DRAFT

The Privacy Gambit

Toward a Game Theoretic Approach to International Data Protection

Horace Anderson[a1]

"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

"You have zero privacy anyway. Get over it."[2]

- Sun Microsystems CEO Scott McNealey, 1999

I. Introduction

"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

---

[a1] 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 and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[2] *See* Polly Sprenger, *Sun on Privacy: Get Over It*, Wire News, January 26, 1999.

[3] S*ee, e.g.,* Patricia Buckley, *Technology Consulting Forum: Electronic Commerce in the Digital Economy,* 7/26/99 ACCOUNTING TODAY 9920802, at 1999 WLNR 5561547.

[4] Warren and Brandeis, *supra* note 1.

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 I will call "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 subject 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

---

[5] Examples of US Federal legislation in this sphere include the Privacy Act of 1974, 5 U.S.C. § 552 (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 (limiting access to, and release of, customer financial records by financial institutions); and the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 and §§ 2701-2709 (prohibiting interception and disclosure of certain electronic, wire, and oral communications. 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.,* Katz v. United States, 389 U.S. 347 (1967); McIntyre v. Ohio Election Comm'n, 514 U.S. 334 (1995); Griswold v. Connecticut, 318 U.S. 479 (1965); Whalen v. Roe, 433 U.S. 425 (1977); NAACP v. Alabama, 357 U.S. 449 (1958).

[6] In the area of information privacy, the Federal government has enacted, for example, the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 et seq.; the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d; the Children's Online Privacy Protection Act of 1998, 5 U.S.C. § 6501 et seq.; and the Financial Modernization Act of 1999, 15 U.S.C. § 1801 et seq. (commonly known as the Gramm-Leach-Bliley Act).

[7] *See, e.g.,* Susan Llewelyn Leach, *Privacy Lost With the Touch of a Keystroke?*, 11/10/04 CHRISTIAN SCI. MONITOR 15, at 2004 WLNR 6716743; William Safire, *Medical Intrusiveness Puts Privacy Rights on the Ropes,* 3/11/04 SAN MATEO COUNTY TIMES, at 2004 WLNR 17216303.

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, 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, and then focuses on 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. Opportunities for seizing competitive advantage, and for fostering cooperative mutual advantage, through government action are explored, several likely equilibrium states are posited, and a single ultimate equilibrium is predicted.

Part II 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 and actors among which information interactions take place. Then, Part III 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 IV expresses the US-EU privacy conflict as an extensive form game, explains the history of interaction between the actors in terms of such game, and assesses the

---

[8] *See generally* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L. J. 2381 (July 1996); 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 (Fall 2004).

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.

II. 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.[9] Increasingly, the "commodity production of knowledge" is the focus of advanced economies.[10] 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.[11] In what has been called an "unprecedented proliferation of records and data," vast fields of information about people and their activities populate large and valuable databases.[12] In the modern information economy, even navigating

---

[9] By some estimates, "as 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 3 (October 22, 2005).

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

[11] 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 (August 18, 2003) available at www.rfidjournal.com/article/articleview/539/1/1/; Laurie Sullivan, *Wal-Mart Outlines RFID Expansion Plans*, INFORMATION WEEK (June 17, 2004), available at www.informationweek.com/story/showArticle.jhtml?articleID=22100511.

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

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.[13] 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 an Amazon.com to provide "1-Click" ordering, Wish Lists, and product recommendations for its regular customers.[14] 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.

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.

---

[13] *See* Baron, *supra* note 11, at135; Solove, *supra* note 13, at 1394.

[14] 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. The order can be processed with the click of a single on-screen button. Wish Lists allow users to store their shipping information along with a list of gifts that they would like to receive. 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. Amazon provides its "Recommendations" service by examining a user's past purchases and past ratings of items. By comparing purchasing behavior of other users whose purchase history overlaps with that of the first user, the company recommends future items for consideration. *See* www.amazon.com/exec/obidos/tg/browse/-/508510/ref=br_lr_/102-4428196-8289759.

Actors in the marketplace for information assets, including individual data subjects, negotiate, sometimes overtly, 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.[15] 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.[16] Absent a negotiation over use of personal data, many on-line transactions could not occur at all.[17] Overall, the marketplace in personal information has been said to promote lower costs for businesses and for society as a whole.[18]

---

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

[16] *Id.* at 80-81.

[17] 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.

[18] Robert W. Hahn and Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN L. REV. 85, 86 (2002). *See also Id. at 106* (describing how information collection and credit reporting facilitate

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.[19] However, while the "price" of an individual's data may be readily apparent in some situations (in order to receive a confirmation/receipt, I must provide my 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."[20]

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.[21] 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 psychological profile."[22]

---

pooling of loans, increasing creditor liquidity and making more funds available to borrowers at lower cost).

[19] 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.

[20] *See* Robert W. Hahn and Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN L. REV. 85, 103 (2002)

[21] *See Id.* at 102.

[22] Daniel J. Solove, *supra* note 13, at 1404.

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."[23] The frustration described by Solove explains the periodic public outcry over a particular announced use or misuse of personal information[24], as well as attempts by users of personal

---

[23] *Id.* at 1421.

[24] 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 Direct. 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 Direct's databases. 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. 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, e.g.,* Jeri Clausing, *US Investigating DoubleClick Over Privacy Concerns*, 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 February 18, 2000, available at http://www.privacytimes.com/NewWebstories/doubleclick_priv_2_23.htm.

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. 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. *See, e.g.,* Timothy Burn, *Database Companies Agree to Police On-line Information on Net Users,* The Washington Times June 11, 1997 B12.

Also in 1997, online portal Yahoo! discontinued its reverse telephone directory, which had allowed users to access the name and address of an

information to assuage that frustration. An example of such an attempt is the corporate Website privacy policy.[25] 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?[26] Paula Baron characterizes the debate over privacy and the use of data as being "about the struggle for ownership in pure information.[27] The struggle may also be characterized as one for the economic/marketing value represented by personal information. As discussed further *infra*, the struggle defined by Baron is ongoing, contextual, and advanced by a potential host of players beyond the individual and his bookseller.

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

---

individual by entering that person's telephone number. The company cited e-mail complaints received from users as the reason for abandoning the service. *See, e.g., Yahoo Pulls Phone Search*, available at http://news.com.com/Yahoo+pulls+phone+search/2100-1023_3-259291.html.

[25] 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 . . . phrased in a vague, self-aggrandizing manner to make the corporation look good.")

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

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

"concrete, historical, and factual circumstances of life."[28] Privacy, and in particular, information privacy, "is not reducible to a single set of neutral conditions that apply to all matters we deem private."[29] 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.[30]

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.[31] In U.S. West, the telecommunications carrier used First Amendment grounds to challenge FCC rules implementing consumer privacy provisions of 47 U.S.C. § 222.[32] Using the Central Hudson

---

[28] *See* Solove, *supra* note 26, at 1091.

[29] *Id.* at 1092.

[30] *Id.* at 1093.

[31] *Id.* at 1152.

[32] 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 "[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). The statute provides exceptions for, *inter alia,* billing, fraud prevention, and inbound telemarketing and administrative services. *See* 47 U.S.C. § 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

intermediate scrutiny test, the Court held that the FCC's restriction on commercial speech did not directly and materially advance a substantial state interest.[33] In questioning the substantiality of the state's interest in protecting privacy, the court falls back on familiar and traditional ways of thinking about the harms that flow from inadequate privacy protection, specifically, the traditional tort paradigm. 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.[34] 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. Although one way of looking at privacy is as the right to secrecy, the right to "conceal discreditable facts,"[35] facts do not have to be discreditable for the individual to have an economic interest in concealing them. Selective disclosure of facts about herself 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 with regard to my virtue, trustworthiness, or sense of honor. Nevertheless, I might be selective about revealing this information to an interested party 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'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 our new wine into old bottles will not suffice, and updated paradigms of how multiple actors

---

information could be used for marketing purposes. *See* U.S. West, Inc. v. Federal Communications Commission, 182 F. 3d 1224, 1230 (10th Cir. 1999).

[33] 182 F. 3d at 1240.

[34] Solove, *supra* note 26, at 1153.

[35] Richard A. Posner, ECONOMIC ANALYSIS OF LAW 40 (6th ed. 2003). *See also* Solove, *supra* note 26 at 1106.

(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.[36]

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 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, the "traditional" privacy mentioned earlier in this Article.[37] Although this pairing is typically discussed in terms of civil liberties, individual rights, or constitutional rights,[38] it may also be

[36] Solove, *supra* note 26, at 1127.

[37] *Supra,* 1-2.

[38] 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.

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 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's 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 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 company 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, or for each new use, or for each request for additional information. For example, the customer 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 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.[39] As the size of a bulk e-mail list grows, the probability of the Illegitimate Business receiving a positive response, and a potential sale, increase. Even though response rates to bulk marketing (including bulk mail and bulk e-mail) are extremely low,[40] 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.[41] 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 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 services provider by the Illegitimate Business.[42] In the United States,

---

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

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

[41] *See* Fisher, 23 COLUM.-VLA J.L. & ARTS 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).

[42] The costs of spam are particularly irksome to Individuals, because such costs are almost completely externalized by the sender. The marginal cost

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.[43] 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.[44]

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.[45] I will refer to the Individual trying to protect her information as the data subject, and the Individual seeking to profit from the data subject's information as the identity thief. 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

---

to the Illegitimate Business will tend toward zero. *See, e.g.,* Ayres and Funk, 20 YALE J. ON REG. AT 136.

[43] CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act), P.L. 108-187, 117 Stat. 2719.

[44] 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. 15 U.S.C. § 7706.

[45] Identity theft is "the deliberate assumption of another person's identity, usually to gain access to their finances or frame them for a crime." *See* http://en.wikipedia.org/wiki/Identity_theft.

data subject.[46] The data subject's main options for retaining the value of 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.[47] As we will see later in this Article, information policy can be used to reinforce the cohesion of a trade alliance. The next section 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. We will see that, as with the other contexts discussed *supra,* the essence of the relationship is a contextual, ongoing, negotiation and competition over the value in the personal information of Individuals.

---

[46] 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. 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. *See Do You Know Where Your Identity Is? Personal Data Theft Eludes Easy Remedies*, available at http://knowledge.wharton.upenn.edu/index.cfm?fa=printArticle&ID=1176.

[47] 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, *Rules, Regulations of Global Economy are Increasingly Being Set in Brussels*, WALL STREET JOURNAL, April 23, 2003.

III. 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 ideas about data privacy, including the appropriateness of government regulation of the collection and use of personal information by the private sector. 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 set the stage for the dissimilar privacy approaches and outcomes that we observe 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.[48] Stephen Kobrin has described the European approach to privacy as putting the burden of protection on society rather than the individual.[49] Others have noted that "[g]overnment on the European continent is perceived . . . 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."[50] Still others have gone as far as to call the European privacy model a "command and control model, with precise

---

[48] *See, e.g.,* 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).

[49] Stephen J. Kobrin, *Safe Harbors are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, 30 REV. INT'L STUDIES 111, 116 (2004) (contrasting with American approach to privacy, emphasizing individual ownership and control over, and alienability of, personal information).

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

rules governing the handling of personal information."[51] James Whitman mines the 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.[52] The EU Directive on Data Protection makes clear the approach expected of its Member States when it declares that "data-processing systems are designed to serve man" and must "respect the fundamental rights of individuals, notably the right to privacy."[53]

By contrast, privacy in US law is generally concerned with privacy rights against the government.[54] "At its conceptual core, the American right to privacy still takes much the same 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."[55] Regarding private actors, the information privacy philosophy the United States is most often characterized as a market-based or largely *laissez-faire* type of approach (at least for most of the nation's history).[56] In this view, privacy rights are property-like; they

---

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

[52] *See* James Q. Whitman, *The Two Western Cultures Of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1156-1158 (2004) (describing European protection in the areas of consumer data, credit reporting, workplace privacy, civil discovery, dissemination of nude images on the Internet, and shielding criminal offenders from public exposure, and further describing underpinnings of European privacy culture in the European Convention on Human Rights).

[53] Directive 95/46/EC of the European Parliament on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Preamble par. (2), 24 October 1995.

[54] Kobrin, *supra* note 49 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).

[55] Whitman, *supra* note 52 at 1161 (citing Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* 5 (2000).

[56] *See, e.g.,* Steve Lohr, *Seizing the Initiative on Privacy: Online Industry Presses its Case for Self-Regulation*, New York Times October 11, 1999 at C8 (describing concerns raised by the Federal Trade Commission regarding efficacy of the traditional US self-regulatory model of data protection).

are alienable, tradable, and waivable.[57] Such an approach is consistent with Whitman's argument that American notions of privacy are grounded in liberty, rather than dignity.[58] The most important thing is to protect the individual from state intrusion into the choices she 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.[59] 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. The Clinton Administration's Framework for Global Internet 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.[60]

B. Conflicting Legislative Results

Not surprisingly, the legislative regimes of the two jurisdictions in question evolved in markedly different directions. The laws of the United States regarding data protection have justifiably been called a "legal patchwork,"[61] "fragmented,"[62] a "discordant morass,"[63] "reactive,"[64]

---

[57] *See, e.g.,* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, at 1246-1249 (April 1998); Murphy, 84 GEO. L. J. at 2402-2403.

[58] Whitman, *supra* note 52, at 1162-4. Whitman describes American anxieties about privacy as being concerned with "maintaining a kind of private sovereignty within our own walls." In his conception of comparative US-EU 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."

[59] *See* Zinser, *supra* note 48 at 11 (characterizing US policymaking as "reactive," and in favor of targeted solutions to privacy problems).

[60] *See* Felsenfeld, *supra* note 50 at 365; White House Infrastructure Task Force, A Framework for Global Electronic Commerce (July 1997), at http://www.technology.gov/digeconomy/framewrk.htm.

[61] *See, e.g.,* Zittrain, *supra* note 54, at 1229.

"a crazy quilt of piecemeal statutes,"[65] "sporadic,"[66] and "inchoate."[67] Although Congress has considered a number of bills in this area,[68] there is to date no comprehensive federal information privacy statute. Instead, there are sector specific laws designed to address specific types and uses of personal information. As a matter of national statutory law, the US protects, for example, financial information,[69] information about children,[70] health-related information,[71] information contained in credit reports,[72] video rental information,[73]and certain information regarding cable television

---

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

[63] Stephen J. Davidson and Daniel M. Bryant, *The Right of Privacy: International Discord and the Interface with Intellectual Property Law*, 18 COMPUTER & INTERNET LAW. 1 (2001).

[64] *See, e.g.,* Zinser, *supra* note 48, at 12.

[65] Rustad and Koenig, *supra* note 51.

[66] Kobrin, *supra* note 49.

[67] *Id.*

[68] Recent attempts have included the proposed Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (September 29, 2005); the proposed Online Privacy Protection Act of 2005, H.R. 84, 109th Cong. January 4, 2005); and the proposed Consumer Privacy Protection Act of 2005, H.R. 1263, 109th Cong. (March 10, 2005).

[69] *See* Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6801 et seq.

[70] *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 et seq.

[71] *See* the Health Insurance Portability and Accountability Act of 1996, and its attendant Privacy Rule.

[72] See Fair Credit Reporting Act, 15 U.S.C. § 1581.

[73] *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

subscribers.[74] 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 . . ."[75] More specifically, section 5 of 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.[76] Additionally, protection against certain specific and intrusive uses has been provided by recent federal action in the areas of, for example, SPAM and unwanted telemarketing calls.[77] By and large, however, most of the immense amount of data collected by private interests in the US slips through the statutory cracks of US law.[78]

Meanwhile, information privacy protection in the European Union has long been the subject of comprehensive legislative action. Beginning in the 1970's, several countries developed national laws regulating the processing of data about individuals, including collection, use, and storage.[79] These laws, although emanating from a shared

---

[74] *See* customer proprietary network information provisions of the Telecommunications Act of 1996, 47 U.S.C. § 222.

[75] Banks, savings & loan institutions, credit unions, and common carriers are excepted from this authority. FTC Act Section 6(a), 15 U.S.C. § 46 (a).

[76] 15 U.S.C. § 45 (a) (1).

[77] *See* the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 **(**also known as the CAN-SPAM Act), and the federal Do-Not-Call Registry.

[78] 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.

[79] *See* European Commission, Data Protection Background Information, at http://europa.eu.int/comm/internal_market/privacy/adequacy/background-info_en.htm; Act on Data Processing, Date Files and Individual Liberties, January 1978 (France); Act Relating to Personal Data Registers, June 1978

understanding of individual rights, did not provide a uniform level of protection.[80] 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 EU 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 (the "EU Data Protection Directive" or "EU Directive").[81] The EU Directive prescribes specific requirements for the handling (or "processing") of personal data, defined as "any information relating to an identified or identifiable natural person."[82] 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."[83]

"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."[84] The Directive covers the processing activities of both "data controllers" (those who determine the purposes of, and means for, processing), and "data processors" (those who actually process the data on behalf of a controller).[85]

(Norway); Data Protection Act, July 1989 (Netherlands); Data Protection Act, Number 25 of 1988 (Ireland).

[80] *Id.*

[81] *Id.*

[82] Directive 95/46/EC of the European Parliament on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 24 October 1995.

[83] *Id.*

[84] Directive 95/46/EC of the European Parliament, art. 2(b), 24 October 1995.

[85] Directive 95/46/EC of the European Parliament, art. 2(d), 2(e), 24 October 1995.

The Member States of the EU are required to adopt national laws consistent with the Directive, which 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.[86]

The Directive requires that the laws enacted by Member States provide for adherence to certain principles in the processing of personal data. Personal data must be processed fairly, processed 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.[87] Member States must provide in their national laws that personal data may only be processed where

> (a) the data subject has given his consent unambiguously; 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 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).[88]

---

[86] Directive 95/46/EC of the European Parliament, art.4, 24 October 1995.

[87] Directive 95/46/EC of the European Parliament, art.6, 24 October 1995.

[88] Directive 95/46/EC of the European Parliament, art.7, 24 October 1995.

Certain categories of data receive an even higher level of protection under the Directive. 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.[89]

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.[90] The access right, provided by Article 12 of the 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 categories of data being processed, purpose of the processing, source of the data, and the logic by which the data is being processed.[91] Article 12 also provides that data may be rectified, erased, or blocked, if its processing does not comply with the provisions of the Directive.[92] 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.[93] 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.[94]

Data controllers face additional requirements and constraints under the 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. The

---

[89] Directive 95/46/EC of the European Parliament, art.8, 24 October 1995.

[90] Directive 95/46/EC of the European Parliament, art.10-11, 24 October 1995.

[91] Directive 95/46/EC of the European Parliament, art.12, 24 October 1995.

[92] *Id.*

[93] Directive 95/46/EC of the European Parliament, art.14, 24 October 1995.

[94] Directive 95/46/EC of the European Parliament, art.15, 24 October 1995.

appropriateness of security measures is to be determined with reference to the state of the art regarding data security.[95] 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.[96] 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.[97] All Member States of the union were required by the Directive to enact implementing legislation bringing their national laws into harmony with the Directive's requirements by October 1998.[98]

C. The Tie That Binds

The EU Data Protection Directive certainly establishes a comprehensive regime, one that might even seem stifling to a person or company used to a more American information privacy ethos. But why exactly did Europe'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 EU is enormous. In 2003, the total value of trade with the 15 nations that made up the EU when the Directive was adopted was almost $400 billion.[99] By one estimate, inclusion of transactions between affiliates in the trade calculation would bring the value of US-EC trade to $1.7 trillion.[100] As the European Union continues to

---

[95] Directive 95/46/EC of the European Parliament, art.17, 24 October 1995.

[96] *Id.*

[97] Directive 95/46/EC of the European Parliament, art.18, 24 October 1995.

[98] Directive 95/46/EC of the European Parliament, art.32, 24 October 1995.

[99] *See* Trade with European Union (15): 2003 at http://www.census.gov/foreign-trade/balance/c0011.html#2003. Total trade for the first five months of 2005 with the 25 nations of the recently expanded Union was $202 billion. *See* Trade with European Union: 2005 at http://www.census.gov/foreign-trade/balance/c0003.html.

[100] *See* Gregory Schaffer, *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 (2002) (citing *Transatlantic Governance in Historical and*

expand, the value of transactions between the two jurisdictions can be expected to continue to grow as well.[101] Much of the commercial traffic between the United States and the EU 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[102]) may involve the collection of information from and/or about a customer. Online purchases of services or technology goods (such as software) similarly involve exchanges of information.

Secondly, the Directive creates the possibility that the streams of information alluded to above might come to a halt. Article 25 requires the Member States to allow transfers of personal data to countries outside of the EU only if "the third country in question ensures an adequate level of protection."[103] "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 those countries."[104] A finding of inadequacy requires a Member State to take steps to prevent transfers to a given third country.[105] A third country may enter into negotiations with the

---

Theoretical Perspective, in Transatlantic Governance in the Global Economy 3, 4 (Mark Pollack & Gregory Shaffer eds., 2001)).

[101] 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. An additional four nations (Bulgaria, Croatia, Romania, and Turkey) are currently candidate countries.

[102] *See, e.g.,* the Nike ID online customization store at http://nikeid.nike.com/nikeid/index.jhtml?ref=www.nike.com#home.

[103] Directive 95/46/EC of the European Parliament, art.25 (1), 24 October 1995.

[104] Directive 95/46/EC of the European Parliament, art.25 (2), 24 October 1995.

[105] Directive 95/46/EC of the European Parliament, art.25 (4), 24 October 1995.

European Commission in order to rectify the situation, and may achieve adequacy via its domestic law or its international commitments.[106] Article 26 provides a number of derogations from, or exceptions to, Article 25's prohibition on transfers to countries with inadequate privacy protection. 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.[107] 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.[108]

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.[109] The 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.[110] The practical limitations of Article 26 and the stark prohibitions of Article 25 have resonance with US-based companies because the United States was not at the time of the Directive's adoption, nor is it currently, deemed to provide adequate protection to personal data.[111] Without some sort of accommodation on either side, the American

---

[106] Directive 95/46/EC of the European Parliament, art.25 (5) – 25 (6), 24 October 1995.

[107] Directive 95/46/EC of the European Parliament, art. 26 (1), 24 October 1995.

[108] Directive 95/46/EC of the European Parliament, art. 26 (2), 24 October 1995.

[109] *See, e.g.,* Rose Barcelo, *Seeking Suitable Options for Importing Data from the European Union*, 36 INT'L LAW 985, 995 (Fall 2002).

[110] *See, e.g.,* Rose Barcelo, 36 INT'L LAW at 996.

[111] 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/EC on July 26, 2000); Canada (Commission Decision 2002/2/EC on December 20, 2001); Argentina (Commission Decision 2003/490/EC on June 30, 2003);

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 US 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 EU standards without unduly burdening US-based multinationals.[112] The result was Safe Harbor, a self-certification program that allows participating US firms to be deemed adequate protectors of personal data, as far as the Member States of the EU 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.[113] Participating companies join Safe Harbor by annually certifying to the Department of Commerce that they are in compliance with seven Safe Harbor Principles.[114] They must also state in their published privacy statements that they adhere to the principles. A firm may achieve the promised adherence by "(1) join[ing] a self-regulatory privacy program that adheres to the safe harbor's

---

Guernsey (Commission Decision 2003/821/EC on November 21, 2003); and the Isle of Man (Commission Decision 2004/411/EC on April 28, 2004). *See, e.g.,* Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries at http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm.

[112] *See* Kobrin, *supra* note 49, at 113.

[113] *See* Safe Harbor Benefits, available at http://export.gov/safeharbor/sh_overview.html. *See also generally* Commission Decision on Adequacy of Safe Harbor, July 28, 2000, available at http://www.useu.be/ISSUES/deci0728.html.

[114] *See* Shaffer, *supra* note 100, at 62.

requirements; or (2) develop[ing] its own self regulatory privacy policy that conforms to the safe harbor."[115] The Department of Commerce maintains a list of companies that have self-certified.[116]

The seven Safe Harbor Principles are: Notice, Choice, Onward Transfer, Access, Security, Data Integrity, and Enforcement. 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. Data subjects must have access to their data and be reasonably able to correct, amend, or delete their information. 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.[117]

Participation in Safe Harbor is currently open to organizations that are subject to the regulatory authority of the Federal Trade Commission or the United States Department of Transportation.[118] 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.[119] Under Section 5 of the Federal Trade Commission Act, along with the terms of the Safe Harbor program, participants who fail to provide adequate protection may be subject to an

---

[115] *See* Safe Harbor Overview, available at http://export.gov/safeharbor/sh_overview.html.

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

[117] For a more detailed treatment of the Safe Harbor Principles, see http://export.gov/safeharbor/sh_overview.html.

[118] 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.

[119] *See* Safe Harbor Overview: Government Enforcement at http://export.gov/safeharbor/sh_overview.html.

FTC action for engaging in "unfair or deceptive acts or practices in or affecting commerce."[120] 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.[121]

Safe Harbor has received mixed reviews. To some, it represents a successful compromise that may contribute to "a gradual convergence in data privacy practices."[122] 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."[123] Participation levels have not been overwhelming. As of January 2006, approximately 850 companies were current in their certification status with the Safe Harbor program.[124] This represents a fairly small percentage of US companies in total. Of the current Safe Harbor companies, only 60 are members of the Fortune 500. 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,[125] but has also noted the absence of complaints from data subjects as one indication that those companies that are registered are mainly in compliance.[126] Of greater concern to the Commission is the fact

---

[120] *See* 15 U.S.C.A. § 45 (a) (1).

[121] *See* Safe Harbor Overview: Government Enforcement at http://export.gov/safeharbor/sh_overview.html.

[122] Shaffer, *supra* note 100, at 66.

[123] Kobrin, *supra* note 49, at 128.

[124] *See* Safe Harbor List at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list!OpenDocument&Start=772.

[125] 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.

[126] *See* Commission Staff Working Document on the Implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and Frequently Asked

that few Safe Harbor companies have incorporated the Safe Harbor Principles into their written privacy policies to the Commission's satisfaction, and the EC seeks a more proactive compliance effort from the Department of Commerce and the FTC.[127] How did the EU and US 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? The next Part examines and assesses the interaction of the US and EU using concepts from game theory and attempts to chart a course for a more satisfactory outcome.

Questions issued by the US Department of Commerce, October 10, 2004, at 6.

[127] *See Id.* at 7-8.

IV. Setting the Model

The utility of game theoretic models to analyze problems of law and policy is well established.[128] Scholars have used game theory analysis to model competitive behavior with respect to valuable intangible assets, such as intellectual property.[129] 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.[130] 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.[131] 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 playing

---

[128] *See generally* Martin Shubik, *Game Theory, Law, and the Concept of Competition*, 60 U. CIN. L. REV. 285 (Fall 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).

[129] *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, 317 (Fall 1991) (modeling foreign direct investment decisions, including technology transfer); Ruth Okediji, *Public Welfare and the Role of the WTO: Reconsidering the TRIPS Agreement*, 17 EMORY INT'L L. REV. 819 (Summer 2003) (analyzing negotiation of the Agreement on Trade-Related Aspects of Intellectual Property, or TRIPS Agreement).

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

[131] Shubik, 60 U. CIN. L. REV. at 288.

environment).[132] 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.[133] 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. As noted above, however, a player does not know which strategy her co-player will actually choose.[134] 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 US 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 administrative and/or judicial apparatus to enforce the regulatory regime. The decision to regulate also reduces US 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 more timely basis. Fewer transactions may be completed by US 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 US as a player in the game, the decrease in the revenue of US firms can be represented as an aggregate loss by all US firms, or as a loss of tax revenues for the US as a state (such tax revenue loss amounting to a percentage of the aggregate loss by the firms).

The EU 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 US. However, we assume the EU's marginal cost to be lower than the US cost, due to a more developed pre-existing infrastructure for the regulation of commercial transactions,

---

[132] *See* Douglas G. Baird et al., GAME THEORY AND THE LAW 6-7 (1994).

[133] *See Id. at 8.*

[134] *Id. at 10.*

including data transactions.[135] A decision by the EU to Restrict reduces US revenues, potentially by a larger amount than that caused by a US decision to Regulate (due to, for example, less concern on the part of EU regulators for revenue effects of their activities on foreign firms than US regulators would likely demonstrate for their own domestic firms). If the EU decides to Allow, it faces a number of costs, some 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 EU Member States for failing to protect their rights, or make increased use of the administrative and judicial apparatus 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 EU might incur by deciding to Allow. If the EU Restricts, more transactions that would otherwise have been completed between EU consumers and US merchants will instead be completed between EU consumers and EU firms. Therefore, by Allowing, the EU creates the possibility for the US to capture more of the value of the personal data of EU consumers. This value is made up of the raw value of transactions with EU consumers, plus whatever multiplier effect operates on future transactions.[136] The value-capture issue forces the EU, when making the Allow/Restrict decision, to consider the global reach of US firms, the relatively aggressive marketing culture of US business, and the general orientation among US 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 EU consumers is 100. The US faces a cost to Regulate of 20. The EU maintains a baseline cost of regulation of 10, reflecting a more highly regulated economy in general than that of the US. If the EU chooses to Restrict, it incurs an additional cost of 10. If the US declines to

---

[135] *See* discussion *supra*, Part III(A).

[136] 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.

Regulate, while the EU chooses to Allow, the US captures 70% of the value of the personal data, with the EU capturing 30%, less its baseline regulatory costs of 10, for a net payoff of 20. If the US declines to regulate while the EU Restricts, the US captures 40% of the value, while the EU receives 60%, less regulation costs of 10 and costs to Restrict of 10, resulting in a net payoff of 40. If the US Regulates while the EU Allows, each captures half the value of the data, less their respective regulation costs (20 in the case of the US, and 10 in the case of the EU. If the US Regulates while the EU Restricts, the US earns 30% of the value, less regulation costs of 20 (for a payoff of 10), while the EU captures 70% of the value, less baseline regulation costs and cost to Restrict (for a net payoff of 70 minus 20, or 50). The matrix and each party's payoffs appear as below[137]:

EU

US	**Allow**	**Restrict**
Regulate	(30, 40)	(10, 50)
Don't Regulate	(70, 20)	(40, 40)

[137] In each pair of payoffs, the US payoff is listed first, and the EU payoff second.

A strictly dominant strategy for the US under this model is non-Regulation.[138] Regardless of whether the EU decides to Allow or Restrict, the US is better off choosing not to Regulate (earning a payoff of 70 versus 30 in the event of an Allow strategy by the EU, and earning a payoff of 40 versus 10 in the event of a Restrict strategy by the EU). Given the dominance of the Don't Regulate strategy for the US, the EU, acting rationally, will be forced to pursue a Restrict strategy. As the EU expects the US 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 an equilibrium, it does not necessarily produce an optimal or even desirable result. The US ends up capturing less value than it otherwise would, and processing fewer transactions with EU consumers. This is obviously a poor result for the US, but it also problematic for EU consumers, some significant number of whom *want* to transact with US firms. There are transactions for which US firms might be better suited, either because EU firms do not provide the goods/services involved, or because US firms can provide the goods/services more cheaply or efficiently. The inability of such transactions to be consummated represents a loss to the system, potential value uncaptured by anyone. Additionally, there may be some appetite among US consumers for *some* regulation of US firms.[139] An outcome that essentially means zero regulation by the US of its firms is an unfavorable one for US 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 US and EU 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

---

[138] 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., GAME THEORY AND THE LAW, at 11.

[139] The vigorous nature of the debate over privacy issues in the US, 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.

predicted draconian restrictions on data usage.[140] The predictive shortcoming of the normal form game here is due to its inadequately capturing the structure of the relationship between the players. Unlike the motorist and pedestrian often used to illustrate tort applications of the normal form game[141], the US and EU do not make a single decision regarding data protection with no idea of what move will be made by their opponent. 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. The parties use their opponent's early round moves to inform strategy for later rounds. Thus, a more robust tool for analyzing the US-EU 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 players during each round.[142] Despite its usefulness in iterative interactions, however, it is possible to use the extensive form game to model an interaction between the US and EU that does little more than replicate the results of the normal form game. For example, in the figure below, with the US moving first, backwards induction indicates that the outcome will be Don't Regulate/Restrict. Moving last, and faced with the indicated choices, the EU will choose Restrict over Allow in the event of a US decision to Regulate (earning 50 rather than 40, as in the normal form model above), and will also choose Restrict over Allow in the event of a US decision not to Regulate (earning 40 over 20, as in the normal form model above).[143] The US, in determining

---

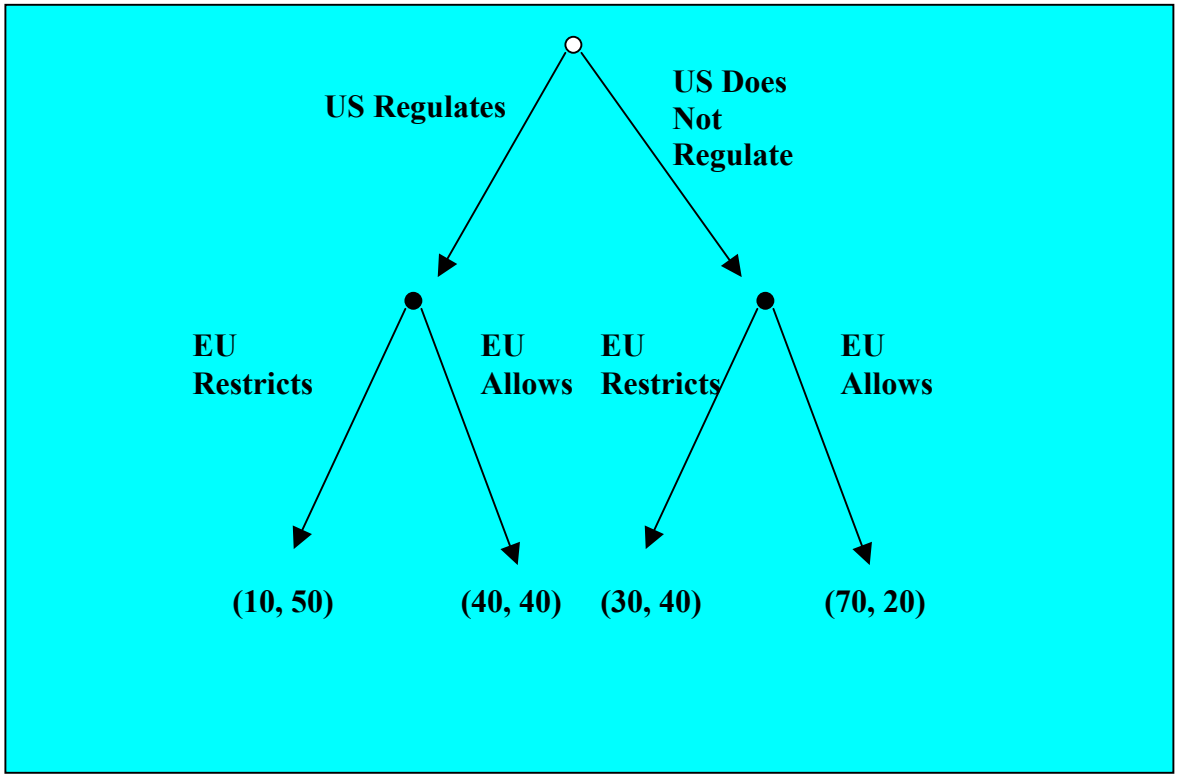
[140] *See* discussion, *supra* at III.D., regarding the US-EU Safe Harbor program.

[141] *See, e.g.,* A. Mitchell Polinsky, An Introduction to Law and Economics 43 (3d ed. 2003) (citing John Prather Brown, *Toward an Economic Theory of Liability*, 2 J. LEGAL STUD. 323 (1973); Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1 (1980); Peter A. Diamond, *Single Activity Accidents*, 3 J. LEGAL STUD. 104 (1974).

[142] *See generally* Shubik, 60 U. CIN. L. REV. at 286-288.

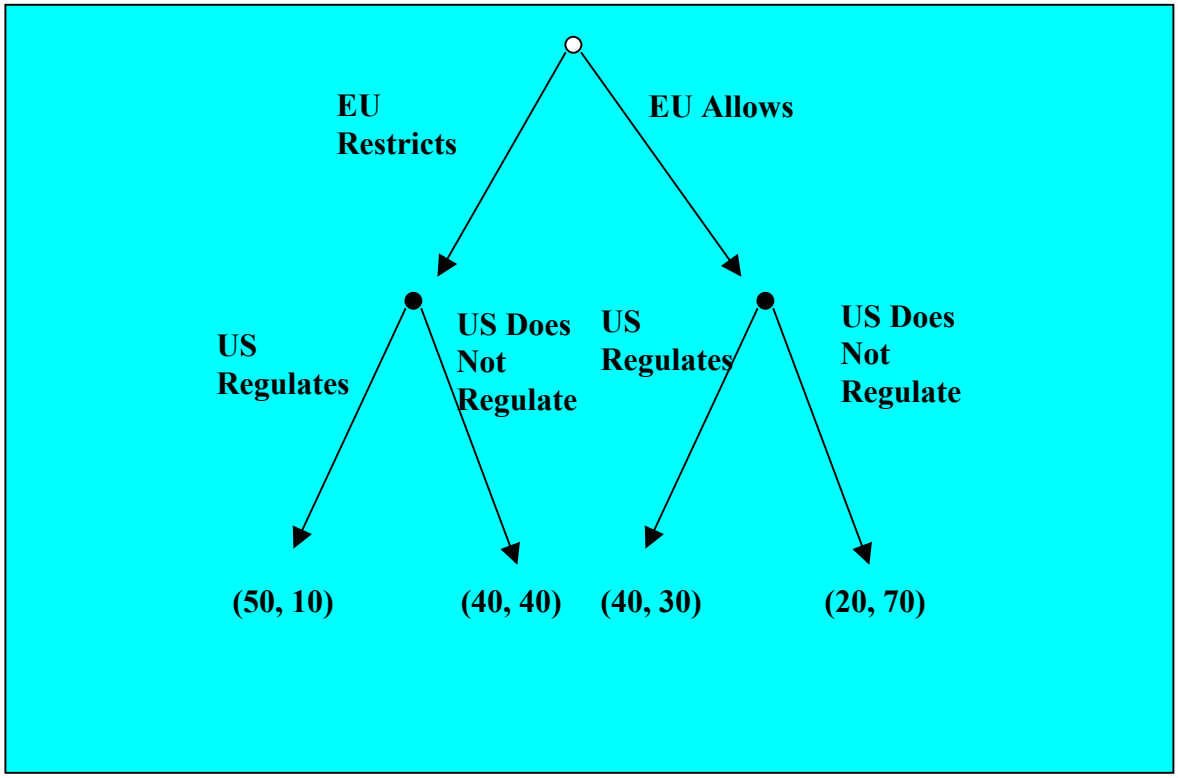
[143] By convention, in each pair of payoffs, the payoff of the first mover, in this case the US, is listed first.

its first move, will take in to account that the EU's only rational strategy in the second round is Restrict. Therefore, in order to secure a payoff of 30 rather than 10, the US will choose Don't Regulate.



Under the current set of payoffs, the outcome is no different if the EU is the first mover (See figure below). Moving last, the US will choose Don't Regulate as its more lucrative strategy in the case of both possible moves by the EU. Don't Regulate nets the US a payoff of 70 over 30 in the event of an Allow decision, and a payoff of 40 over 10 if the EU has chosen Restrict. Knowing the decision set faced by the US in the last

move, the EU will choose Restrict in the first move, in order to earn 40 rather than 20.[144]



To demonstrate more accurately the impact of iterative play in the US-EU data protection game, we must make adjustments to the model. The revised model introduces an additional round of play, with the EU playing first. The EU chooses strategy, the US follows, and then the EU receives a final play.[145] Along with the additional round, there are

[144] By convention, in each pair of payoffs, the payoff of the first mover, in this case the EU, is listed first.

[145] 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 EU makes the first and *n*th moves, and every odd-numbered move in between.

adjustments to the parties' payoffs, due in part to an additional strategy available to the EU: Halt.

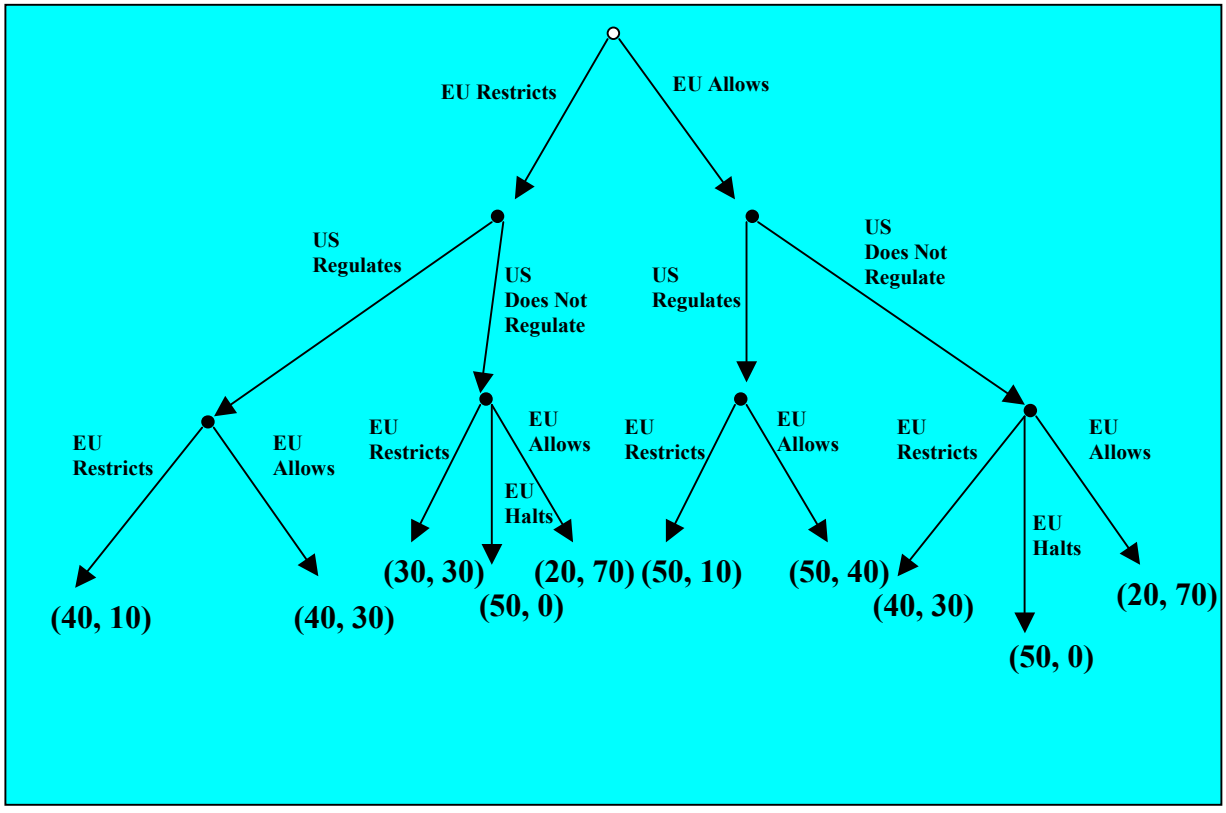
A number of additional assumptions are necessary in analyzing the revised model with the Halt strategy available to the EU. First, adopting the Halt strategy imposes a significant cost on the EU. For purposes of the model, employing the Halt strategy means ceasing all data transfers from the EU to the US. It is obvious that such a move would heavily and negatively impact US payoffs, but the strategy is not without pain for the EU. The Halt strategy would necessitate more rigorous (and expensive) enforcement in order to ensure that no personal information is transferred to the US; such enforcement costs can be expected to reduce the net amount of any payoff to the EU from the game. Additionally, collaborative opportunities between US firms and EU firms would be lost almost completely under the Halt strategy. Without the ability to share data about customers by transferring data files to US joint venture partners, for example, EU 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 EU to the US are EU firms, or at least EU divisions of US firms. Such firms or divisions may employ EU citizens locally and pay taxes to EU 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 EU.

Given the costs of the Halt strategy to the EU, the EU will not employ the strategy lightly. If during any round the US chooses Regulate as its strategy, the EU can be expected not to pursue the Halt strategy during its turn. If the US chooses Don't Regulate, however, it can expect the EU to choose Halt in the next round, leading to a zero payoff for the US. We also assume that the cost to Restrict is cumulative; if the EU 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 EU initially Restricts, and then Restricts again after the US 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 EU 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 US Regulates in response to a Restrict decision by the EU, the payoff to the US is reduced by 10. This result reflects increased costs caused by the adjustment on the part of US businesses to the practical limitations of the

EU restrictions coupled with the legal burdens of a new US regulatory scheme. If the EU Allows initially, and then Allows again following a US play of Regulate, it gains incremental revenue (its persistently permissive environment acting cumulatively and providing space for more EU-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 EU earns 40 and the US earns 10, while if they pursue Restrict-Regulate-Allow, the EU earns 40 and the US earns 30. A choice by the US not to Regulate following an EU Restrict decision leads to a 30-30 split in payoffs if the EU Restricts again, a payoff of 50 for the EU with a zero payoff for the US if the EU Halts, and a payoff of EU=20 and US=70 if the EU Allows on its second turn. If the players pursue Allow-Regulate-Restrict, the EU earns 50 and the US earns 10, while if they pursue Allow-Regulate-Allow, the EU earns 50 and the US earns 30. Meanwhile, a choice by the US not to Regulate following an EU Allow decision leads to a payoff of EU=40 and US=30 if the EU Restricts, a payoff of 50 for the EU with a zero payoff for the US if the EU Halts, and a payoff of EU=20 and US=70 if the EU Allows again on its second turn. These payoffs are illustrated in the figure below.



We can predict that the US will not pursue any strategy that would present the EU with a Restrict/Halt/Allow set of strategy choices. When presented with such a choice, the EU 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 EU's choosing the Halt strategy (and consigning the US to a payoff of 0) is for the US *not* to choose Don't Regulate. Knowing that the US will not elect a strategy that presents the Halt option to the EU, we can effectively remove the branches of the tree that include a choice by the US not to Regulate. 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 EU 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 EU is indifferent, as either will yield a payoff of 50.

If, after an Allow-Regulate set of moves by the players, the EU 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 US) and an Allow choice by the EU? One explanation involves each player's communicating important information to the other in advance of, or even simultaneously with, its actual moves in the game. First, the EU communicates to the US a credible threat to reduce its payoff from data transfers to zero. The framework constructed by the Data Protection 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.[146] In any round where such a strategy is available to the EU, the EU rationally adopts it, because of the opportunity for a superior payoff. Knowing this fact, and respecting the threat, the US has an incentive to avoid the "Halt" choice presenting itself in any given round of play. Thus, the US is pushed toward the adoption of some kind of Regulate strategy.

---

[146] *See* Directive 95/46/EC of the European Parliament, art.25, 24 October 1995.

Once the Regulate strategy is chosen by the US, there is still the question of whether the EU will choose Restrict or Allow (each of which offers the same EU payoff). The US has an incentive to attempt to induce an outcome that produces a higher US 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 EU might cooperate with such a move by the US (by Allowing rather than Restricting on its second and later turns) because the certainty of some regulation by the US is better than the uncertainty of the game without the US 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 US to communicate some commitment to privacy and implement some mild form of regulation, Safe Harbor, and the Allow-Regulate-Allow progression that it represents, thus presents a Pareto superior outcome to the Allow-Regulate-Restrict progression that might otherwise unfold.[147]

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 the nations of the EU, and seems to preserve elements of the historical American *laissez-faire* approach. For example, rather than US 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, and they have the option to have

[147] 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. 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. *See, e.g.,* Richard A. Posner, Economic Analysis of Law at 12-13 (6th Ed. 2003).

privacy disputes settled privately.[148] Other nations that have earned the "adequate" designation from the EU have had to create much more pervasive and comprehensive systems in order to do so.[149]

The EU's own assessment of the game illustrates the degree to which the US has been able to implement a "Regulate Lite" system. The Commission Staff Working Document on the implementation of Safe Harbor (the "Safe Harbor Report"), required by Decision 520/2000/EC[150], 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.[151] 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 US regulators, and it is unclear at best whether any of the members' privacy policies undergo regulatory scrutiny.[152] The EU Safe Harbor Report expresses concern with the effectiveness of Safe Harbor companies' attempts to translate the Safe

---

[148] *See* Safe Harbor Frequently Asked Questions FAQ 6, available at http://export.gov/safeharborFAQ6SelfCertFINAL.htm; FAQ 11, available at http://export.gov/safeharborFAQ11FINAL.htm.

[149] 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 that the organization collects, uses or discloses in the course of commercial activities; or is about an employee of the organization . . ." PIPEDA imposes specific affirmative obligations on collection, use, disclosure, access, notice, and the like. Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5.

[150] 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* Commission Staff Working Document on 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 Department of Commerce 3 (October 20, 2004).

[151] *Id.* at 5.

[152] *Id.* at 6.

Harbor principles into written (and posted) privacy policies, and proposes a more proactive posture on the part of the Department of Commerce and the Federal Trade Commission in policing these issues.[153] The issues raised by the 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 US however, nor is it a pure loss for the EU. Although the Commission notes that there have been no comprehensive audits of compliance with Safe Harbor principles, it also notes that it has received no complaints from data subjects.[154] 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.[155]

It may be that, from the perspective of the European data subject, US 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 Report, the Commission finds that the US Department of Commerce is generally "carrying out its role in accordance with the Safe Harbor requirements."[156] Additionally, there is much anecdotal evidence that US 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. [157] Even though the result here can

---

[153] *See* Decision 520/2000/EC, *supra* note 150, at 7-8.

[154] *Id.* at 6.

[155] *Id.* at 11.

[156] *Id.* at 13.

[157] *See, e.g.,* John Schwartz, *The Nation: Surveillance 101; Privacy and Security on Campus*, NEW YORK TIMES, August 4, 2002; Claudia Rose, *In Business; Keeping it Confidential*, NEW YORK TIMES, March 3, 2002.

be counted as a US win, it certainly presents an outcome much more favorable to the EU than that which would result from total US non-cooperation.

The US-EU 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."[158] 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.[159] When these keys are present, iteration can lead to more cooperative behavior than defecting behavior, and to more jointly beneficial outcomes.[160] 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.[161]

Game theory also predicts the structural and institutional underpinnings of the US-EU data privacy result. Where several possible equilibria 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 a particular equilibrium, in a way that is recognized by all players, such that such equilibrium is the one expected, and ultimately

---

[158] Chinen, 23 Mich. J. Int'l L. at 148-149.

[159] *Id.* at 167.

[160] *See* Michael Whincop, *The Recognition Scene: Game Theoretic Issues in the Recognition of Foreign Judgments*, 23 Melb. U. L. Rev. 416, 419 (August 1999) (citing Robert Axelrod, the Evolution of Cooperation (1984)).

[161] *See* discussion *supra* at II.A.

implemented, by the players.[162] Communication is a means for creating focal points, and thus treaties, or similar agreements, can serve the as focal points in interactions between states. Cooperative moves that would lead to high joint payoffs can be recorded in an agreement in order to inform parties as they consider their moves during the life of the agreement, and to set a minimum behavioral benchmark.[163] In the case of the US-EU data privacy competition, the EU Privacy Directive, as an agreement among the EU Member States, and the Safe Harbor program (including the reporting mechanism of the Working Party), as an agreement between the EU and the US, serve the focal point function by focusing the players on strategy choices, and therefore equilibria, that involve some level of regulation by the US, in order to avoid possible outcomes that might invoke a cessation of data flows from the EU to the US.

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 initially, but will cooperate in a sustained manner over time.[164] Like agreements, institutions can also serve to reduce uncertainty and transaction costs associated with dynamic playing environments.[165] 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.[166] Given the dynamic nature of the US-EU data collection and usage environment, and the vital nature of the trade, creation of institutions such as the Safe Harbor framework is entirely predictable based on a careful application of game theory concepts in this space.

---

[162] Chinen, 23 MICH. J. INT'L L. at 153.

[163] *See* Jack L. Goldsmith and Eric Posner, *A Theory of Customary International Law,* 66 U. Chi. L. Rev. 1113, 1171 (1999).

[164] Frischmann, 51 BUFF. L. REV. at 719.

[165] *Id.* at 683.

[166] *Id.*

V. Conclusion

What is the future of the US-EU data privacy game? Have the players reached an equilibrium that is, in addition to being mutually beneficial, also stable? 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 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 EU continues to signal, via the EU Safe Harbor Report, that certain US 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 EU also continues to signal that "the EU panel and data protection authorities should invite organizations that subscribe to the 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.[167] 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 EU as a player, to the US as a player, and to their 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.

[167] EU Safe Harbor Report at 8.