15 U.S.C. § 46(a) (2000). Banks, savings & loan institutions, credit unions, and common carriers are excepted from this authority. *Id.*

88. *Id.* § 45(a)(1).

89. *See* Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2719 (codified at 15 U.S.C. § 7701 (Supp. III 2003)).

90. FTC Telemarketing Sales Rule (the Federal "Do-Not-Call" Registry), 16 CFR § 310.1-9 (2006).

91. Some states, notably California, have moved to fill the gaps left by federal statutes, but this Article is concerned with statutory action at the national level. *See* Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575-79 (Deering 2003).

Meanwhile, information privacy protection in the European Union has long been the subject of comprehensive legislative action.[92] Beginning in the 1970's, several countries developed national laws regulating the processing of data about individuals, including collection, use, and storage.[93] These laws, although emanating from a shared understanding of individual rights, did not provide a uniform level of protection.[94] In an effort to harmonize the differences among national laws and facilitate the free flow of data across intra-Union borders, the then-fifteen Member States of the E.U. put into effect Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("E.U. Directive").[95] The E.U. Directive prescribes specific requirements for the handling (or "processing") of personal data, defined as "any information relating to an identified or identifiable natural person."[96] An "identifiable person" (the "data subject" of the personal data) is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[97]

"Processing" of personal data is defined broadly to mean "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[98] The E.U. Directive covers the processing activities of both "data controllers" (those who determine the purposes of, and means for, processing),[99] and "data processors" (those who actually process the data on behalf of a controller).[100] The Member States of the European Union are required to adopt national laws consistent

---

92. *See infra* notes 93-96.

93. *See* European Commission, Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited Nov. 4, 2006) (listing legislation in various countries, including France's 1978 Act on Data Processing, Data Files and Individual Liberties, and Ireland's Data Protection Act 1988).

94. See generally statutes listed in *id.* that preceded Council Directive 95/46/EC.

95. *See* Council Directive 95/46, *supra* note 62.

96. *Id.* art. 2(a).

97. *Id.*

98. *Id.* art. 2(b).

99. *Id.* art. 2(d).

100. *Id.* art. 2(e).

with the E.U. Directive.[101] Those national laws are required to apply where the processing activities of a data controller take place in the territory of a Member State, where a Member State's national law applies by virtue of international public law, or where a data controller makes use of equipment situated within the territory of a Member State.[102]

The E.U. Directive requires that the laws enacted by Member States provide for adherence to certain principles in the processing of personal data.[103] Personal data must be processed fairly and in a manner consistent with specified, explicit and legitimate purposes, maintained accurately, updated periodically, erased or rectified in a timely manner, and kept anonymously when identification of data subjects is no longer necessary.[104] Member States must provide in their national laws that personal data may only be processed where:

> (a) the data subject has unambiguously given his consent; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).[105]

Certain categories of data receive an even higher level of protection under the E.U. Directive.[106] Data about race, ethnicity, political or religious affiliation, health, sex life, or union membership may not be processed, subject to an explicit consent exception, and certain other narrow exceptions.[107]

---

101. *Id.* art. 4(1).
102. *Id.*
103. *See id.* art. 6.
104. *Id.*
105. *Id.* art. 7.
106. *See id* art. 8.
107. *Id.*

Data controllers must give notice to data subjects of, among other things, their own status as data controllers, the purpose of the processing, the identities of the recipients of the data, and the fact that the data subject has a right of access and correction.[108] The access right, provided by Article 12 of the E.U. Directive, requires Member States to guarantee that data subjects may obtain from the data controller information regarding the processing of the data subject's information, including the categories of data being processed, the purpose of the processing, the source of the data, and the logic by which the data is being processed.[109] Article 12 also provides that data may be rectified, erased, or blocked if its processing does not comply with the provisions of the E.U. Directive.[110] Article 14 grants further objection rights to the data subject, allowing prohibition of use of data where the data subject articulates "compelling legitimate grounds," and enabling the data subject to object to the use of his personal data for direct marketing purposes.[111] Data subjects also have the right not to be subject to decisions about them that are arrived at via automated processing rather than human decision-making.[112]

Data controllers face additional requirements and constraints under the E.U. Directive. Data security measures must provide (or require from its data processors) an "appropriate" level of protection against destruction, loss, unauthorized alteration, or unauthorized disclosure.[113] The appropriateness of security measures is to be determined with reference to the state of the art regarding data security.[114] Any processing involving retention of a data processor must be governed by contract wherein the processor agrees to act only on instructions from the controller, and also assumes the data security responsibilities that bind the controller.[115] Generally, the data controller must also notify the data protection authority ("DPA") of the relevant Member State before carrying out a data processing operation that is automatic in nature, either in whole or in part.[116] All Member States of the union were required by the E.U. Directive to

---

108. *Id.* art. 10-11.
109. *Id.* art. 12(a).
110. *Id.* art. 12(c)
111. *Id.* art. 14.
112. *Id.* art. 15.
113. *Id.* art. 17(1).
114. *Id.*
115. *Id.* art. 17(3).
116. *Id.* art. 18(1).

enact implementing legislation bringing their national laws into harmony with the Directive's requirements by October 1998.[117]

### C. The Tie That Binds

The E.U. Directive certainly establishes a comprehensive regime, one that might even seem stifling to an individual or company used to a more American information privacy ethos. But why exactly did the European Union's subjecting itself to a hyper-stringent set of data privacy practices gore America's ox? The answer is twofold. First, the value of trade between the United States and the European Union is enormous. In 2003, the total value of trade with the fifteen nations that made up the European Union when the E.U. Directive was adopted was over $400 billion.[118] By one estimate, inclusion of transactions between affiliates in the trade calculation would bring the value of U.S.-E.U. trade to $1.7 trillion.[119] As the European Union continues to expand, the value of transactions between the two jurisdictions can be expected to continue to grow as well.[120] Much of the commercial traffic between the United States and the European Union is accompanied by, or consists of, streams of data. Sales of goods (for example, the purchase of a pair of customized athletic shoes by a French teenager from an American multinational[121]) may involve the collection of information from and/or about a customer. Online

---

117. *Id.* art. 32. As of this writing, all Member States had enacted legislation seeking to comply with the Directive. *See* Status of Implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited Oct. 10, 2006).

118. *See* U.S. Census Bureau, Trade with European Union: 2003, http://www.census.gov/foreign-trade/balance/c0011.html#2003 (last visited Oct. 10, 2006). Total trade for the first five months of 2005 with the 25 nations of the recently expanded Union was $202 billion. *See* U.S. Census Bureau, Trade with European Union: 2005, http://www.census.gov/foreign-trade/balance/c0003.html#2005 (last visited Oct. 10, 2006).

119. *See* Shaffer, *supra* note 73, at 30 (citing *Transatlantic Governance in Historical and Theoretical Perspective*, *in* TRANSATLANTIC GOVERNANCE IN THE GLOBAL ECONOMY 3, 4 (Mark Pollack & Gregory Shaffer eds., 2001)).

120. The European Union currently consists of 25 Member States: Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. *See* European Union Member States, http://europa.eu/abc/governments/index_en.htm (last visited Nov. 4, 2006). An additional five nations (Bulgaria, Croatia, Romania, the Former Yugoslav Republic of Macedonia, and Turkey) are currently candidate countries. *Id.*

121. See, for example, NikeID.com, Nike's online customization store, http://nikeid.nike.com/nikeid/index.jhtml?ref=www.nike.com#home (last visited Oct. 10, 2006).

purchases of services or technology goods (such as software) similarly involve exchanges of information.

Secondly, the E.U. Directive creates the possibility that the streams of information alluded to above might come to a halt.[122] Article 25 requires the Member States to allow transfers of personal data to countries outside of the European Union "only if ... the third country in question ensures an adequate level of protection."[123] "Adequacy" is to be assessed based upon a number of factors, including:

> the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[124]

A finding of inadequacy requires a Member State to take steps to prevent transfers to a given third country.[125] A third country may enter into negotiations with the European Commission in order to rectify the situation, and may achieve adequacy via its domestic law or its international commitments.[126] Article 26 provides a number of derogations from, or exceptions to, Article 25's prohibition on transfers to countries with inadequate privacy protection.[127] Among these are unambiguous consent of the data subject, necessity of the transfer for performance or completion of a contract, protection of the vital interests of the data subject, and necessity to the public interest.[128] Additionally, a data controller may make certain guarantees regarding protection of privacy rights in order to gain approval from a Member State's DPA for a particular data transfer or set of transfers.[129]

As a practical matter, the derogations do not provide much relief for a company located in an "inadequate" country that wishes to import data from a European Union Member State. Obtaining unambiguous consent from every data subject that is part of a high volume of online transactions can be nearly impossible.[130] The

---

122. *See* Council Directive 95/46, *supra* note 62, art. 25(1).
123. *Id.*
124. *Id.* art. 25(2).
125. *Id.* art. 25(4).
126. *Id.* art. 25(5)–(6).
127. *Id.* art. 26(1).
128. *Id.*
129. *Id.* art. 26(2).
130. *See* Rose Barcelo, *Seeking Suitable Options for Importing Data from the European Union*, 36 INT'L LAW. 985, 995 (2002).

European Commission's interpretation of what constitutes a "necessary" transfer is extremely narrow and renders the necessity-based derogations of little use to most data controllers.[131] The practical limitations of Article 26 and the stark prohibitions of Article 25 have resonance with U.S.-based companies because the United States was not at the time of the E.U. Directive's adoption, nor is it currently, deemed to provide adequate protection to personal data.[132] Without some sort of accommodation on either side, American multinationals faced the prospect of not being able to move crucial information (including transactional data, marketing profiles, and employee records) from the European countries where they were collected to the United States divisions in which their value would be realized.

### *D. A Negotiated Solution*

The prospect of a catastrophic cessation of data flows from Europe prompted the United States Department of Commerce to enter into bilateral negotiations with the European Commission, with the goal of finding a data protection solution that would pass muster as "adequate" by European Union standards without excessively burdening U.S.-based multinationals.[133] The result was Safe Harbor, a self-certification program that allows participating U.S. firms to be deemed adequate protectors of personal data, as far as the Member States of the European Union are concerned. Data transfers from all Member States to Safe Harbor companies are allowed to continue without prior approval from the DPAs of the Member States.[134]

---

131. *See id.* at 996.

132. To date, the following non-Member States have been declared by the European Commission to provide adequate protection to personal data, for purposes of Article 25: Switzerland (Commission Decision 2000/518, 2000 O.J. (L 215) 1); Canada (Commission Decision 2002/2, 2001 O.J. (L 2) 13); Argentina (Commission Decision 2003/490, 2003 O.J. (L 168)); Guernsey (Commission Decision, 2003/821, 2003 O.J. (L 308) 27); and the Isle of Man (Commission Decision, 2004/411, 2004 O.J. (L 151) 1). *See* Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm (last visited Oct. 10, 2006).

133. *See* Kobrin, *supra* note 58, at 113.

134. *See* U.S. Department of Commerce, Safe Harbor Overview, http://export.gov/safeharbor/sh_overview.html (last visited Oct. 10, 2006); *see also* Commission Decision Pursuant to Directive 95/46/EC on the Adequacy of Safe Harbor Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, http://www.export.gov/safeharbor/DecisionSECGEN-EN.htm (last visited Nov. 4, 2006) (assuring that additional guarantees are not necessary for Safe Harbor companies).

Participating companies join Safe Harbor by annually certifying to the Department of Commerce that they are in compliance with seven Safe Harbor Principles.[135] They must also state in their published privacy statements that they adhere to the principles.[136] A firm may achieve the promised adherence by "(1) join[ing] a self-regulatory privacy program that adheres to the safe harbor's requirements; or (2) develop[ing] its own self regulatory privacy policy that conforms to the safe harbor."[137] The Department of Commerce maintains a list of companies that have self-certified.[138]

The seven Safe Harbor Principles are: Notice, Choice, Onward Transfer, Access, Security, Data Integrity, and Enforcement.[139] In essence, the principles require that a firm notify data subjects about the purpose for the collection and use of their information and that the data subject be able to choose whether the data will be used for any other purpose or disclosed to a third party. In order to disclose data to a third party (Onward Transfer), the firm must comply with the Notice and Choice principles.[140] Data subjects must have access to their data and be reasonably able to correct, amend, or delete their information.[141] Firms must take reasonable steps to provide effective data security and data integrity, and they must provide procedures and mechanisms for handling data subjects' complaints and disputes regarding the handling of their data.[142]

Participation in Safe Harbor is currently open to organizations that are subject to the regulatory authority of the FTC or the United States Department of Transportation.[143] Both agencies have indicated via letters to the European Commission that they will take action against Safe Harbor companies who do not meet their obligations under the program.[144] Under Section 5 of the FTC Act, along with the terms of the Safe Harbor program, participants who fail to provide adequate protection may be subject to an FTC action for engaging in

---

135. *See* Shaffer, *supra* note 73, at 62.

136. *See* U.S. Department of Commerce, Safe Harbor Overview, *supra* note 134.

137. *Id.*

138. The Department of Commerce Safe Harbor list may be found at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

139. *See* U.S. Department of Commerce, Safe Harbor Overview, *supra* note 134.

140. *Id.*

141. *See id.*

142. For a more detailed treatment of the Safe Harbor Principles, see *id.*

143. *Id.* This means that companies in certain industries, including much of the financial services sector, is unable to participate in Safe Harbor, and thus have not resolved their issues regarding Article 25 of the Data Protection Directive.

144. *See id.*

"unfair or deceptive acts or practices in or affecting commerce."[145] A delinquent Safe Harbor firm may find itself subject to administrative orders, penalties of up to $12,000 per day, and removal from the Safe Harbor list.[146]

Safe Harbor has received mixed reviews. To some, it represents a successful compromise that may contribute to "a gradual convergence in data privacy practices."[147] To others, Safe Harbor means that both Americans and Europeans find themselves "subject to a privacy regime that is not of their making and certainly does not reflect their common interests."[148] Participation levels have not been overwhelming. As of September 2006, approximately 1014 companies were current in their certification status with the Safe Harbor program.[149] This represents a fairly small percentage of U.S. companies in total. Of the current Safe Harbor companies, only 60 are members of the Fortune 500.[150] Presumably, companies of that size and global reach were the types of companies for whom Safe Harbor was designed in the first place. The European Commission has voiced disappointment in the number of registered Safe Harbor organizations,[151] but has also noted the absence of complaints from data subjects as one indication that those companies that are registered are mainly in compliance.[152] Of greater concern to the European Commission is the fact that few Safe Harbor companies have incorporated the Safe Harbor Principles into their written privacy policies to the Commission's satisfaction, and the Commission seeks a more proactive compliance effort from the Department of

145. 15 U.S.C. § 45(a)(1) (2000).

146. *See* U.S. Department of Commerce, Safe Harbor Overview, *supra* note 134.

147. Shaffer, *supra* note 73, at 66.

148. *See* Kobrin, *supra* note 58, at 128.

149. *See* U.S. Department of Commerce, Safe Harbor List, *supra* note 138.

150. *Compare Fortune 500 2006: Our Annual Ranking of America's Largest. Corporations*, FORTUNE, Apr. 17, 2006, at F1-F20, *available at* http://money.cnn.com/magazines/fortune/fortune500/full_list/, *with* U.S. Department of Commerce, Safe Harbor List, *supra* note 138.

151. The Commission is even considering analyzing the market share of Safe Harbor companies as a way of measuring whether the program is likely having a significant impact on data practices. Commission of the European Communities, Commission Staff Working Document, *The Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce*, 5, SEC (2004) 1323 (Oct. 20, 2004), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf [hereinafter *Implementation of Commission Decision 520/2000/EC*].

152. *Id.* at 6.

Commerce and the FTC.[153] How did the European Union and the United States get to the current state of play regarding data privacy, and to what extent have they addressed their privacy issues? More importantly, where do they go from here in terms of their relationship *vis-à-vis* privacy? Part III examines and assesses the interaction of the United States and the European Union using concepts from game theory and attempts to chart a course for a more satisfactory outcome.

## III. SETTING THE MODEL

The utility of game theoretic models to analyze problems of law and policy is well established.[154] Scholars have used game theory analysis to model competitive behavior with respect to valuable intangible assets, such as intellectual property.[155] They have also long used game theory to better understand and predict the actions of states in the areas of international law and international trade.[156] The State vs. State context of the data privacy game presents a competition among nations to capture or retain the value of intangible information and may be modeled separately from either the IP or the international trade games.

One potentially useful game theory model for examining the State vs. State context is the normal form game, a 2x2 competition/cooperation matrix, the most familiar flavor of which is the Prisoner's Dilemma.[157] In the normal form game, the players move simultaneously, each choosing a strategy without knowledge of the course of action chosen by the other player (although each player may know a good deal of information about other aspects of their

153. *See id.* at 7-8.

154. *See generally* Martin Shubik, *Game Theory, Law, and the Concept of Competition*, 60 U. CIN. L. REV. 285, 297-303 (1991) (citing game theory applications in collective bargaining, antitrust, contracts, sales, property law, industrial organizations, and agency theory, and relating legal applications of game theory to cross-purposes optimization).

155. *See, e.g.*, David W. Leebron, *A Game Theoretic Approach to the Regulation of Foreign Direct Investment and the Multinational Corporation*, 60 U. CIN. L. REV. 305, 316-18 (1991) (modeling foreign direct investment decisions, including technology transfer); Ruth L. Okediji, *Public Welfare and the Role of the WTO: Reconsidering the TRIPS Agreement*, 17 EMORY INT'L L. REV. 819, 852-72 (2003) (analyzing negotiation of the Agreement on Trade-Related Aspects of Intellectual Property, or TRIPS Agreement).

156. *See, e.g.*, Mark A. Chinen, *Game Theory and Customary International Law: A Response to Professors Goldsmith and Posner*, 23 MICH. J. INT'L L. 143 (2001), Brett Frischmann, *A Dynamic Institutional Theory of International Law*, 51 BUFF. L. REV. 679 (2003).

157. *See* Shubik, *supra* note 154, at 288-90.

playing environment).[158] The players face a binary choice of strategies, promising different payoffs for each player depending upon which of the two available strategies she chooses, and which of two strategies is adopted by her co-player.[159] In a game of complete but imperfect information, a common variant, the players know their own available strategies and payoffs, as well as the available strategies and payoffs of their co-player.[160] As noted above, however, a player does not know which strategy her co-player will actually choose.[161] Payoffs are often represented, and will be represented here, as dollar amounts gained or lost by the players.

A number of assumptions are necessary in creating the model and situating the players therein. The United States faces a choice between regulating uses and transfers of personal data or permitting such uses and transfers to occur without interference (the choice will be represented in the model as Regulate/Don't Regulate). Regulation entails direct dollar costs in the form of creation and maintenance of an administrative and/or judicial apparatus to enforce the regulatory regime. The decision to regulate also reduces U.S. revenues from commercial uses of personal data. A scheme that regulates data flows may lead to certain transactions being halted that would otherwise be completed. Such a scheme may also slow down transactions that would otherwise be completed on a timelier basis. Fewer transactions may be completed by U.S. firms, and those firms' revenues can be expected to decrease over time. Delays in completing those transactions that do succeed will also cost the firms revenue. For the United States as a player in the game, the decrease in the revenue of U.S. firms can be represented as an aggregate loss by all U.S. firms, or as a loss of tax revenues for the United States as a state (such tax revenue loss amounting to a percentage of the aggregate loss by the firms).

The European Union faces a choice between permitting data use and transfers by foreign firms on a fairly *laissez faire* basis, or restricting such activity (represented in the model as Allow/Restrict). Restriction entails a direct cost, just as regulation does for the United States. However, we assume the European Union's marginal cost to be lower than the United States' cost, due to a more developed pre-existing infrastructure for the regulation of commercial transactions,

158. *See* DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW 6-7 (1994).
159. *See id.* at 8.
160. *Id.* at 9-10.
161. *Id.* at 10.

including data transactions.[162] A decision by the European Union to Restrict reduces United States revenues, potentially by a larger amount than that caused by a United States decision to Regulate (due to, for example, less concern on the part of E.U. regulators for revenue effects of their activities on foreign firms than U.S. regulators would likely demonstrate for their own domestic firms). If the European Union decides to Allow, it faces a number of costs, some of which are more quantifiable than others. There will, of course, be political costs for a government that is seen as failing to protect what its constituents hold to be a fundamental right. There may even be an increase in direct litigation costs, as citizens either sue E.U. Member States for failing to protect their rights or make increased use of administrative and judicial apparatuses in enforcing rights against private actors (whose data use and transfer activities are likely to increase under an "Allow" regime).

Even more important from a strategic perspective is the question of what costs in the way of lost revenues the European Union might incur by deciding to Allow. If the European Union Restricts, more transactions that would otherwise have been completed between E.U. consumers and U.S. merchants will instead be completed between E.U. consumers and E.U. firms. Therefore, by Allowing, the European Union creates the possibility for the United States to capture more of the value of the personal data of E.U. consumers. This value is made up of the raw value of transactions with E.U. consumers, plus whatever multiplier effect operates on future transactions.[163] The value-capture issue forces the European Union, when making the Allow/Restrict decision, to consider the global reach of U.S. firms, the relatively aggressive marketing culture of U.S. business, and the general orientation among U.S. firms toward maximizing the use of, and return on, personal data as an investment in the growth of the company.

In the model, for convenience, we assume that the value of the personal data of E.U. consumers is 100. The United States faces a cost to Regulate of 20. The European Union maintains a baseline cost of regulation of 10, reflecting a more highly regulated economy in general than that of the United States. If the European Union chooses to Restrict, it incurs an additional cost of 10. If the United

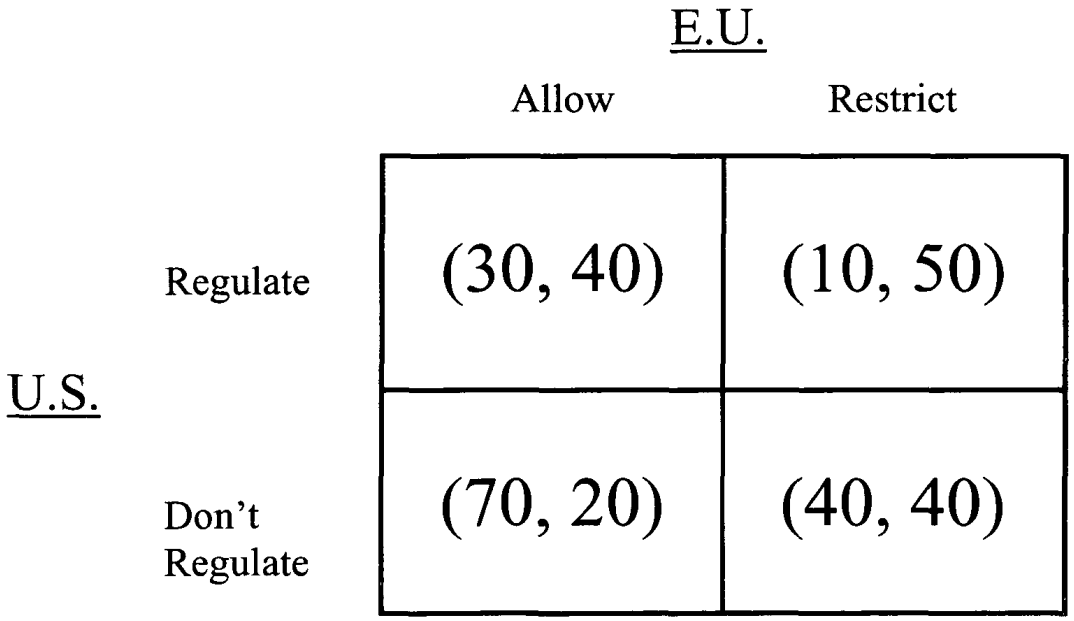
---

162. *See* discussion *supra* Part II.A.

163. For example, maintaining a robust database of customer identifying data, preferences, and purchase history may lead to more transactions in the future with existing customers than if no such data is kept. Additionally, more new customers may be marketed to, and transacted with in the future, if consumer data can be collected and transferred to a central marketing department for analysis.

States declines to Regulate, while the European Union chooses to Allow, the United States captures 70% of the value of the personal data, with the European Union capturing 30% (less its baseline regulatory costs of 10, for a net payoff of 20). If the United States declines to regulate while the European Union Restricts, the United States captures 40% of the value, while the European Union receives 60% (less regulation costs of 10 and costs to Restrict of 10, resulting in a net payoff of 40). If the United States Regulates while the European Union Allows, each captures half the value of the data, less their respective regulation costs (20 in the case of the United States, and 10 in the case of the European Union). If the United States Regulates while the European Union Restricts, the United States earns 30% of the value, less regulation costs of 20 (for a payoff of 10), while the European Union captures 70% of the value, less baseline regulation costs and costs to Restrict (for a net payoff of 70 minus 20, or 50). The matrix and each party's payoffs appear as below[164]:

Figure 1: Normal Form Game Between U.S. and E.U.




164. In each pair of payoffs, the U.S. payoff is listed first, and the E.U. payoff second.

A strictly dominant strategy for the United States under this model is non-Regulation.[165] Regardless of whether the European Union decides to Allow or Restrict, the United States is better off choosing not to Regulate (earning a payoff of 70 versus 30 in the event of an Allow strategy by the European Union, and earning a payoff of 40 versus 10 in the event of a Restrict strategy by the European Union). Given the dominance of the Don't Regulate strategy for the United States, the European Union, acting rationally, will be forced to pursue a Restrict strategy. As the European Union expects the United States to choose Don't Regulate, it is better off choosing Restrict (and earning 40), rather than Allow (earning 20).

Although the game as set forth above reaches equilibrium, it does not necessarily produce an optimal or even desirable result. The United States ends up capturing less value than it otherwise would, and processing fewer transactions with E.U. consumers. This is obviously a poor result for the United States, but it is also problematic for those E.U. consumers who *want* to transact with U.S. firms. There are transactions for which U.S. firms might be better suited, either because E.U. firms do not provide the goods/services involved, or because U.S. firms can provide the goods/services more cheaply or efficiently. The inability of such transactions to be consummated represents a loss to the system in the form of potential value left uncaptured by anyone. Additionally, there may be some appetite among U.S. consumers for *some* regulation of U.S. firms.[166] An outcome that essentially means zero regulation by the United States of its firms is an unfavorable one for U.S. consumers.

Beyond the suboptimality of the result, the model as defined so far does not quite capture or predict the actual outcome of the game as "played" in the real world. The United States and the European Union forged a solution to their data privacy dilemma that provided not only more than the zero regulation regime anticipated by the normal form game, but also less than the predicted draconian restrictions on data usage.[167] The predictive shortcoming of the normal form game here is because it does not adequately capture the structure of the relationship between the players. Unlike the motorist and pedestrian

---

165. A strictly dominant strategy is one that is always the best choice for a particular player, regardless of the strategy chosen by the other player. *See* BAIRD ET AL., *supra* note 158, at 11.

166. The vigorous nature of the debate over privacy issues in the U.S., and the advocacy activities of organizations such as the Electronic Privacy Information Center, the Electronic Frontier Foundation, and the Coalition Against Unsolicited Commercial Email, provide strong evidence of such a phenomenon.

167. *See* discussion *supra* Part II.D regarding the U.S.-E.U. Safe Harbor Program.

often used to illustrate tort applications of the normal form game,[168] the United States and the European Union do not each make a single decision regarding data protection with no idea of what move will be the opponent will make. Instead, the players here make a series of moves as part of an ongoing, recurring set of trade actions. Rather than being simultaneous, as in the normal form game, the players' interaction is dynamic and iterative. A party may make a move in one round of play with an eye toward the effect of that move on future rounds. Each party uses its opponent's early round moves to inform strategy for later rounds. Thus, a more robust tool for analyzing the U.S.-E.U. data competition is the extensive form game, which provides the players an opportunity to assess and re-calculate strategy over the course of repeated interactions.

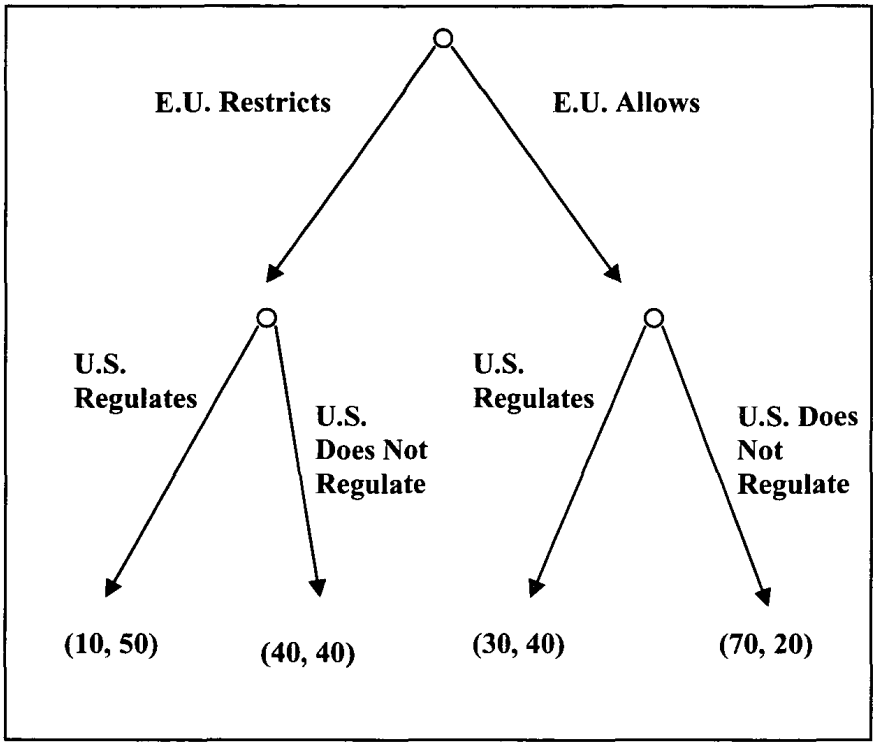
The extensive form game models multiple rounds of actions taken by the players, the sequence in which actions are taken, and the information and options available to the players during each round.[169] Despite its usefulness in iterative interactions, however, it is possible to use the extensive form game to model an interaction between the United States and the European Union that does little more than replicate the results of the normal form game. For example, in the Figure 2 below, with the United States moving first, backwards induction indicates that the outcome will be Don't Regulate/Restrict. Moving last, and faced with the indicated choices, the European Union will choose Restrict over Allow in the event of a decision by the United States to Regulate (earning 50 rather than 40, as in the normal form model above), and it will also choose Restrict over Allow in the event of a decision by the United States not to Regulate (earning 40 over 20, as in the normal form model above).[170] In determining its first move, the United States will take into account that the European Union's only rational strategy in the second round is Restrict. Therefore, in order to secure a payoff of 40 rather than 10, the United States will choose Don't Regulate.

168. *See, e.g.*, A. MITCHELL POLINSKY, AN INTRODUCTION TO LAW AND ECONOMICS 43-46 (3d ed. 2003) (citing generally John Prather Brown, *Toward an Economic Theory of Liability*, 2 J. LEGAL STUD. 323 (1973)).

169. *See generally* Shubik, *supra* note 154, at 286-88 (describing the game tree used in extensive form game models).

170. By convention, in each pair of payoffs, the payoff of the first mover (in this case the U.S.) is listed first.

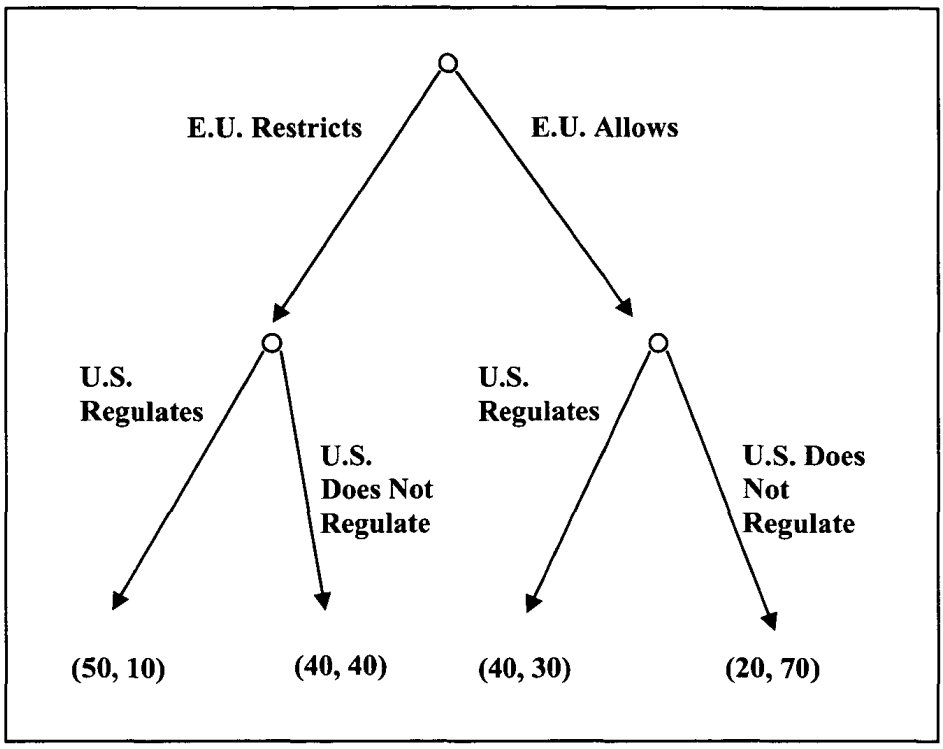
Figure 2: Extensive Form Game with U.S. as First Mover




Under the current set of payoffs, the outcome is no different if the E.U. is the first mover (see Figure 3 below). Moving last, the U.S. will choose Don't Regulate as its more lucrative strategy in the case of both possible moves by the E.U.. Don't Regulate nets the U.S. a payoff of 70 over 30 in the event of an Allow decision, and a payoff of 40 over 10 if the E.U. has chosen Restrict. Knowing the decision set faced by the U.S. in the last move, the E.U. will choose Restrict in the first move, in order to earn 40 rather than 20.[171]

171. By convention, in each pair of payoffs, the payoff of the first mover (in this case the E.U.) is listed first.

Figure 3: Extensive Form Game with E.U. as First Mover




To demonstrate more accurately the impact of iterative play in the U.S.-E.U. data protection game, we must make adjustments to the model. The revised model introduces an additional round of play, with the European Union playing first. The European Union chooses strategy, the United States follows, and then the European Union receives a final play.[172] Along with the additional round, there are adjustments to the parties' payoffs, due in part to an additional strategy available to the European Union: Halt.

A number of additional assumptions are necessary in analyzing the revised model with the Halt strategy available to the European Union. First, adopting the Halt strategy imposes a significant cost on the European Union. For purposes of the model, employing the Halt strategy means ceasing all data transfers from the European Union to the United States. It is obvious that such a move would heavily and negatively impact U.S. payoffs, but the strategy is not without pain for the European Union. The Halt strategy would necessitate more rigorous (and expensive) enforcement in order to ensure that no

172. It should be noted that, although we posit three rounds of play here, the model may also be framed as having up to *n* rounds, with *n* being an odd number. The E.U. makes the first and *n*th moves, and every odd-numbered move in between.

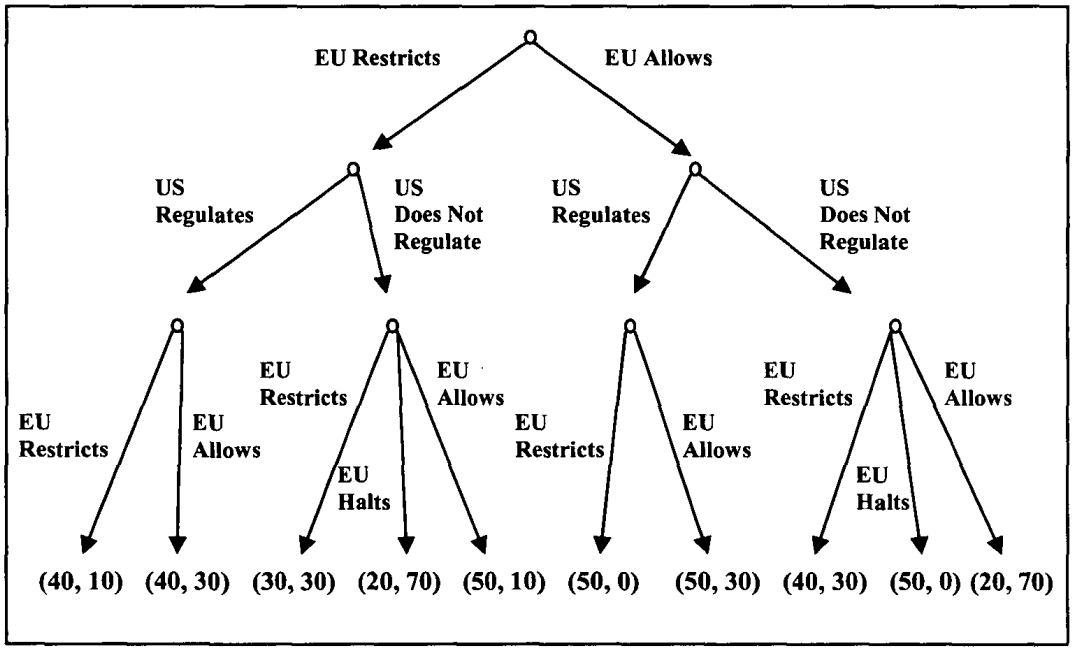
personal information is transferred to the United States; such enforcement costs can be expected to reduce the net amount of any payoff to the European Union from the game. Additionally, collaborative opportunities between U.S. firms and E.U. firms would be lost almost completely under the Halt strategy. Without the ability to share data about customers by transferring data files to U.S. joint venture partners, for example, E.U. firms will be less able to strategically exploit the value of their information by forming marketing alliances across the Atlantic. Finally, some of the data controllers seeking to move data from the European Union to the United States are E.U. firms, or at least E.U. divisions of U.S. firms. Such firms or divisions may employ E.U. citizens locally and pay taxes to E.U. Member States. Cessation of data flows would impact the revenues of these local players, and reduce the wages and taxes that they would typically pay in the European Union.

Given the costs of the Halt strategy to the European Union, it will not employ the strategy lightly. If during any round the United States chooses Regulate as its strategy, the European Union can be expected not to pursue the Halt strategy during its turn. If the United States chooses Don't Regulate, however, it can expect the European Union to choose Halt in the next round, leading to a zero payoff for the United States. We also assume that the cost to Restrict is cumulative; if the European Union incurs such cost in multiple rounds, then the total cost to Restrict will be a multiple of the base restriction cost of 10. For example, if the European Union initially Restricts, and then Restricts again after the United States moves, its additional cost to Restrict will be 20 rather than the 10 incurred when the Restrict strategy is chosen (only once) in the normal form game. Therefore, the payoff to the European Union will be reduced by 10, in the event that the players pursue a Restrict-Regulate-Restrict chain of strategies.

Other payoffs are similarly affected by the iterative nature of the game, and the particular sequence in which moves play out. If the United States Regulates in response to a Restrict decision by the European Union, the payoff to the United States is reduced by 10. This result reflects increased costs caused by the adjustment on the part of U.S. businesses to the practical limitations of the E.U. restrictions coupled with the legal burdens of a new U.S. regulatory scheme. If the European Union Allows initially, and then Allows again following a play by the United States of Regulate, it gains incremental revenue (its persistently permissive environment acting cumulatively and providing space for more E.U.-involved transactions to occur) and sees a +10 change in its payoff over the Allow-Regulate pairing of the normal form game.

The players' payoffs thus emerge as follows: If the parties pursue Restrict-Regulate-Restrict, the European Union earns 40 and the United States earns 10, while if they pursue Restrict-Regulate-Allow, the European Union earns 40 and the United States earns 30. A choice by the United States not to Regulate following a decision by the European Union to Restrict leads to a 30-30 split in payoffs if the European Union Restricts again, a payoff of 50 for the European Union with a zero payoff for the United States if the European Union Halts, and a payoff of E.U. = 20 and U.S. = 70 if the European Union Allows on its second turn. If the players pursue Allow-Regulate-Restrict, the European Union earns 50 and the United States earns 10, while if they pursue Allow-Regulate-Allow, the European Union earns 50 and the United States earns 30. Meanwhile, a choice by the United States not to Regulate following a European Union decision to Allow leads to a payoff of E.U. = 40 and U.S. = 30 if the European Union Restricts, a payoff of 50 for the European Union with a zero payoff for the United States if the European Union Halts, and a payoff of E.U. = 20 and U.S. = 70 if the European Union Allows again on its second turn. These payoffs are illustrated in Figure 4 below.

Figure 4: Extended Form Game Including E.U. "Halt" Strategy




We can predict that the United States will not pursue any strategy that would present the European Union with a Restrict/Halt/Allow set of strategy choices. When presented with such

a choice, the European Union will always choose Halt, opting to receive a payoff of 50 rather than 30 (in the case of a Restrict-Don't Regulate-Restrict progression of play), 20 (in the case of either Restrict-Don't Regulate-Allow or Allow-Don't Regulate-Allow), or 40 (Allow-Don't Regulate-Restrict). The only way to avoid the European Union's choosing the Halt strategy (and consigning the United States to a payoff of 0) is for the United States *not* to choose Don't Regulate. Because the United States will not elect a strategy that presents the Halt option to the European Union, the branches of the tree that include a Don't Regulate choice by the United States can effectively be removed. Only the Restrict-Regulate-Restrict, Restrict-Regulate-Allow, Allow-Regulate-Restrict, and Allow-Regulate-Allow progressions are viable. Both progressions that begin with Allow provide higher payoffs for the European Union than the progressions that begin with Restrict (50 versus 40). Intuitively, this makes sense, as the two Allow progressions provide more of an opportunity to avoid cumulative enforcement costs associated with the Restrict strategy over multiple rounds of play. As between the two remaining outcomes that result from an Allow-first strategy, the European Union is indifferent, as either will yield a payoff of 50.

If, after an Allow-Regulate set of moves by the players, the European Union is indifferent between Allow and Restrict, how did the players arrive at the current state of affairs, Safe Harbor (a regime of mild regulation by the United States) and an Allow choice by the European Union? One explanation involves each player communicating important information to the other in advance of, or even simultaneously with, its actual moves in the game. First, the European Union communicates to the United States a credible threat to reduce its payoff from data transfers to zero. The framework constructed by the E.U. Directive supports this threat by requiring Member States to take steps to discontinue the flow of data to states not deemed adequate protectors of personal information.[173] In any round where such a strategy is available to the European Union, it rationally adopts that strategy because of the opportunity for a superior payoff. Knowing this fact, and respecting the threat, the United States has an incentive to avoid the "Halt" choice presenting itself in any given round of play. Thus, the United States is pushed toward the adoption of some kind of Regulate strategy.

Once the United States chooses the Regulate strategy, there is still the question of whether the European Union will choose Restrict or Allow (each of which offers the same E.U. payoff). The United

173. *See* Council Directive 95/46, *supra* note 62, art. 25.

States has an incentive to attempt to induce an outcome that produces a higher U.S. payoff (Allow, rather than Restrict). One way to do this might be to communicate a commitment to protecting personal information, such as by making an *a priori* promise to Regulate, albeit mildly. The European Union might cooperate with such a move by the United States (by Allowing rather than Restricting on its second and later turns) because the certainty of some regulation by the United States is better than the uncertainty of the game without the U.S. commitment. It is also possible that preserving other aspects of the trade relationship between the players is worth choosing a strategy that makes the rival better off, especially when it can be done without making the mover worse off. By allowing the United States to communicate some commitment to privacy and to implement some mild form of regulation, Safe Harbor and the Allow-Regulate-Allow progression that it represents, a Pareto superior outcome is presented to the Allow-Regulate-Restrict progression that might otherwise unfold.[174]

So which player has "won," or is winning, this version of the data privacy game? The short answer is the United States. Although it has been persuaded to adopt a form of a Regulate strategy, such regulation is relatively mild. The Safe Harbor regime does not reach the level of comprehensiveness of the privacy protection systems in European Union nations, and seems to preserve elements of the historical American *laissez-faire* approach. For example, rather than U.S. companies being subject to blanket rules, the Safe Harbor regime allows a subset of those companies to "opt in" to a privacy-protective mode of operation. Arguably, this would be a self-selecting group of firms that consider privacy protection important, and large numbers of firms that should be the object of regulation will escape scrutiny. The companies set their own specific rules, via their privacy policies, although they must align such rules with the Safe Harbor principles. Further, members of Safe Harbor largely self-report their progress in achieving privacy goals,[175] and they have the option to have privacy

174. *See e.g.*, POSNER, *supra* note 38, at 12-13 (explaining that a transaction or allocation of resources is Pareto Superior to another if it makes at least one participant better off without making any participant worse off, and that a Pareto optimal state of affairs is one where any reallocation of resources would only increase the wealth of one party at the expense of another).

175. *See* U.S. Department of Commerce, Final Safe Harbor Documents: Frequently Asked Question 6, http://export.gov/safeharbor/FAQ6SelfCertFinal.htm (last visited Nov. 4, 2006).

disputes settled privately.[176] Other nations that have earned the "adequate" designation from the European Union have had to create much more pervasive and comprehensive systems in order to do so.[177]

The European Union's own assessment of the game illustrates the degree to which the United States has been able to implement a "Regulate Lite" system. The Commission Staff Working Document on the implementation of Safe Harbor (the "E.U. Safe Harbor Report"), required by Decision 520/2000/EC,[178] reports that, although there has been steady growth in the number of Safe Harbor companies, the absolute number of companies signed up for the program is still small, and the market share represented by such companies has not been analyzed.[179] Therefore, the actual impact of the program on the marketplace may be slight. Further, the privacy performance of members of the program has yet to be audited by U.S. regulators, and it is unclear at best whether any of the members' privacy policies undergo regulatory scrutiny.[180] The E.U. Safe Harbor Report expresses concern with the effectiveness of attempts by Safe Harbor companies to translate the Safe Harbor principles into written (and posted) privacy policies, and proposes a more proactive posture on the part of the Department of Commerce and the FTC in policing these issues.[181] The issues raised by the E.U. Safe Harbor Report are indicative of a regime that is still functioning in a largely self-regulatory manner, with mild government oversight, rather than the all-encompassing regulation that could have been.

The game's outcome is not a pure victory for the United States however, nor is it a pure loss for the European Union. Although the Commission notes that there have been no comprehensive audits of compliance with Safe Harbor principles, it also notes that it has

---

176. U.S. Department of Commerce, Final Safe Harbor Documents: Frequently Asked Question 11 http://export.gov/safeharbor/FAQ11FINAL.htm (last visited Nov. 4, 2006).

177. For example, Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") is broad-based, applying with certain exceptions to "every organization in respect of personal information (a) that the organization collects, uses or discloses in the course of commercial activities; or (b) is about an employee of the organization. . . ." Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 (Can.). PIPEDA imposes specific affirmative obligations on collection, use, disclosure, access, notice, and the like. *Id.*

178. Decision 520/2000/EC requires the Commission to assess Safe Harbor three years after its announcement and evaluate whether the system is providing adequate protection. *See Implementation of Commission Decision 520/2000/EC, supra* note 151, at 3.

179. *Id.* at 5.

180. *Id.* at 6.

181. *See id.* at 7-8.

received no complaints from data subjects.[182] The number of Safe Harbor complaints referred to alternative dispute resolution ("ADR") organizations such as TRUSTe, the Direct Marketing Association, BBBOnline, and the American Arbitration Association, has been "insignificant," such that the Commission does not have enough of a sample to evaluate fully the privacy decisions of the program's ADR providers.[183]

It may be that, from the perspective of the European data subject, U.S. data usage under Safe Harbor has not been objectionable, or at least not sufficiently objectionable for the harm done to outweigh the transaction costs of invoking the complaint system. And despite the issues raised in the E.U. Safe Harbor Report, the Commission finds that the U.S. Department of Commerce is generally "carrying out its role in accordance with the Safe Harbour requirements."[184] Additionally, there is much anecdotal evidence that U.S. firms are becoming more thoughtful about their data protection posture and policies. A proliferation of written (and posted) privacy policies, the installation of executive level hires with titles like Chief Privacy Officer, and the institution by some companies of data privacy audits are a few examples of this trend. [185] Even though the result here can be counted as a U.S. win, it certainly presents an outcome much more favorable to the European Union than that which would result from total U.S. non-cooperation.

The U.S.-E.U. outcome contains elements of two types of game settings recognized in the game theory literature. The data privacy competition is related to both cooperation games, where the players mutually benefit from cooperating, but only repeated play discourages defection, and coordination games, where "each state's best move depends on the move of the other state."[186] The keys to bringing about a semblance of a "win-win" outcome, as in many iterative interactions, are mutual concern for the future, an expectation that the players will encounter each other again, and the capacity for a player to punish the other in some future period.[187] When these keys are present, iteration can lead to more cooperative behavior than defecting

182. *Id.* at 6.

183. *Id.* at 11.

184. *Id.* at 13.

185. *See, e.g.*, Claudia Rowe, *In Business; Keeping it Confidential*, N.Y. TIMES, Mar. 3, 2002, § 14WC, at 3; John Schwartz, *The Nation: Surveillance 101; Privacy vs. Security on Campus*, N.Y. TIMES, Aug. 4, 2002, § 4, at 3.

186. Chinen, *supra* note 156, at 148-49 (quoting Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113 (1999)).

187. *See id.* at 167.

behavior, and to more jointly beneficial outcomes.[188] The trade relationship between the United States and the European Union (especially as regards personal information) fits the classic criteria for this sort of result. The volume and connectedness of their mutual trade make the two parties extremely important partners to each other, and their interactions can be expected to continue into future periods without end. Further, the capacity for punishment carries particular potency in the data arena, given the pervasiveness and importance of data as both a commodity itself, and as a vital component of trade in all other commodities.[189]

Game theory also predicts the structural and institutional underpinnings of the U.S.-E.U. data privacy result. Where several possible equilibriums exist, focal points can be essential to bringing about a particular, jointly beneficial one. A focal point is "anything that tends to focus the players' attention on one particular equilibrium, in a way that is commonly recognized, tends to make this the equilibrium that the players will expect and thus actually implement."[190] Communication is a means for creating focal points; therefore treaties, or similar agreements, can serve as focal points in interactions between states. Cooperative moves that would lead to high joint payoffs can be recorded in an agreement to inform parties as they consider their moves during the life of the agreement and to set a minimum behavioral benchmark.[191] In the case of the U.S.-E.U. data privacy competition, the E.U. Directive, as an agreement among the E.U. Member States, and the Safe Harbor program (including the reporting mechanism of the Working Party), as an agreement between the European Union and the United States, serve the focal point function by focusing the players on strategy choices, and therefore equilibriums, that involve some level of regulation by the United States in order to avoid possible outcomes that might invoke a cessation of data flows from the European Union to the United States.

Establishment of institutions can also engender cooperative strategies such as those employed by the players in the current game. Jointly created institutions, such as Safe Harbor, can be used as a method for implementing cooperative strategies. Their joint nature increases the likelihood that the players will not only cooperate

---

188. *See* Michael Whincop, *The Recognition Scene: Game Theoretic Issues in the Recognition of Foreign Judgments*, 23 MELB. U. L. REV. 416, 419 (1999) (citing ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984)).

189. *See* discussion *supra* at Part I.A.

190. Chinen, *supra* note 156, at 153 (quoting ROGER B. MEYERSON, GAME THEORY: ANALYSIS OF CONFLICT 371 (1991)).

191. *See* Goldsmith & Posner, *supra* note 186, at 1171.

initially, but will cooperate in a continued manner over time.[192] Like agreements, institutions can also serve to minimize uncertainty and transaction costs associated with dynamic playing environments.[193] Where the underlying assumptions and setting are subject to evolution, institutions can be used to adjust payoffs and commitments in an orderly and mutually beneficial manner, with minimal harm to the relationship between the players.[194] Given the dynamic nature of the U.S.-E.U. data collection and usage environment, and the vital nature of the trade, creation of institutions such as Safe Harbor is entirely predictable based on a careful application of game theory concepts in this space.

## IV. CONCLUSION

What is the future of the U.S.-E.U. data privacy game? Have the players reached an equilibrium that is stable in addition to being mutually beneficial? What changes can be expected in the relationship between the players, and in their views regarding the strategies available to them in the ongoing competition? How will the parties seek either to seize further advantage, or to protect gains under the current equilibrium? Of course, none of the answers to the above questions can be predicted with certainty, but the play of the game thus far and the levers used by the parties to arrive at the current state of the world provide some guidance. The parties have used communication and institutions to create focal points and reduce uncertainty. Communication of a credible threat to halt data flows, and the existence of a supranational institution to facilitate carrying out the threat, led to the adoption of a mild form of regulation by the United States, rather than no regulation at all. The Safe Harbor program itself represents an institution that sets baseline expectations for acceptable strategy choices in the ongoing game, and also provides communication opportunities.

The European Union continues to signal, via the E.U. Safe Harbor Report, that certain U.S. strategy choices (more proactive oversight, audits of Safe Harbor companies by regulators, analysis of Website privacy policies) are more conducive to continuation of the mutually favorable current equilibrium than others. The European Union also continues to signal that "the E.U. panel and data protection authorities should invite organizations that subscribe to the

192. Frischmann, *supra* note 156, at 719.
193. *Id.* at 683.
194. *Id.*

Principles to effectively comply with the Principles and use their power to suspend data flows if they conclude that there is a substantial likelihood that the Principles are being violated."[195] Cessation of data flows is still an option, and both players understand that. The institutional anchors and communication devices that have been put in place in this game can be expected to preserve the core gains (to the European Union as a player, to the United States as a player, and to their respective data subjects) of the current equilibrium, while slowly introducing more substance to the "Regulate Lite" strategy. The individual European citizen will not be completely let alone, but her data privacy rights with respect to United States actors will certainly exceed zero.

195. *Implementation of Commission Decision 520/2000/EC*, *supra* note 151, at 8.